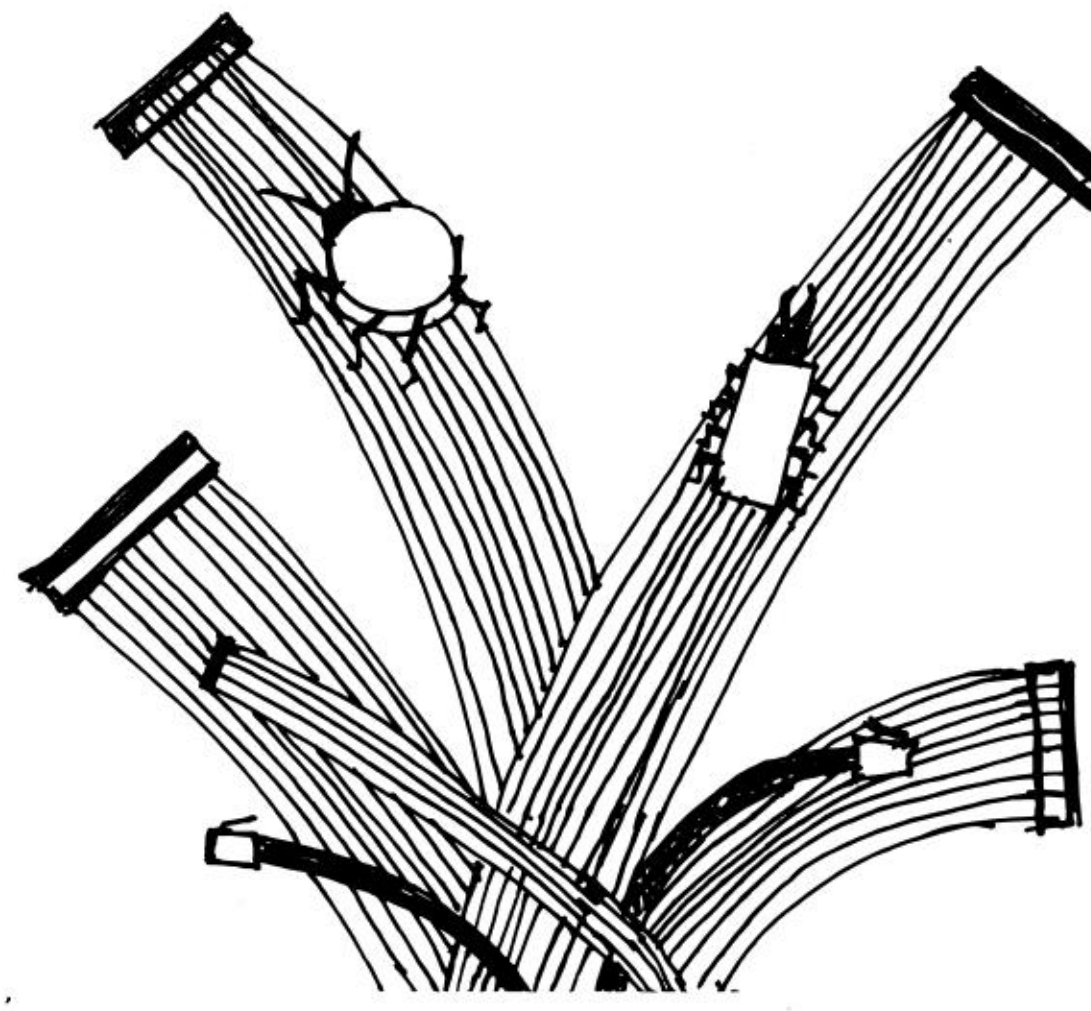
guide d'autodéfense numérique

ouvrage collectif



sixième édition

hiver 2023

guide d'autodéfense numérique

Ouvrage collectif
guide@boum.org

Empreinte OpenPGP :
D487 4FA4 F6B6 88DC 0913
C9FD 326F 9F67 250B 0939

hiver 2023

Réalisé avec des logiciels libres, en particulier *bookdown*, *Pandoc* et *LaTeX* pour la mise en page, *GIMP* et *Inkscape* pour les images, *Scribus* pour les couvertures, *Git* ainsi que de nombreuses discussions pour travailler ensemble, le tout sous *Debian GNU/Linux* et *Tails*.



Copyleft : cette œuvre est libre, vous pouvez la copier, la diffuser et la modifier selon les termes de la *Licence Art Libre* — http://www.artlibre.org/

ISBN : 978-2-912631-05-3

Sommaire

Sommaire iii

Préface à cette édition xi

Pourquoi ce guide ? 1
- Les revers de la mémoire numérique . . . 1
- Rien à cacher ? . . . 1
- Comprendre pour pouvoir choisir . . . 2
- Prendre le temps de comprendre . . . 3

Comment lire ce guide ? 5
- Un tome « hors ligne » . . . 5
- Un tome « en ligne » . . . 5
- Larguer les amarres . . . 5

Tome 1 – Hors connexions 9

I Comprendre 11

Introduction 13

1 Quelques bases sur les ordinateurs 15
- 1.1 Des machines à traiter les données . . . 15
- 1.2 Le matériel . . . 15
- 1.3 Électricité, champs magnétiques, bruits et ondes radio . . . 21
- 1.4 Les logiciels . . . 22
- 1.5 Le rangement des données . . . 23

2 Traces à tous les étages 27
- 2.1 Dans la mémoire vive . . . 27
- 2.2 Dans la mémoire virtuelle . . . 28
- 2.3 Veille et hibernation . . . 28
- 2.4 Les journaux . . . 29
- 2.5 Sauvegardes automatiques et autres listes . . . 29
- 2.6 Les métadonnées . . . 30

3 Logiciels malveillants, mouchards et autres espions **31**
3.1 Contexte légal . . . 31
3.2 Les logiciels malveillants . . . 32
3.3 Les matériels espions . . . 34
3.4 Les keyloggers, ou enregistreurs de frappe au clavier . . . 35
3.5 Les plateformes d'investigation numérique . . . 36
3.6 Des problèmes d'impression ? . . . 36

4 Quelques illusions de sécurité **39**
4.1 Logiciels propriétaires, open source, libres . . . 39
4.2 Le mot de passe d'un compte ne protège pas ses données . . . 41
4.3 À propos de l'« effacement » des fichiers . . . 42
4.4 Les logiciels portables : une fausse solution . . . 44

5 Une piste pour protéger des données : la cryptographie **47**
5.1 Protéger des données des regards indiscrets . . . 47
5.2 S'assurer de l'intégrité de données . . . 53
5.3 Symétrique, asymétrique ? . . . 55

II Choisir des réponses adaptées **57**

Introduction **59**

6 Confiance et réduction des risques **61**
6.1 Réduction des risques . . . 61
6.2 Une histoire de confiance . . . 62

7 Évaluation des risques **63**
7.1 Que veut-on protéger ? . . . 63
7.2 Contre qui veut-on se protéger ? . . . 63

8 Définir une politique de sécurité **65**
8.1 Une affaire de compromis . . . 65
8.2 Comment faire ? . . . 65
8.3 Quelques règles . . . 66

Cas d'usage **69**

9 Cas d'usage : un nouveau départ, pour ne plus payer les pots cassés **71**
9.1 Contexte . . . 71
9.2 Évaluer les risques . . . 72
9.3 Définir une politique de sécurité . . . 72

10 Cas d'usage : travailler sur un document sensible **79**
10.1 Contexte . . . 79
10.2 Évaluer les risques . . . 79
10.3 Quel système d'exploitation privilégier pour travailler sur le document ? 80
10.4 Travailler sur un document sensible… sur un système *live* . . . 82
10.5 Travailler sur un document sensible… sous Windows . . . 82
10.6 Nettoyer les métadonnées du document terminé . . . 88
10.7 Limites communes à ces politiques de sécurité . . . 88

11 Cas d'usage : archiver un projet achevé **89**
11.1 Contexte . . . 89
11.2 Est-ce bien nécessaire ? . . . 89
11.3 Évaluer les risques . . . 89
11.4 Méthode . . . 90
11.5 Quelle phrase de passe ? . . . 90
11.6 Un disque dur ? Une clé ? Plusieurs clés ? . . . 91

III Outils **93**

Introduction **95**

12 Utiliser un terminal **97**
12.1 Qu'est-ce qu'un terminal ? . . . 97
12.2 À propos des commandes . . . 98
12.3 Privilèges d'administration . . . 99
12.4 Mise en garde . . . 100
12.5 Un exercice . . . 100
12.6 Attention aux traces ! . . . 101
12.7 Pour aller plus loin . . . 101

13 Choisir une phrase de passe **103**

14 Démarrer sur un CD, un DVD ou une clé USB **107**
14.1 Essayer naïvement . . . 107
14.2 Tenter un choix ponctuel du périphérique de démarrage . . . 107
14.3 Modifier les paramètres du microprogramme . . . 108

15 Utiliser un système *live* **113**
15.1 Des systèmes *live* discrets . . . 113
15.2 Télécharger, vérifier et installer Tails . . . 114
15.3 Cloner ou mettre à jour une clé Tails . . . 115
15.4 Démarrer sur un système *live* . . . 115
15.5 Utiliser la persistance de Tails . . . 116

16 Installer un système chiffré **119**
16.1 Limites . . . 119
16.2 Télécharger un support d'installation . . . 120
16.3 Vérifier l'empreinte de l'image d'installation . . . 121
16.4 Préparer le support d'installation . . . 122
16.5 L'installation proprement dite . . . 123
16.6 Paramétrage du dépôt principal de paquets Debian . . . 128
16.7 Quelques pistes pour continuer . . . 129
16.8 Un peu de documentation sur Debian et GNU/Linux . . . 129

17 Choisir, vérifier et installer un logiciel **131**
17.1 Critères de choix . . . 131
17.2 Trouver et installer un logiciel . . . 134
17.3 Trouver et installer un paquet Debian . . . 135
17.4 Ajouter des dépôts . . . 136

18 Effacer des données « pour de vrai » 139
18.1 Un peu de théorie . . . 139
18.2 Sur d'autres systèmes . . . 140
18.3 Allons-y . . . 140
18.4 Supprimer des fichiers… et leur contenu . . . 141
18.5 Effacer « pour de vrai » tout un disque . . . 141
18.6 Effacer tout le contenu d'un disque . . . 142
18.7 Rendre irrécupérables des données déjà supprimées . . . 143

19 Partitionner et chiffrer un disque dur 145
19.1 Vue d'ensemble . . . 145
19.2 Préparer un disque à chiffrer . . . 146
19.3 Créer une partition non chiffrée . . . 147
19.4 Créer une partition chiffrée . . . 148
19.5 Utiliser un disque dur chiffré . . . 148

20 Sauvegarder des données 151
20.1 Cas particulier du stockage persistant de Tails . . . 151
20.2 Avec le gestionnaire de fichiers et un stockage chiffré . . . 151
20.3 En utilisant Déjà Dup . . . 153

21 Partager un secret 157
21.1 Partager une phrase de passe . . . 157
21.2 Reconstituer la phrase de passe . . . 158

22 Utiliser les sommes de contrôle 161
22.1 Obtenir la somme de contrôle d'un fichier . . . 161
22.2 Vérifier l'intégrité d'un fichier . . . 162

23 Installer et utiliser un système virtualisé 163
23.1 Installer le Gestionnaire de machines virtuelles . . . 163
23.2 Activer la virtualisation matérielle . . . 164
23.3 Installer un Windows virtualisé . . . 165
23.4 Prendre un instantané d'une machine virtuelle . . . 168
23.5 Restaurer l'état d'une machine virtuelle à partir d'un instantané . . . 168
23.6 Installer un nouveau logiciel sur un système virtualisé . . . 169
23.7 Partager une clé USB avec un système virtualisé . . . 170
23.8 Partager un CD ou un DVD avec un système virtualisé . . . 171
23.9 Partager un dossier avec un système virtualisé . . . 171

24 Garder un système à jour 175
24.1 Garder Tails à jour . . . 175
24.2 Garder à jour un système chiffré . . . 176
24.3 Les mises à jour quotidiennes d'un système chiffré . . . 176
24.4 Passage à une nouvelle version stable . . . 177

25 Nettoyer les métadonnées d'un document 185
25.1 Installer les logiciels nécessaires . . . 185
25.2 Nettoyer un ou des fichiers . . . 185

Tome 2 – En ligne **189**

IV Comprendre **191**

Introduction **193**

26 Bases sur les réseaux **197**
26.1 Des ordinateurs branchés entre eux 197
26.2 Protocoles de communication 199
26.3 Les réseaux locaux 203
26.4 Internet : des réseaux interconnectés 205
26.5 Des clients, des serveurs 209

27 Traces sur toute la ligne **213**
27.1 Sur l'ordinateur client 213
27.2 Sur la « box » : l'adresse matérielle de la carte réseau 215
27.3 Sur les routeurs : les en-têtes de paquets 217
27.4 Sur le serveur 217
27.5 Les traces qu'on laisse soi-même 219

28 Surveillance et contrôle des communications **221**
28.1 Qui veut récupérer les données ? 221
28.2 Journaux et rétention de données 224
28.3 Écoutes de masse 229
28.4 Attaques ciblées 231
28.5 En conclusion 238

29 Web 2.0 **239**
29.1 Des « applications Internet riches »… 239
29.2 … et des internautes bénévoles 240
29.3 Centralisation des données 240
29.4 Mainmise sur les programmes 241
29.5 De la centralisation à l'auto-hébergement décentralisé 242

30 Identités contextuelles **243**
30.1 Définitions 243
30.2 De l'identité contextuelle à l'identité civile 244
30.3 La compartimentation 246
30.4 Les médias sociaux : centralisation de fonctions et identité unique . . 247

31 Cacher le contenu des communications : la cryptographie asymétrique **249**
31.1 Limites du chiffrement symétrique 249
31.2 Une solution : la cryptographie asymétrique 249
31.3 Chiffrement de bout en bout 251
31.4 Signature numérique 252
31.5 Vérifier l'authenticité de la clé publique 253
31.6 Confidentialité persistante 258
31.7 Résumé et limites 258

32 Tor ou le routage en oignon **261**
32.1 La problématique : cacher l'origine et la destination 261
32.2 Une solution : Tor 261
32.3 Les services onion 266
32.4 Participer au réseau Tor 266
32.5 Quelques limites de Tor 267

V Choisir des réponses adaptées 273

Introduction 275

33 Cas d'usage : consulter des sites web 277
33.1 Contexte . . . 277
33.2 Évaluer les risques . . . 277
33.3 Définir une politique de sécurité . . . 278
33.4 Choisir parmi les outils disponibles . . . 279
33.5 Naviguer sur des sites web avec le Navigateur Tor . . . 281
33.6 Naviguer sur des sites web avec Tails . . . 282

34 Cas d'usage : publier un document 285
34.1 Contexte . . . 285
34.2 Évaluer les risques . . . 285
34.3 Définir une politique de sécurité . . . 285

35 Cas d'usage : échanger des messages 289
35.1 Contexte . . . 289
35.2 Évaluer les risques . . . 289
35.3 Deux problématiques . . . 290
35.4 Webmail ou client mail ? . . . 290
35.5 Webmail . . . 291
35.6 Client mail . . . 292
35.7 Échanger des emails en cachant son identité . . . 293
35.8 Échanger des emails confidentiels . . . 295

36 Cas d'usage : dialoguer 299
36.1 Contexte . . . 299
36.2 Évaluer les risques . . . 299
36.3 Définir une politique de sécurité . . . 299
36.4 Les limites . . . 301

37 Cas d'usage : partager des documents sensibles 303
37.1 Contexte . . . 303
37.2 Évaluer les risques . . . 303
37.3 Protéger la source . . . 304
37.4 Protéger les destinataires . . . 305
37.5 Protéger les fichiers confidentiels . . . 305

VI Outils 309

Introduction 311

38 Installer et configurer le Navigateur Tor 313
38.1 Installer le Navigateur Tor . . . 314
38.2 Mise à jour du Navigateur Tor . . . 314

39 Naviguer sur le web avec Tor 315
39.1 Accéder au dossier Téléchargement du Navigateur Tor . . . 315
39.2 Limites concernant la géolocalisation . . . 316

40 Choisir un hébergement web 319
40.1 Quelques critères de choix . . . 319
40.2 Type de contenu . . . 320
40.3 En pratique . . . 322

41 Vérifier un certificat électronique **323**
41.1 Vérifier un certificat ou une autorité de certification 323
41.2 Trouver l'empreinte d'un certificat déjà installé 326

42 Utiliser un clavier visuel dans Tails **327**

43 Configurer et utiliser le client mail Thunderbird **329**
43.1 Lancer Thunderbird 329
43.2 Configurer le routage en oignon pour Thunderbird 329
43.3 Définir un mot de passe principal dans Thunderbird 330
43.4 Configurer un compte mail 330
43.5 Configuration avancée de Thunderbird 331

44 Utiliser le chiffrement OpenPGP dans Thunderbird **333**
44.1 Créer une paire de clés 333
44.2 Exporter et partager notre clé publique 336
44.3 Importer, vérifier et exporter des clés publiques 337
44.4 Gestion de sa paire de clé : la prolonger, en changer, la révoquer . . . 340
44.5 Chiffrer et/ou signer ses emails dans Thunderbird 342

45 Utiliser le chiffrement OpenPGP dans le bureau **343**
45.1 Importer une clé dans le trousseau du bureau 343
45.2 Signer une clé 344
45.3 Vérifier une signature numérique 345
45.4 Signer des données 346
45.5 Chiffrer des données 347
45.6 Déchiffrer des fichiers 348

46 Utiliser la messagerie instantanée avec OTR **351**
46.1 Installer le client de messagerie instantanée Pidgin 351
46.2 Lancer Pidgin 351
46.3 Configurer un compte de messagerie 352
46.4 Créer un compte de messagerie instantanée XMPP 352
46.5 Chiffrer la connexion au serveur 352
46.6 Activer le plugin OTR (*Off-the-Record*) 352
46.7 Mettre en place une conversation privée 353

47 Gérer des mots de passe **355**
47.1 Choisir une bonne phrase de passe 355
47.2 Utiliser un gestionnaire de mots de passe 355

48 Utiliser OnionShare **359**
48.1 Utiliser OnionShare dans Tails 359
48.2 Utiliser OnionShare dans Debian 359

Qui parle ? **361**

Index **363**

Crédits **367**

Préface à cette édition

Depuis la parution de la seconde édition papier du *guide* en 2017, de nouvelles informations à propos des technologies d'espionnage numériques, des outils que nous recommandons ou des lois que nous subissons ont vu le jour.

*
* *

Commençons par une virée dans le côté obscur des nouveautés numériques.

« Les données déterminent tout ce que nous faisons » [1] : voici le slogan cynique de Cambridge Analytica. Cette société a été au cœur d'un scandale qui a fait connaître le pouvoir des grands groupes de l'Internet sur la société : elle a siphonné les données personnelles de dizaines de millions de comptes Facebook avec l'accord de la plateforme pour une prétendue « étude scientifique ». Elle a ensuite vendu ses services de manipulation psychologique ciblée qui ont servi à influencer la campagne présidentielle de 2015 au Nigeria [2], l'élection présidentielle états-unienne de 2016 et le vote du Brexit [3]. Le scandale a été révélé dans les médias en 2018 grâce aux révélations d'un ancien salarié.

Avec le COVID-19 des nouvelles étapes ont été franchies quant aux abus du numérique. « Dans l'ère du COVID-19, la connectivité n'est pas une commodité, mais une nécessité. Quasiment toutes les activités humaines — commerce, éducation, santé, politique, socialisation — semblent s'être déplacées en ligne. [...] États et acteurs non-étatiques dans tous les pays exploitent maintenant les opportunités créées par la pandémie pour façonner de nouveaux récits en ligne, censurer les discours critiques et construire de nouveaux systèmes technologiques de contrôle social » [4]. Tel est le constat de l'organisation de défense des libertés numériques Freedom House.

Ainsi, le passe sanitaire français est un code-barre en deux dimensions, signé numériquement, qui contient le nom et le statut sanitaire de la personne, mais aussi des informations sur le vaccin reçu et les dates des dernières injections. Non seulement ces informations sont lisibles en clair, mais elles permettent « d'inférer des informations de santé encore plus privées sur certains citoyens » [5]. Au-delà de ces critiques sur la

1. « Data drives all we do » en anglais, cité par Le Monde (Le Monde, 2018, *Ce qu'il faut savoir sur Cambridge Analytica, la société au cœur du scandale Facebook* [https://www.lemonde.fr/pixels/article/2018/03/22/ce-qu-il-faut-savoir-sur-cambridge-analytica-la-societe-au-c-ur-du-scandale-facebook_5274804_4408996.html]).
2. Wikipédia, 2022, *Christopher Wylie* [https://fr.wikipedia.org/wiki/Christopher_Wylie].
3. Wikipédia, 2021, *Scandale Facebook-Cambridge Analytica* [https://fr.wikipedia.org/wiki/Scandale_Facebook-Cambridge_Analytica].
4. Adrian Shahbaz et Allie Funk, 2020, *The Pandemic's Digital Shadow*, dans Freedom House, 2020, *Freedom of the Net 2020* [https://freedomhouse.org/sites/default/files/2020-10/10122020_FOTN2020_Complete_Report_FINAL.pdf] (en anglais), traduit par nos soins.
5. Florian Maury, Piotr Chmielnicki, 2021, *Pass sanitaire et vie privée : quels sont les risques ?* [https://www.broken-by-design.fr/posts/pass-sanitaire/].

façon dont le passe sanitaire fonctionne, son adoption massive habitue la population à se soumettre à un contrôle généralisé via des outils numériques [6].

Célia Izoard dénonce « sous le masque du Covid, la numérisation intégrale de la société » [7], qui « se poursuit, brutalisant quotidiennement les dépassés et les réfractaires » [8]. Pour elle, la question à laquelle répondent les politiques de santé est trop souvent « comment la France peut-elle utiliser la pandémie pour conforter son leadership technologique et économique sur la scène internationale ? » Dans un rapport du sénat français, on peut ainsi lire « les perspectives ouvertes par le recours aux technologies numériques sont immenses, et la crise du Covid-19 n'a donné qu'un avant-goût des multiples cas d'usage possibles. [...] Il serait irresponsable de ne pas se saisir de telles possibilités. » [9]

Les frontières de l'Union Européenne donnent un aperçu de ce que pourraient être ces « possibilités à saisir ». Avec le programme E-Borders, « les espaces numériques qui permettent de collecter des données sur les migrants sont au cœur de la stratégie des partenaires européens » [10]. Frontex, l'agence européenne de garde-frontières et de garde-côtes, se targue d'utiliser toujours plus les technologies « en constante évolution » [11] : automatisation des contrôles, robotisation, intelligence artificielle [12].

Ces frontières qui servent de laboratoire font écho à l'utilisation croissante dans des enquêtes judiciaires de moyens de surveillance numériques, encore il y a peu, réservés à l'antiterrorisme : utilisation de keyloggers, déchiffrement de disque durs, *etc.* Ainsi, dans une enquête visant le mouvement antinucléaire autour de Bure, des dizaines d'ordinateurs et de téléphones ont été expertisés [13]. Selon une magistrate « le caractère exceptionnel des mesures d'investigation, avec des technologies très avancées et des mises sur écoute, découle de toutes les impasses de l'association de malfaiteurs. » [14]

page 35

Dans la même logique, les états semblent monter des attaques utilisant des failles de sécurité encore inconnues (dites « vulnérabilité *zero-day* ») de plus en plus massivement. Elles ont été utilisées par la Chine contre les Ouïghours en 2018, ce qui fait dire à une organisation de défense des libertés numériques états-unienne qu'« il est très probable que ça ne soit pas la dernière fois que l'on voit un acteur étatique cibler un groupe ethnique ou un groupe activiste en masse grâce à des vulnérabilités

page 33

6. La Quadrature du Net, 2021, *Passe sanitaire : quelle surveillance redouter ?* [https://www.laquadrature.net/2021/08/19/passe-sanitaire-quelle-surveillance-redouter/].

7. Celia Izoard, 2021, *Sous le masque du Covid, la numérisation intégrale de la société*, Reporterre [https://reporterre.net/Sous-le-masque-du-Covid-la-numerisation-integrale-de-la-societe].

8. Celia Izoard, 2021, *La numérisation du quotidien, une violence inouïe et ordinaire*, Reporterre [https://reporterre.net/La-numerisation-du-quotidien-une-violence-inouie-et-ordinaire].

9. Véronique Guillotin, Christine Lavarde, René-Paul Savary, 2021, *Rapport d'information fait au nom de la délégation sénatoriale à la prospective sur les crises sanitaires et outils numériques : répondre avec efficacité pour retrouver nos libertés*, Sénat français [https://www.senat.fr/rap/r20-673/r20-6731.pdf], p. 51.

10. Catherine Puzzo, 2018, *Frontières multiples et nouveaux agents du contrôle migratoire au Royaume Uni*, Sciences & Actions Sociales n° 9, p 20 [https://www.cairn.info/revue-sciences-et-actions-sociales-2018-1-page-18.htm#pa20].

11. Frontex, 2017, *Research and Development in border management* [https://frontex.europa.eu/media-centre/multimedia/videos/research-and-development-in-border-management-GIoaIn](en anglais).

12. Piotr Szostak, 2021, *Avec les drones et algorithmes, l'Europe construit un mur virtuel contre les migrants*, Gazeta Wyborcza traduit par Courrier International [https://www.courrierinternational.com/article/interview-avec-les-drones-et-algorithmes-leurope-construit-un-mur-virtuel-contre-les].

13. Marie Barbier, Jade Lindgaard, 2020, *L'État a dépensé un million d'euros contre les antinucléaires de Bure*, Reporterre [https://reporterre.net/2-3-L-Etat-a-depense-un-million-d-euros-contre-les-antinucleaires-de-Bure].

14. Laurence Blisson, magistrate et ancienne secrétaire générale du Syndicat de la magistrature, cité par Marie Barbien et Jade Lindgaard (*op. cit.*)

zero-day »[15]. Des sociétés comme NSO Group[16] ou Cellebrite[17] vendent aux états des logiciels espions qui incluent de tels outils.

Suite à toutes ces révélations dans les médias, la protection de l'intimité numérique est plus que jamais d'actualité. À tel point que des entreprises se saisissent de la question pour proposer des services « sécurisés » avec les limites qu'on leur connaît : la volonté de faire du profit les pousse à prétendre donner des garanties qu'elles ne sont pas capables de tenir. En 2021, le fournisseur d'emails chiffrés Protonmail a ainsi fourni aux autorités françaises des informations sur des activistes de Youth for Climate qu'elle prétendait ne pas enregister[18]. Protonmail a affirmé ensuite n'avoir aucune possibilité de refuser une telle demande légale et a modifié son site qui prétendait le contraire[19]. En 2021, Proton a répondu à 4 920 demandes légales (sur 6 243 demandes reçues)[20].

*
* *

Sur le plan légal au niveau européen, plusieurs textes sur le droit qui s'applique aux données personnelles ont pris effet en mai 2018 : un règlement qui fixe le cadre général de la protection des données (RGPD)[21] ainsi qu'une directive applicable uniquement aux fichiers de la sphère pénale (directive Police-Justice)[22]. Ils sont censés protéger les données personnelles en régulant la façon dont elles peuvent être traitées[23] par les administrations publiques et les organisations. Le RGPD impose aussi que les données personnelles soient stockées et traitées de manière sécurisée. Dans les faits, le règlement est faiblement mis en œuvre par les organisations car les manquements sont très peu contrôlés[24]. La directive qui s'applique aux traitements policiers et judiciaires, elle, facilite les transferts de données entre les forces de l'ordre au niveau européen et au-delà[25].

La bataille juridique autour de la rétention des données au niveau européen illustre bien les limites de ces règlements. La Cour de Justice de l'Union Européenne (CJUE) a invalidé deux fois la directive européenne[26][27] de 2006 pour finalement, à la de-

15. Cooper Quintin and Mona Wang, 2019, *Watering Holes and Million Dollar Dissidents : the Changing Economics of Digital Surveillance*, Electronic Frontier Foundation [https://www.eff.org/deeplinks/2019/09/watering-holes-and-million-dollar-dissidents-changing-economics-digital], traduit par nos soins.

16. Le Monde, 2021, *Apple répare une faille informatique liée au logiciel d'espionnage* Pegasus** [https://www.lemonde.fr/pixels/article/2021/09/14/apple-repare-une-faille-informatique-liee-au-logiciel-d-espionnage-pegasus_6094541_4408996.html].

17. Privacy International, 2012, *Surveillance Company Cellebrite Finds a New Exploit : Spying on Asylum Seekers* [https://privacyinternational.org/fr/node/2776].

18. Gaspard d'Allens, 2021, *Réputé sûr, Protonmail a livré à la police des informations sur des militants climat*, Reporterre [https://reporterre.net/Repute-sur-Protonmail-a-livre-a-la-police-des-informations-sur-des-militants-climat].

19. Emma Confrere, 2021, *Émoi après que la messagerie sécurisée ProtonMail a collaboré à une enquête judiciaire*, Le Figaro [https://web.archive.org/web/20210916174658/https://www.lefigaro.fr/secteur/high-tech/emoi-apres-que-la-messagerie-securisee-protonmail-a-collabore-a-une-enquete-judiciaire-20210907].

20. Proton, 2022, *Transparency Report* [https://proton.me/legal/transparency] (en anglais).

21. Journal officiel de l'Union européenne, 2016, *Règlement (UE) n° 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE* [https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016R0679].

22. Journal officiel de l'Union Européenne, 2016, *Directive n° 2016/680 du 27 avril 2016* [https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32016L0680], dite « directive Police-Justice ».

23. Le « traitement » comprend tout ce qui est lié à la collecte, l'agrégation, l'exploitation ou le partage de données.

24. La Quadrature du Net, 2021, *Les GAFAM échappent au RGPD, la CNIL complice* [https://www.laquadrature.net/2021/05/25/les-gafam-echappent-au-rgpd-avec-la-complicite-de-la-cnil/].

25. La Quadrature du Net, 2016, *Synthèse de la directive sur les données personnelles* [https://wiki.laquadrature.net/Synth%C3%A8se_de_la_directive_sur_les_donn%C3%A9es_personnelles#Transferts_et_.C3.A9changes_de_donn.C3.A9es_personnelles].

26. Cour de Justice de l'Union Européenne, 2014, *La Cour de justice déclare la directive sur la conservation des données invalide*, Communiqué de presse n° 54/14 [https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054fr.pdf] sur l'arrêt « Digital Rights ».

27. Cour de justice de l'Union Européenne, 2016, *Les États membres ne peuvent pas imposer une obligation générale de conservation de données aux fournisseurs de services de communications*

page 29

mande de la France[28], revenir partiellement sur sa position[29]. La France en a profité pour maintenir la conservation systématique des journaux de connexion au titre de la sécurité nationale ou de la recherche des autrices d'infractions pénales[30] alors que la Belgique, au contraire, a confirmé renoncer, pour l'essentiel, à la conservation généralisée et indifférenciée des données de connexion[31].

Les autres nouveaux textes réglementaires applicables en France sont trop nombreux pour tous être listés et développés ici[32]. Et, comme ce n'est pas l'objet premier de l'ouvrage, nous nous contenterons de citer deux exemples. Le pouvoir de censure des autorités est étendu avec celui de faire retirer des contenus web pour « contenu terroriste » en moins d'une heure[33]. Ou encore l'énième tour de passe-passe qui a permis d'annoncer la fin de l'état d'urgence tout en normalisant dans le droit commun certaines de ses dispositions exorbitantes[34], « une prolongation indéfinie de l'état d'urgence »[35].

Encore une fois, malgré la propagation d'un sentiment d'impuissance, ces différentes révélations sur l'état de la surveillance numérique rendent d'autant plus nécessaire de se donner les moyens de la comprendre et d'adapter ses pratiques en conséquence.

*
* *

Depuis la dernière édition du *guide*, des évolutions techniques ont aussi amené à mettre à jour plusieurs passages : la généralisation des disques SSD nécessite de repenser la suppression de données ; les technologies de processeurs ont évolué[36]. Du côté des animations web, la technologie *flash* qui posait de nombreux problèmes d'intimité a été abandonnée au profit du HTML5 et de diverses technologies associées… qui posent de nouveaux problèmes.

Au sujet des attaques, les mises à jour concernent les microprogrammes (par exemple le Management Engine d'Intel) et l'exfiltration de données qui utilisent des failles dans les services web.

électroniques, Communiqué de presse n° 145/16 [https://curia.europa.eu/jcms/jcms/p1_268807/fr/] sur l'affaire « Tele2 ».

28. Conseil d'État français, 2018, *Lecture du 26 juillet 2018* [https://www.conseil-etat.fr/fr/arianeweb/CE/decision/2018-07-26/394922].

29. Cour de Justice de l'Union Européenne, 2020, *La Cour de justice confirme que le droit de l'Union s'oppose à une réglementation nationale imposant à un fournisseur de services de communications électroniques, à des fins de lutte contre les infractions en général ou de sauvegarde de la sécurité nationale, la transmission ou la conservation généralisée et indifférenciée de données relatives au trafic et à la localisation*, Communiqué de presse n° 123/20 [https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-10/cp200123fr.pdf] sur les affaires Privacy International, La Quadrature du Net, French Data Network et Ordre des barreaux francophones et germanophone.

30. Conseil d'État français, 2021, *Décision du 21 avril 2021* [https://www.conseil-etat.fr/content/download/159464/file/393099.pdf].

31. Cour Constitutionnelle belge, 2021, *Arrêt n° 57/2021 du 22 avril 2021* [https://www.const-court.be/public/f/2021/2021-057f.pdf].

32. Liste non exhaustive : loi n° 2019-222 du 23 mars 2019 de programmation 2018-2022 et de réforme pour la justice, loi n° 2019-1479 du 28 décembre 2019 de finances pour 2020, loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur Internet, ordonnance n° 2020-1733 du 16 décembre 2020 portant partie législative du code de l'entrée et du séjour des étrangers et du droit d'asile, loi n° 2021-646 du 25 mai 2021 pour une sécurité globale préservant les libertés, loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République, loi n° 2021-998 du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement…

33. Le gouvernement s'est battu bec et ongles pour l'obtenir. La Quadrature du Net, 7 mai 2021, *Règlement de censure terroriste adopté : résumons* [https://www.laquadrature.net/2021/05/07/reglement-de-censure-terroriste-adopte-resumons/].

34. Developpez.com, 2017, *France : les députés approuvent la saisie de matériel informatique et la copie de données d'un suspect* [https://www.developpez.com/actu/162736/France-les-deputes-approuvent-la-saisie-de-materiel-informatique-et-la-copie-de-donnees-d-un-suspect-dans-le-cadre-de-la-lutte-contre-le-terrorisme/].

35. Commission nationale consultative des droits de l'Homme, 6 juill. 2017, *avis sur le projet de loi renforçant la sécurité intérieure et la lutte contre le terrorisme* [https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000036039262].

36. Notamment avec la disparition des processeurs 32 bits.

Les explications sur Tor ont été largement revues car Tor ne prétend plus fournir d'anonymat, mais plutôt de la confidentialité. Les recommandations pour le choix de phrases de passe et l'utilisation de mots de passe ont aussi été revues en prenant en compte les nouvelles recherches à ce sujet.

Du côté des outils, deux nouvelles versions du système d'exploitation Debian GNU/-Linux sont sorties, ainsi que des nouvelles versions du système *live* Tails. Cette actualisation du *guide* est basée sur Debian 11 « Bullseye », qui a apporté de nombreux changements tant au niveau graphique que dans les logiciels proposés. Les outils ont donc été revus pour que les recettes fonctionnent sur ces nouveaux systèmes. Cela a également amené à des changements, notamment la refonte de l'utilisation du chiffrement OpenPGP dans Thunderbird et de nouvelles instructions pour utiliser le Navigateur Tor.

Les *smartphones* sont de plus en plus ciblés dans les enquêtes policières comme celle de Bure[37] et beaucoup de dispositifs exploitant les vulnérabilités *zero-day* visent particulièrement les *smartphones*. Pour autant, la réduction des risques pour l'usage des téléphones ne sera pas abordée dans ce guide. Un travail complet serait nécessaire, pour lequel les personnes qui mettent à jour ce *guide* n'ont ni le temps, ni l'expertise requise. Le fonctionnement même de la téléphonie mobile pose des questions d'intimité difficiles à résoudre[38].

Il faudra donc prendre en compte ces nouveautés dans notre approche du monde numérique et de nos politiques de sécurité.

*
* *

Au delà des évolutions techniques, une nouvelle dynamique d'écriture autour du *guide* a amené des évolutions plus générales.

Une relecture complète à été effectuée, ce qui a permis de nombreuses reformulations et la mise à jour d'exemples. Une nouvelle partie sur la réduction des risques appliquée aux outils numériques est venue se glisser dans le choix des réponses adaptées à chaque situation. Le cas d'usage *Travailler sur un document sensible* a été refondu et le cas d'usage *Publier un document* inclut maintenant la protection des personnes qui vont le consulter.

La question du genre dans les formulations du *guide* existe depuis ses débuts. Pour cette édition, un travail de fond visant à utiliser l'écriture épicène a été, au maximum, effectué. Mais la langue française est si discriminante que trouver des formulations non-genrées n'est pas toujours possible. Pour de tels cas, nous avions alors décidé d'utiliser le féminin, choisissant d'aller à l'encontre des règles habituelles spécifiant l'usage du masculin. Cependant, alors que nous écrivons cette préface et souhaitons justifier nos choix, nous réalisons que celui-ci ne permet pas aux personnes transgenres ou non-binaires de se sentir incluses, y compris au sein même de l'équipe du *guide*. À quelques mois de la sortie de l'ouvrage, nous ne pouvons malheureusement pas considérer recommencer ce travail. Nous attendrons donc l'édition suivante, si elle a lieu, pour trouver une solution inclusive.

*
* *

Grâce à cette révision, nous espérons que les pages suivantes restent d'une compagnie avisée dans la traversée de la jungle numérique… du moins, jusqu'à la suivante.

37. Marie Barbier, Jade Lindgaard, 2020, *La justice a massivement surveillé les militants antinucléaires de Bure*, Reporterre [https://reporterre.net/1-3-La-justice-a-massivement-surveille-les-militants-antinucleaires-de-Bure].

38. Surveillance Self-Defense, 2018, *Le Problème avec les Téléphones Portables* [https://ssd.eff.org/fr/module/le-probl%C3%A8me-avec-les-t%C3%A9l%C3%A9phones-portables].


BLEEDING
BLOODY
MURDER

Pourquoi ce guide ?

Les revers de la mémoire numérique

De nos jours, les ordinateurs, Internet et le téléphone portable tendent à prendre de plus en plus de place dans nos vies. Le numérique semble souvent très pratique : c'est rapide, on peut parler avec plein de gens très loin, on peut avoir toute son histoire en photos, on peut écrire facilement des textes bien mis en page… mais ça n'a pas que des avantages ; ou en tout cas, ça n'en a pas seulement pour nous, mais aussi pour d'autres personnes qu'on n'a pas forcément envie d'aider.

Il est en effet bien plus facile d'écouter discrètement des conversations par le biais des téléphones portables que dans une rue bruyante, ou de trouver les informations que l'on veut sur un disque dur plutôt que dans une étagère débordante de papiers.

De plus, énormément de nos informations personnelles finissent par se retrouver publiées quelque part, que ce soit par nous-mêmes ou par d'autres personnes, que ce soit parce qu'on nous y incite — c'est un peu le fond de commerce du *web 2.0* —, parce que les technologies laissent des traces, ou simplement parce qu'on ne fait pas attention.

Rien à cacher ?

« *Mais faut pas être parano : je n'ai rien à cacher !* » pourrait-on répondre au constat précédent…

Deux exemples tout simples tendent pourtant à montrer le contraire : personne ne souhaite voir ses codes secrets de carte bleue ou de compte *eBay* tomber entre n'importe quelles mains. Et personne non plus n'aimerait se faire cambrioler parce que son adresse a été publiée sur Internet malgré soi et son absence confirmée sur les médias sociaux.

Mais au-delà de ces bêtes questions de défense de la propriété privée, la confidentialité des données devrait être *en soi* un enjeu.

Tout d'abord, parce que ce n'est pas nous qui jugeons de ce qu'il est autorisé ou non de faire avec un ordinateur. Des personnes sont arrêtées sur la base des traces laissées par l'utilisation d'outils numériques dans le cadre d'activités qui ne plaisaient pas à un gouvernement, pas forcément le leur d'ailleurs — et pas seulement en Chine ou en Iran.

Beaucoup de gens, que ce soient les gouvernants, les employeurs, les publicitaires ou les flics [39], ont intérêt à obtenir l'accès à nos données. La place croissante que prend

39. On utilise ici le terme « flics » tel qu'il est défini dans l'introduction du *Guide d'autodéfense juridique : Face à la police / Face à la justice* [https://infokiosques.net/spip.php?article538] : « Dans ce guide, le mot "flic" désigne indifféremment tout type de gendarme ou de policier, quel que soit son grade ou sa qualité […] »

l'information dans l'économie et la politique mondiale ne peut que les encourager. On sait d'ailleurs déjà qu'ils ne se gènent pas pour faire des recoupements entre les individus. Or, que savons-nous des pratiques légales et illégales de nos proches ?

De plus, comment savoir si ce qui est autorisé aujourd'hui le sera demain ? Les gouvernements changent, les lois et les situations aussi. Et cela peut aller extrêmement vite, comme de nombreuses personnes ont pu le constater avec l'application de l'état d'urgence en France pendant deux ans en 2015 [40] avant d'en passer certaines mesures dans le droit commun [41]. Si on n'a pas à cacher aujourd'hui, par exemple, la fréquentation régulière d'un site web militant, comment savoir ce qu'il en sera si celui-ci se trouve lié à un processus de répression ? Des traces *auront été laissées* sur l'ordinateur… et pourraient être employées comme éléments à charge.

Mettre en place des pratiques de protection des données lorsqu'on a le sentiment de ne pas directement en avoir besoin permet aussi de les rendre plus « normales », plus acceptables et moins suspectes. Les personnes qui n'ont pas d'autre possibilité pour survivre que de cacher leurs activités numériques nous en seront reconnaissantes, sans aucun doute.

De manière générale, nous bridons nos actions dès que nous savons que d'autres peuvent nous écouter, nous regarder ou nous lire. Chanterions-nous sous la douche si l'on savait que des micros y sont installés ? Apprendrions-nous à danser si des caméras étaient pointées sur nous ? Écririons-nous une lettre intime aussi librement si une personne lisait par dessus notre épaule ? Avoir des choses à cacher n'est pas seulement une question de légalité, mais aussi d'intimité.

Ainsi, les sociétés de contrôle voient derrière chacune de nous une menace potentielle qu'il faut surveiller. Se cacher est donc un enjeu *politique* et de fait *collectif*, ne serait-ce que pour mettre des bâtons dans les roues aux personnes qui nous voudraient exposées et identifiables en permanence.

Tout ça peut amener à se dire que nous n'avons pas envie d'être contrôlables par quelque « Big Brother » que ce soit. Qu'il existe déjà ou que l'on anticipe son émergence, le mieux est sans doute de faire en sorte qu'il ne puisse pas utiliser, contre nous, tous ces merveilleux outils que nous offrent — ou que lui offrent — les technologies modernes.

Alors, *ayons aussi quelque chose à cacher, ne serait-ce que pour brouiller les pistes !*

Comprendre pour pouvoir choisir

Ce guide se veut une tentative de décrire dans des termes compréhensibles l'intimité (ou plutôt son absence) dans le monde numérique ; une mise au point sur certaines idées reçues en vue de mieux comprendre à quoi on s'expose dans tel ou tel usage de tel ou tel outil.

Afin, aussi, de pouvoir faire le tri parmi les « solutions », qui peuvent s'avérer dangereuses si l'on ne connaît pas leurs limites.

À la lecture de ces quelques pages, on pourra avoir le sentiment que rien n'est vraiment sûr avec un ordinateur ; eh bien, c'est vrai. Et c'est faux. Il y a des outils et des usages appropriés. Et souvent la question n'est finalement pas tant « doit-on utiliser ou pas ces technologies ? », mais plutôt « quand et comment les utiliser (ou pas) ? »

---

40. Wikipédia, 2017, *État d'urgence en France* [https://fr.wikipedia.org/wiki/Etat_d%27urgence_en_France].

41. République Française, 2021, *Loi du 30 juillet 2021 relative à la prévention d'actes de terrorisme et au renseignement* [https://www.vie-publique.fr/loi/279661-loi-30-juillet-2021-prevention-terrorisme-et-renseignement].

Prendre le temps de comprendre

Les logiciels sont conçus pour être le plus accessible et le plus simple d'utilisation possible. De même, l'accélération des ordinateurs et des connexions à Internet rendent leur fonctionnement quasi instantané, presque imperceptible. Grâce à la généralisation des réseaux Wi-Fi, il n'est même plus nécessaire de brancher nos appareils à des câbles pour qu'ils puissent échanger des données.

Cette simplification des outils laisse croire que comprendre leurs fonctionnements serait superflu. Malheureusement, cela implique aussi d'accorder notre confiance et de déléguer de nombreuses décisions à des expertes que l'on croit sur parole. Si apprendre et comprendre demande du temps et de la patience, cela redonne aussi du pouvoir et de l'autonomie.

Comment lire ce guide ?

Ce guide est une tentative de rassembler ce que nous avons pu apprendre au cours de nos années de pratiques, d'erreurs, de réflexions et de discussions pour le partager.

Afin de rendre le tout plus digeste, nous avons divisé tout ce que nous souhaitions raconter en deux tomes. Le volet *hors ligne* étant un préalable incontournable pour pouvoir comprendre les enjeux liés au volet *en ligne*, ces deux tomes se retrouvent donc réunis dans un même livre.

Un tome « hors ligne »

Un premier tome, consacré à l'utilisation de l'ordinateur *hors ligne*, est sorti en 2010. Avant même de penser à connecter notre ordinateur, ce premier volet nous propose d'abord de regarder de plus près comment fonctionnent ces machines. On verra ainsi que les possibilités de contrôle et de surveillance *via* l'outil numérique sont innombrables.

Un tome « en ligne »

Comme son nom l'indique, ce second volet s'intéressera donc à l'utilisation des ordinateurs en ligne, c'est-à-dire connectés entre eux. Vaste programme…

Dans les pays riches du moins, l'utilisation d'Internet est entrée dans les mœurs. Consulter ses mails, télécharger des fichiers, obtenir des informations en ligne sont aujourd'hui pour beaucoup d'entre nous des gestes quotidiens. Chaque personne pourrait dire que, d'une certaine manière, elle *sait ce que c'est* qu'Internet. Admettons plutôt que tout le monde, ou presque, est capable de s'en servir pour quelques usages communs.

Notre propos dans ce second tome, pour autant, ne sera pas de définir dans les moindres détails ce qu'est Internet. Tout au plus fournira-t-on quelques éléments de compréhension suffisants pour permettre d'y naviguer — ambiguïté du terme, qui renvoie autant à la « navigation sur le web » qu'à la possibilité de s'orienter dans un espace complexe à l'aide d'outils adaptés.

Larguer les amarres

Nous voici donc de nouveau en route pour un voyage dans les eaux troubles du monde numérique. Notre traversée se fera pour chaque tome en trois parties. Une première s'attachera à expliquer le contexte, les notions de base, permettant ainsi une compréhension générale. Une seconde partie traitera quant à elle de cas d'usage typiques. Enfin une troisième et dernière partie décrira précisément les outils nécessaires à la mise en œuvre de politiques de sécurité abordés dans la seconde partie ainsi que leurs usages.

Des encadrés donneront des précisions qui s'écartent du fil du texte :



PRÉCISION

Ce type d'encadré donne des exemples ou des détails supplémentaires dont la lecture est facultative.



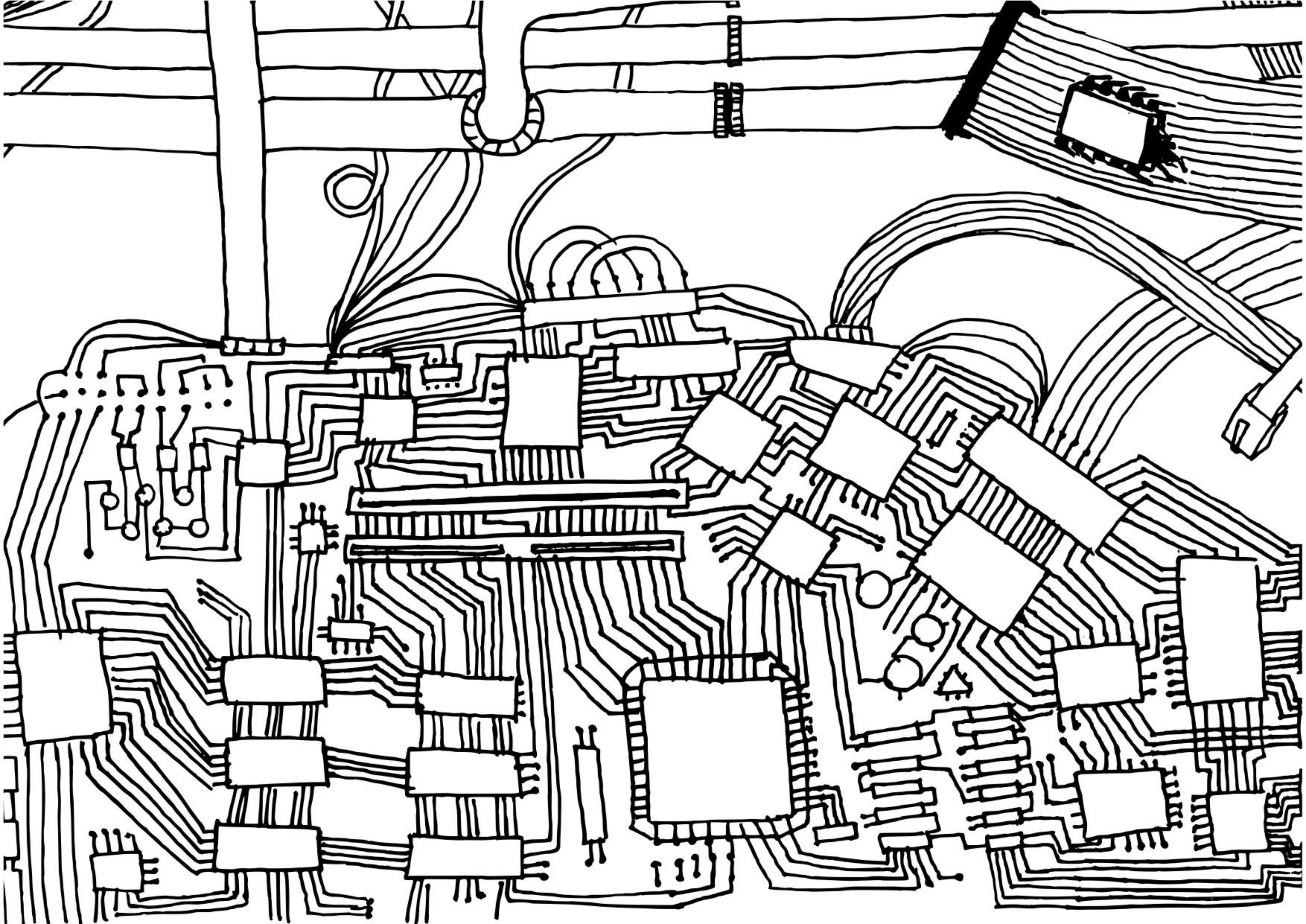
POUR ALLER PLUS LOIN…

Ici, ce seront des directions pour aller plus loin pour les personnes qui se sentent de bidouiller en hors-piste.

*
* *

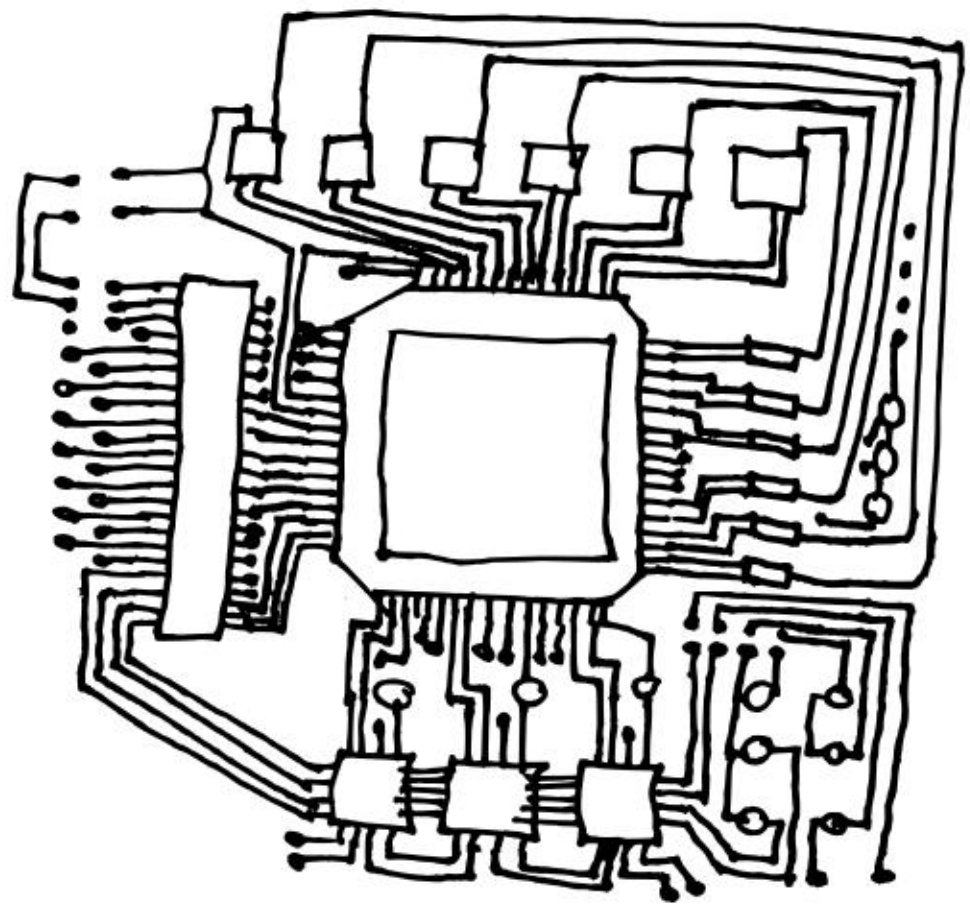
Non seulement les technologies évoluent très vite, mais nous avons pu commettre des erreurs ou écrire des contre-vérités dans ces pages. Nous tenterons donc de tenir ces notes à jour à l'adresse : https://guide.boum.org/.

Adapter ses pratiques à l'usage qu'on a du monde numérique est donc nécessaire dès lors qu'on veut, ou qu'on doit, apporter une certaine attention à son impact. Mais la traversée n'a que peu de sens en solitaire. Nous vous enjoignons donc à construire autour de vous votre radeau numérique, à sauter joyeusement à bord, sans oublier d'emmener ce guide et quelques fusées de détresse pour envoyer vos remarques et vos idées de *cas d'usages* à guide@boum.org.



Tome 1

Hors connexions



Première partie

Comprendre

Introduction

Devant la grande complexité des outils informatiques et numériques, la quantité d'informations à avaler pour tenter d'acquérir quelques pratiques d'autodéfense peut paraître énorme. Elle l'est sûrement pour qui chercherait à tout comprendre en même temps...

Ce premier tome se concentrera donc sur l'utilisation d'un ordinateur « hors connexion » — on pourrait aussi bien dire *préalablement à toute connexion*. Mais ce sont aussi des connaissances plus générales qui sont valables *que l'ordinateur soit connecté ou non* à un réseau. On met donc de côté, jusqu'au second tome, les menaces spécifiquement liées à l'usage d'Internet et des réseaux.

Pour ce morceau *hors connexion*, comme pour les autres, on prendra le temps de s'attarder sur des notions de base, leurs implications en termes de sécurité / confidentialité / intimité [1]. Après l'analyse de cas concrets d'utilisation, on pourra se pencher sur quelques recettes pratiques.

Une dernière précision avant de nous jeter à l'eau : *l'illusion de sécurité est bien pire que la conscience nette d'une faiblesse*. Aussi, prenons le temps de bien lire les premières parties avant de nous jeter sur nos claviers ou alors de jeter nos ordinateurs par les fenêtres.

1. On souhaite ici faire appel à une notion un peu floue : quelque chose qui tournerait autour de la possibilité de décider ce qu'on révèle, à qui on le révèle, ainsi que ce que l'on garde secret ; quelque chose qui inclurait aussi une certaine attention à déjouer les tentatives de percer ces secrets. Le terme employé en anglais pour nommer ce qu'on évoque ici est *privacy*. Aucun mot français ne nous semble adapté pour porter tout le sens que l'on aimerait mettre derrière cette notion. Ailleurs, on rencontrera souvent le terme « sécurité », mais l'usage qui en est couramment fait nous donne envie de l'éviter.

Chapitre 1

Quelques bases sur les ordinateurs

Commençons par le commencement.

Un *ordinateur*, ce n'est pas un chapeau de magicienne où on peut ranger des lapins et les ressortir quand on en a besoin, et qui permettrait en appuyant sur le bon bouton d'avoir une fenêtre ouverte sur l'autre bout du monde.

Un ordinateur est un ensemble de composants plus ou moins complexes, reliés entre eux par des connexions électriques, des câbles, et parfois des ondes radios. Tout ce *matériel* stocke, transforme et réplique des signaux pour manipuler l'information que l'on peut voir sur un bel écran avec plein de boutons sur lesquels cliquer.

Comprendre comment s'articulent ces principaux composants, comprendre les bases de ce qui fait fonctionner tout ça, c'est la première étape pour comprendre où sont les forces et les faiblesses de ces engins, à qui l'on confie beaucoup de nos données.

1.1 Des machines à traiter les données

Les ordinateurs sont des machines inventées pour pouvoir traiter des données. Ce qui veut dire qu'elles peuvent enregistrer, analyser et classer ces données en très grande quantité rapidement.

Dans le monde numérique, copier une donnée ne coûte que quelques microwatts, autant dire pas grand-chose. Nous devons donc considérer que *mettre une information sur un ordinateur* (et c'est encore plus vrai quand il est sur un réseau), *c'est accepter que cette information puisse nous échapper* sans même que l'on s'en rende compte.

Ce guide peut aider à réduire les risques, mais il faut malgré tout prendre acte de cette réalité.

1.2 Le matériel

Somme de composants reliés entre eux, notre ordinateur est donc d'abord une accumulation d'objets qu'on peut toucher, déplacer, bidouiller, casser.

L'ensemble *écran / clavier / tour* (ou unité centrale), ou l'ordinateur portable, est pratique quand on veut simplement brancher les fils aux bons endroits. Mais pour savoir ce qu'il advient de nos données, un examen plus fin est nécessaire.

On parle ici du contenu d'un *ordinateur* dit *personnel*, parfois appelé PC. Mais d'autres machines ont les mêmes composants et sont aussi des ordinateurs : téléphone portable, « box » de connexion à Internet, tablette, lecteur MP3, caisse enregistreuse, compteur communicant Linky ou Gazpar [1], ordinateur de bord de voiture, objets connectés en tout genre, *etc.*

1. Les compteurs communicants Linky et Gazpar sont les remplaçants des compteurs électriques et de gaz historiques - Wikipédia, 2021, *Compteur communicant* [https://fr.wikipedia.org/wiki/Compteur_communicant].

1.2.1 La carte mère



Une carte mère

Un ordinateur est surtout composé d'éléments électroniques. La *carte mère* est un gros circuit imprimé qui permet de relier la plupart de ces éléments à travers l'équivalent de fils électriques. Sur la carte mère viendront se brancher au minimum un processeur, une barrette de mémoire vive, un système de stockage (disque dur ou autre mémoire), un microprogramme pour démarrer l'ordinateur et d'autres cartes et périphériques selon les besoins.

Ici, on va faire un tour rapide de chacun de ces éléments afin d'avoir une petite idée de qui fait quoi, ce qui sera fort utile par la suite.

1.2.2 Le processeur



La puce d'un microprocesseur Intel Pentium 60 MHz dans son boîtier

Le processeur (aussi appelé CPU, pour *central processing unit* ou « unité centrale de traitement » en français) est le composant qui s'occupe du traitement des données.

Pour se représenter le travail d'un processeur, l'exemple le plus concret sur lequel se baser est la calculatrice. Sur une calculatrice, on entre des données (les nombres) et des opérations à faire dessus (addition, multiplication ou autre) avant d'examiner le résultat. Puis on se sert éventuellement de ce résultat comme base pour d'autres calculs.

Un processeur fonctionne exactement de la même manière. À partir de données (qui peuvent être une liste d'opérations à effectuer), il va exécuter à la chaîne les traitements demandés. Il ne fait que ça, mais il le fait vraiment très vite.

Mais si le processeur n'est qu'une simple calculatrice, comment peut-on alors effectuer des traitements sur des informations qui ne sont pas des nombres, comme du texte, des images, du son ou un déplacement de la souris ?

Tout simplement en transformant en nombre tout ce qui ne l'est pas, en utilisant un code défini auparavant. Pour du texte, ça peut par exemple être `A = 65`, `B = 66`, *etc.* Une fois ce code défini, on peut *numériser* notre information. Avec le code précédent, on peut ainsi transformer « GUIDE » en `71 85 73 68 69`.

Cette série de nombres permet de représenter les lettres qui composent notre mot. Mais le processus de numérisation fera toujours perdre de l'information. Pour cet exemple, on perd au passage la spécificité de l'écriture manuscrite alors que pourtant, une rature, des lettres hésitantes constituent tout autant de « l'information ». Passer des choses dans le tamis du monde numérique implique forcément d'en perdre des morceaux.

Au-delà des données, les opérations que le processeur doit effectuer (ses *instructions*) sont également codées sous forme de nombres. Un programme est donc une série d'instructions, manipulées comme n'importe quelles autres données.



Précision

À l'intérieur de l'ordinateur, tous ces nombres sont eux-mêmes représentés à l'aide d'états électriques : absence de courant ou présence de courant. Il y a donc deux possibilités, ces fameux `0` et `1` que l'on peut croiser un peu partout. C'est pourquoi on parle de langage binaire (*bi*-naire), dont l'unité de mesure est le *bit*[2]. Finalement, le traitement des données se fait à l'aide d'un bon paquet de fils et de plusieurs milliards de *transistors* (des interrupteurs, pas si différents de ceux pour allumer ou éteindre la lumière dans une cuisine).

Tous les processeurs ne fonctionnent pas de la même manière. Certains ont été conçus pour être plus efficaces pour certains types de calcul, d'autres pour consommer le moins d'énergie possible, *etc.* Par ailleurs, tous les processeurs ne disposent pas exactement des mêmes instructions. Il en existe de grandes familles, que l'on appelle des *architectures*. Cela a son importance car sur un processeur avec une architecture donnée on ne pourra, en général, faire fonctionner que des programmes prévus pour cette architecture.

La majorité des ordinateurs personnels fonctionnent avec l'architecture `x86-64`[3] (aussi appelée `x64`, `AMD64` ou `Intel 64`), tandis que beaucoup de téléphones ou autres mini-ordinateurs fonctionnent avec l'architecture `ARM`.

2. Pour en savoir plus, voir Wikipédia, 2014, *Bit* [https://fr.wikipedia.org/wiki/Bit].

3. Jusque dans les années 2010, une partie des ordinateurs personnels utilisaient une version plus ancienne de l'architecture `x86` dont les données manipulées étaient codées sur 32 bits, contre 64 bits pour la version `x86-64`. On parle ainsi de processeurs *32 bits* ou *64 bits*.

1.2.3 La mémoire vive

La mémoire vive (ou RAM, pour *Random Access Memory*) se présente souvent sous forme de *barrettes* et se branche directement sur la carte mère.



Différentes barrettes de mémoire vive

La mémoire vive sert à stocker tous les logiciels et documents ouverts lorsque l'ordinateur est allumé. C'est à cet endroit que le processeur va chercher les données à traiter et entreposer le résultat des opérations. Quasiment toutes les informations traitées par l'ordinateur passent donc par la mémoire vive sous une forme directement utilisable — et donc non chiffrée.

La mémoire vive est reliée au processeur, permettant ainsi d'y lire, d'y inscrire et d'y modifier des données très rapidement, suivant les besoins du processeur.

On l'appelle *mémoire vive* en opposition à la *mémoire morte* (disque dur, clé USB, disque SSD, *etc.*) : à la différence de ces composants, les données qu'elle contient deviennent illisibles après quelques minutes ou quelques heures (selon les modèles) lorsque la mémoire vive n'est plus alimentée en électricité.

1.2.4 Le disque dur ou le SSD

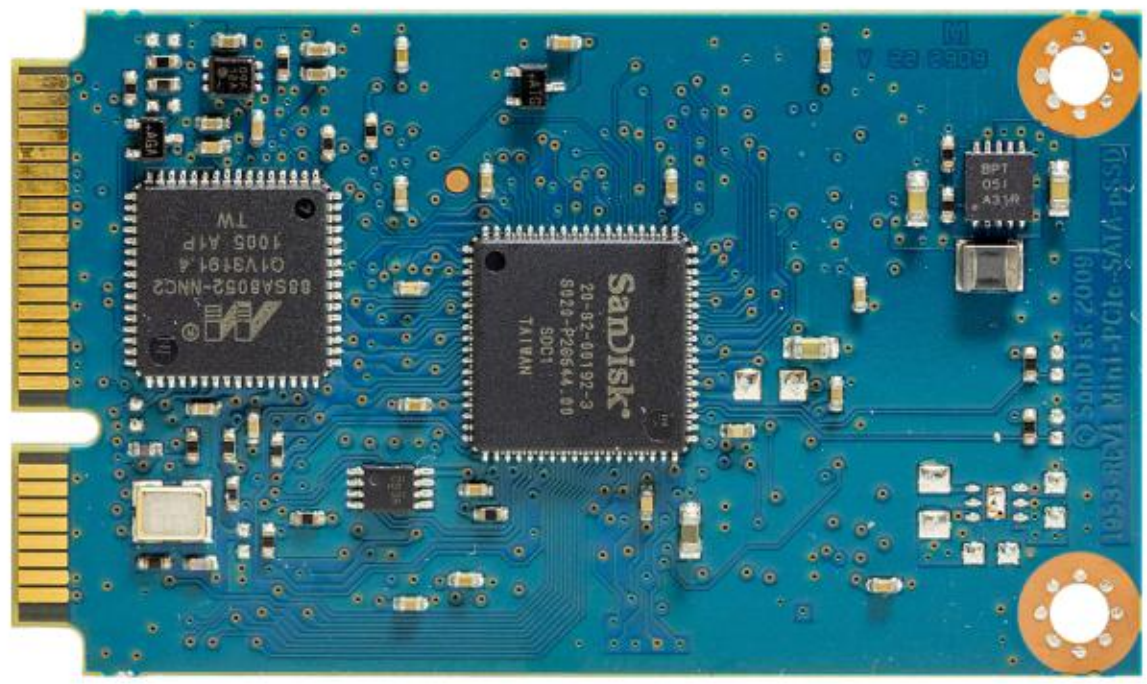


Un disque dur 3 pouces ½

Étant donné que la mémoire vive s'efface à partir du moment où elle n'a plus de courant, l'ordinateur a besoin d'un autre endroit où stocker données et programmes entre chaque allumage. C'est là qu'intervient la *mémoire persistante* ou *mémoire morte* : une mémoire où les informations écrites restent, même sans alimentation électrique.

Pour ce faire, on utilise un support de stockage tel qu'un *disque dur* ou un disque *SSD*.

L'appellation disque dur fait en général référence aux disques durs rotationnels, aussi appelés *disques durs magnétiques* ou *disques durs mécaniques*. Ces disques durs rotationnels se présentent souvent sous la forme d'une coque en métal dans laquelle se trouvent plusieurs disques qui tournent sans s'arrêter, à la manière d'une platine vinyle miniature. Sur ces disques se trouvent de minuscules morceaux de fer et au-dessus de chaque disque se trouvent des *têtes de lecture*. À l'aide de champs magnétiques, ces dernières détectent et modifient la position des morceaux de fer. C'est la position des morceaux de fer qui permet de coder les informations à stocker.



Un disque SSD interne

Du fait des mouvements mécaniques, les disques durs rotationnels sont lents. C'est pourquoi, ces dernières années, plus de la moitié des supports de stockage vendus étaient des disques SSD ou *Solid State Drive* (ou encore disques électroniques ou disques statiques à semi-conducteurs) et non des disques durs rotationnels [4]. Un disque SSD fonctionne avec une mémoire d'un autre type : la mémoire *flash*, celle-là même qui est présente dans les *clés USB* et les *cartes SD*. Dans un disque SSD, les données sont stockées grâce à plusieurs centaines d'interrupteurs miniatures. Cette mémoire entièrement électronique est environ 25 fois plus rapide qu'un disque dur rotationnel.

Les disques durs rotationnels ainsi que les disques SSD permettent de stocker *beaucoup plus d'informations* que la mémoire vive, mais sont beaucoup plus lents.

Les informations y sont stockées sous forme de *bits* dont plusieurs multiples existent [5], page 16 ce qui permet de quantifier simplement la capacité d'un disque dur, souvent en gigaoctets (Go), téraoctets (To), *etc.*

Les informations qui sont enregistrées sur un disque (dur ou SSD) sont, bien souvent, des documents, mais aussi des programmes avec toutes les données dont ils ont besoin pour fonctionner, comme des fichiers temporaires, des journaux système (*logs*), des page 29 fichiers de sauvegarde, des fichiers de configuration, *etc.*

Le disque utilisé conserve donc une mémoire quasi permanente et quasi exhaustive de toutes sortes de traces qui parlent de nous, de ce que nous faisons, avec qui et comment, dès qu'on utilise un ordinateur.

4. T4, 2021, *SSD Market Share* [https://www.t4.ai/industry/ssd-market-share] (en anglais).
5. Wikipédia, 2017, *Octet* [https://fr.wikipedia.org/wiki/Octet].

1.2.5 Les autres périphériques

Avec uniquement un processeur, de la mémoire vive et un support de stockage, on obtient déjà un ordinateur. Pas très causant, par contre. Donc on lui adjoint généralement d'autres *périphériques* comme un écran, un clavier, une souris, une carte réseau (avec ou sans fil), un lecteur de carte micro SD, *etc.*

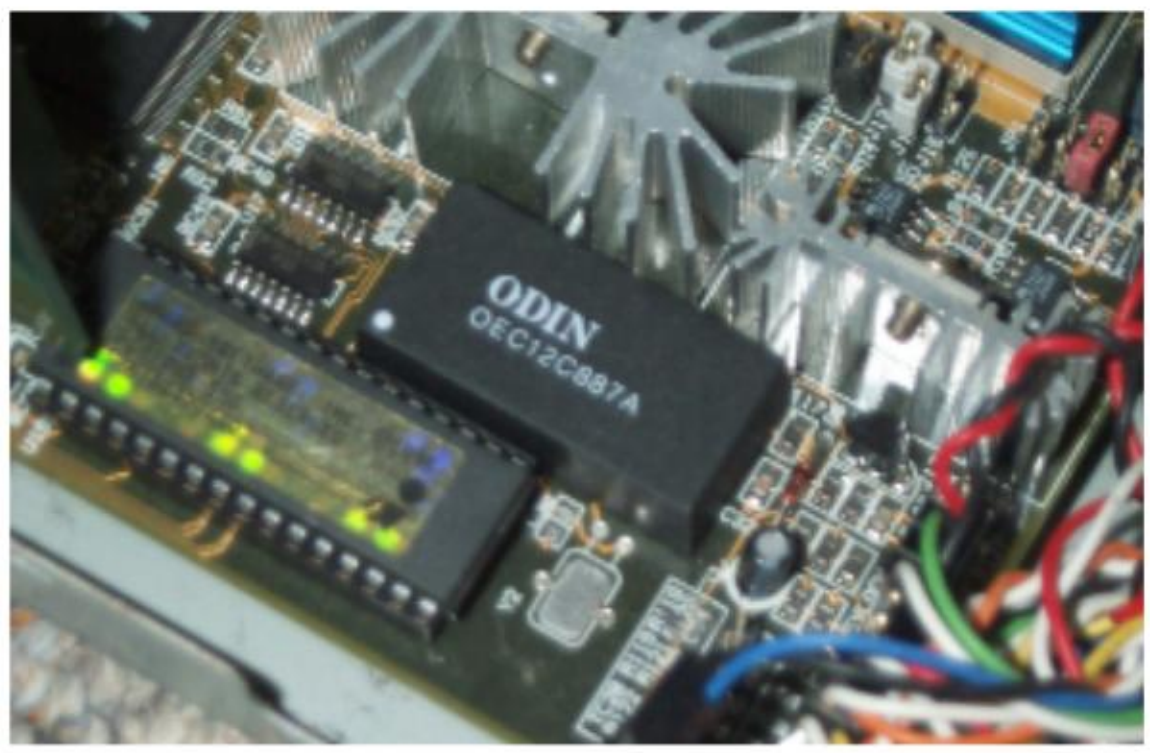
Beaucoup de ces périphériques sont branchés en USB (pour *Universal Serial Bus*), un standard qui permet de connecter imprimantes, claviers, souris, disques durs supplémentaires, adaptateurs réseau ou ce qu'on appelle couramment des « clés USB ».

La liaison entre le processeur et les différents périphériques USB est assurée par un ensemble de puces spécifique, appelé *chipset*. Le chipset est soudé sur la carte mère, voire intégré dans le même boîtier que le processeur.

La plupart des chipsets actuels intègrent des périphériques supplémentaires censés fournir des environnements sécurisés pour le système d'exploitation de l'ordinateur et l'exécution des programmes. On peut ainsi mentionner le Management Engine (ME, système de gestion en français) d'Intel ou le Platform Security Processor (PSP, processeur de sécurité de la plateforme en français) d'AMD. Ces périphériques sont souvent source d'inquiétudes car leur fonctionnement est opaque et ils peuvent parfois servir de portes d'entrée dérobées [6] sur les ordinateurs qui en sont équipés.

D'autres périphériques peuvent nécessiter l'ajout d'une carte supplémentaire, dite *carte fille*, comme c'est le cas pour la plupart des adaptateurs Wi-Fi.

1.2.6 Le microprogramme de la carte mère



Une puce de microprogramme sur une carte mère

Pour démarrer l'ordinateur, il faut donner au processeur un premier programme, pour pouvoir charger les programmes à exécuter ensuite.

Ce petit logiciel, appelé *microprogramme* [7] de la carte mère est contenu dans une puce mémoire fixée sur celle-ci. C'est une mémoire *flash* comme dans les clés USB ou les disques SSD.

Le microprogramme historique de la plupart des ordinateurs personnels est appelé BIOS (*Basic Input/Output System*, ou système d'entrée/sortie de base). Depuis 2012,

6. Ces périphériques fonctionnent avec des logiciels qui peuvent contenir une porte dérobée (ou *backdoor* en anglais), c'est à dire une fonctionnalité qui donne un accès secret au logiciel, voire à l'ordinateur, et dont l'utilisatrice n'a pas connaissance.

7. Un microprogramme peut aussi être appelé *firmware* (en anglais), micrologiciel, microcode, logiciel interne ou encore logiciel embarqué.

de plus en plus d'ordinateurs utilisent un nouveau standard appelé UEFI (*Unified Extended Firmware Interface*).

Ce premier programme exécuté par l'ordinateur permet, entre autres, de choisir où se trouve le système d'exploitation que l'on veut utiliser. Il est en général chargé à partir du disque dur mais peut aussi venir d'une clé USB, d'un CD ou d'un DVD, voire du réseau. page suiv.



Pour aller plus loin…

Pour faire un tour dans le microprogramme d'un ordinateur, on pourra suivre la partie *Entrer dans l'interface de configuration du microprogramme* dans l'outil *Démarrer sur un CD, un DVD ou une clé USB* (voir page 108).

1.3 Électricité, champs magnétiques, bruits et ondes radio

Après ce rapide tour de ce qui le compose, voyons maintenant ce qui concerne la confidentialité des informations qui circulent au sein d'un ordinateur.

Tout d'abord, l'essentiel de l'information circule sous forme de courants électriques. Rien n'empêche donc de mettre l'équivalent d'un *ampèremètre* pour mesurer le courant qui passe, et ainsi pouvoir reconstituer des données manipulées par l'ordinateur sous une forme ou une autre.

Par ailleurs, tout courant électrique qui circule a tendance à émettre un champ magnétique. Ces champs magnétiques peuvent rayonner à quelques mètres, voire plus[8]. Il est donc possible, pour qui s'en donne les moyens, de reconstituer le contenu d'un écran ou ce qui a été tapé sur un clavier, et cela même derrière un mur, depuis la rue ou l'appartement contigu. Ainsi, des chercheurs ont réussi à enregistrer les touches tapées sur des claviers filaires normaux à partir de leurs émissions électromagnétiques, à une distance allant jusqu'à 20 mètres[9].

Le même type d'opération est possible à partir de l'observation des légères perturbations que génère l'ordinateur sur le réseau électrique où il est branché[10].

D'autres expériences consistant à écouter avec un microphone le bruit des composants électroniques de l'ordinateur ainsi que de son alimentation électrique, ont permis dans certaines conditions de déchiffrer des clés de chiffrement contenues sur l'ordinateur cible[11]. Des corrections ont, depuis, été apportées aux logiciels impliqués afin de compliquer ce type d'attaque.

Enfin, certains périphériques (claviers, souris, écouteurs, *etc.*) fonctionnent *sans fil*. Ils communiquent donc avec l'ordinateur par des ondes radio que n'importe qui autour peut capter, et éventuellement décoder.

Pour résumer, même si un ordinateur n'est pas connecté à un réseau, et quels que soient les programmes qui fonctionnent dessus, il est tout de même possible pour des personnes expertes et bien équipées de réaliser une « écoute » de ce qui se passe à l'intérieur.

---

8. Berke Durak a réussi en 1995 à capter les ondes électromagnétiques [http://lambda-diode.com/electronics/tempest/] émises par la plupart des composants de son ordinateur avec un simple *walkman* capable de recevoir la radio (lien en anglais).

9. Martin Vuagnoux et Sylvain Pasini ont réalisé d'effrayantes vidéos [https://lasecwww.epfl.ch/keyboard/] pour illustrer leur papier *Compromising Electromagnetic Emanations of Wired and Wireless Keyboards* publié en 2009 (lien en anglais).

10. En 1998, Paul Kocher, Joshua Jaffe et Benjamin Jun ont publié un rapport [https://www.rambus.com/wp-content/uploads/2015/08/DPATechInfo.pdf] expliquant les différentes techniques d'analyse de consommation électrique (lien en anglais).

11. Clément Bohic, 2013, *Chiffrement : il suffirait d'écouter le processeur pour décoder les clefs*, silicon.fr [https://www.silicon.fr/chiffrement-ecouter-processeur-decoder-clefs-91686.html].

1.4 Les logiciels

Au-delà de la somme d'éléments physiques qui constituent un ordinateur, il faut aussi se pencher sur les éléments moins palpables : les logiciels.

À l'époque des tout premiers ordinateurs, chaque fois qu'il fallait exécuter des traitements différents, il fallait intervenir physiquement pour changer la disposition des câbles et des composants. On en est bien loin aujourd'hui : les opérations à réaliser pour faire ces traitements sont devenues des données comme les autres. Ces données, que l'on appelle *programmes*, sont chargées, modifiées et manipulées par d'autres programmes.

Un ensemble de programmes qui permettent de réaliser une tâche donnée est appelé *logiciel*. C'est ensuite l'interaction de milliers de logiciels entre eux qui permettra de réaliser les tâches complexes pour lesquelles sont généralement utilisés les ordinateurs de nos jours.

L'effet produit lorsqu'on clique sur un bouton, c'est donc le lancement d'une chaîne d'évènements, d'une somme impressionnante de calculs qui aboutissent à des impulsions électriques venant modifier un objet physique. C'est comme les vibrations de la membrane d'une enceinte pour jouer un son, un écran qui modifie ses LED pour afficher une nouvelle page, ou un disque SSD qui active ou désactive des micro-interrupteurs pour créer la suite binaire de données qui constituera un *fichier*.

1.4.1 Le système d'exploitation

Le but d'un *système d'exploitation* est avant tout de permettre aux différents logiciels de se partager l'accès aux composants matériels de l'ordinateur et de communiquer entre eux. Par ailleurs, un système d'exploitation est généralement livré avec des logiciels, au moins pour pouvoir démarrer d'autres logiciels.

La partie fondamentale d'un système d'exploitation est son *noyau*, qui s'occupe de coordonner l'utilisation du matériel par les autres logiciels.

Pour chaque composant matériel de l'ordinateur que l'on veut utiliser, le noyau active un programme qu'on appelle *pilote* (ou *driver* en anglais). Il existe des pilotes pour les périphériques d'entrée (clavier, souris, *etc.*), de sortie (écran, imprimante, *etc.*), de stockage (DVD, clé USB, *etc.*).

Le noyau gère aussi l'exécution des différents programmes, en allouant à chacun des parties de la mémoire vive et du temps de calcul du processeur.

Au-delà du noyau, les systèmes d'exploitation utilisés de nos jours, comme Windows, macOS ou GNU/Linux, incluent aussi de nombreux outils (ou utilitaires) ainsi que des environnements de bureau graphiques qui permettent d'utiliser l'ordinateur en cliquant simplement sur des boutons.

Le système d'exploitation est en général stocké sur le disque dur. Cependant, il est aussi tout à fait possible d'utiliser un système d'exploitation enregistré sur une clé USB ou gravé sur un DVD. Dans ces derniers cas, on parle de système *live*.

1.4.2 Les applications

On appelle *applications*, les logiciels qui permettent réellement de faire ce qu'on a envie de demander à l'ordinateur. On peut citer en exemples Mozilla Firefox comme navigateur web, LibreOffice pour la bureautique ou encore VLC pour la lecture de musique et de vidéo.

Chaque système d'exploitation définit une méthode bien spécifique pour que les applications puissent accéder au matériel, à des données, au réseau, ou à d'autres ressources. Les applications que l'on souhaite utiliser doivent donc être adaptées au système d'exploitation de l'ordinateur sur lequel on veut s'en servir.

1.4.3 Les bibliothèques

Plutôt que de réécrire dans toutes les applications des morceaux de programme chargés de faire les mêmes choses, ces morceaux sont regroupés dans des bibliothèques, ou *libraries* en anglais, que les logiciels se partagent.

Il existe des bibliothèques pour l'affichage graphique (assurant la cohérence de ce qui est affiché à l'écran), pour lire ou écrire des formats de fichier, pour interroger certains services réseaux, *etc.*

Si l'on n'écrit pas soi-même de logiciels, on a rarement besoin d'aller dans ces bibliothèques. Il peut toutefois être intéressant de connaître leur existence, ne serait-ce que parce qu'un problème (comme une erreur de programmation) dans une bibliothèque peut se répercuter sur tous les logiciels qui l'utilisent.

1.4.4 Les paquets

Les systèmes d'exploitation GNU/Linux peuvent être organisés différement en fonction de leur distribution[12]. Certaines distributions (dont Debian ou Tails, sur lesquelles s'appuient la majorité des outils présentés dans ce guide), fonctionnent avec des *paquets* ou paquetages (*packages* en anglais).

page ci-contre

Les logiciels (*système d'exploitation, applications ou bibliothèques*) sont alors installés à partir de paquets. Un paquet est composé de plusieurs fichiers qui permettent, entre autres, l'exécution du programme, de préciser s'il dépend d'autres logiciels ou d'autres paquets, de pouvoir le configurer, de fournir de la documentation, de vérifier son authenticité, *etc.*

Le système pourra fonctionner avec un logiciel qui permet d'automatiser l'installation, la désinstallation et la mise à jour des paquets. Ces logiciels s'appellent des *gestionnaires de paquets*. En général, les paquets d'une distribution sont disponibles sur Internet dans ce qu'on appelle des *dépôts*. Le gestionnaire de paquets va donc récupérer les paquets nécessaires depuis ces dépôts, qui sont spécifiques à chaque distribution.

1.5 Le rangement des données

On a vu qu'un disque dur (ou une clé USB) permettait de garder des données entre deux allumages d'un ordinateur.

Mais pour pouvoir s'y retrouver, les données sont agencées d'une certaine manière : un meuble sans étagères dans lequel on entasse des feuilles de papier n'est pas forcément la forme de rangement la plus efficace.

1.5.1 Les partitions

Tout comme on peut mettre plusieurs étagères dans un meuble, on peut « découper » un disque dur en plusieurs *partitions*.

Chaque étagère pourra avoir une hauteur différente et un classement différent, selon que l'on souhaite y mettre des livres ou des classeurs, par ordre alphabétique ou par ordre chronologique.

De la même manière sur un disque dur, chaque partition pourra être de taille différente et contenir un mode d'organisation différent : cela s'appelle un *système de fichiers*.

12. La distribution d'un système d'exploitation est une version de celui-ci adaptée à des usages ou des besoins spécifiques. Cela peut être pour qu'il soit particulièrement léger ou plus facile d'utilisation par exemple, mais aussi pour des fonctionnements spéciaux (pour une entreprise ou un outil particulier). Chaque distribution rassemble une collection de logiciels adaptée et cohérente, depuis le système jusqu'aux applications, avec plus ou moins de fonctionnalités.

1.5.2 Les systèmes de fichiers

Un système de fichiers sert donc à pouvoir retrouver des informations dans notre immense pile de données, comme la table des matières d'un livre de cuisine permet d'aller directement à la bonne page pour lire la recette du festin du soir.

Notons toutefois que la suppression d'un fichier ne supprime pas le contenu du fichier et ne fait qu'enlever une ligne dans la table des matières. En parcourant toutes les pages, on pourra toujours retrouver notre recette, tant que la page n'aura pas été réécrite — ce point sera développé plus loin.

page 42

On peut imaginer des milliers de formats différents pour ranger des données, et il existe donc de nombreux systèmes de fichiers différents. On parle de *formatage* lors de la création d'un système de fichiers défini sur un support.

Comme c'est le système d'exploitation qui donne aux programmes l'accès aux données, un système de fichiers est souvent fortement lié à un système d'exploitation particulier.



Précision

Pour en citer quelques-uns : les types NTFS et FAT32 sont ceux employés habituellement par les systèmes d'exploitation Windows ; le type *ext* (`ext2`, `ext4`) est souvent utilisé par GNU/Linux ; les types HFS, HFS+ et HFSX sont employés par macOS.

Une des conséquences de cela est qu'il peut exister sur un ordinateur donné des espaces de stockage non reconnus par le système d'exploitation, auxquels on ne pourra donc pas accéder aisément.

Il est néanmoins possible de lire un système de fichiers *a priori* inconnu par le système qu'on utilise, moyennant l'usage du logiciel adéquat. Windows est par exemple capable de lire une partition *ext3*, si on installe le logiciel approprié.

1.5.3 Les formats de fichiers

Les données que l'on manipule sont généralement regroupées sous forme de fichiers. Un fichier a un contenu -les données- ainsi que des métadonnées à savoir un nom, un emplacement (le dossier dans lequel il se trouve), une taille, et d'autres détails selon le système de fichiers utilisé.

page 30

Mais à l'intérieur de chaque fichier, les données sont elles-mêmes organisées différemment selon leur nature et les logiciels utilisés pour les manipuler. On parle de *format* de fichier pour les différencier.

En général, on met à la fin du nom d'un fichier un code, qu'on appelle parfois *extension*, permettant d'indiquer le format du fichier. On peut choisir une extension ou une autre et la modifier. Toutefois c'est surtout à titre indicatif et ne signifie pas, qu'en changeant l'extension, on change le format du fichier.

Quelques exemples d'extensions : pour la musique, on utilisera souvent les formats MP3 ou Ogg ; pour un document texte de LibreOffice ce sera OpenDocument Text (ODT) ; pour des images, on aura le choix entre JPEG, PNG et d'autres ; *etc.*

Comme les logiciels, les formats peuvent être *ouverts* ou *propriétaires*. Les formats *ouverts* sont définis publiquement, afin, entre autres, de ne pas restreindre leur utilisation à un seul logiciel.

page 39

Certains formats *propriétaires* ont été étudiés à la loupe pour les rendre utilisables par d'autres logiciels, mais leur compréhension reste souvent imparfaite. C'est typiquement le cas pour l'ancien format de Microsoft Word (DOC) ou celui d'Adobe Photoshop (PSD).

1.5.4 La mémoire virtuelle (*swap*)

En théorie, toutes les données auxquelles le processeur doit accéder, et donc tous les programmes et les documents ouverts, devraient se trouver en mémoire vive. Mais pour pouvoir ouvrir plein de programmes et de documents en même temps, les systèmes d'exploitation modernes trichent : ils échangent, quand c'est nécessaire, des morceaux de mémoire vive avec un espace du disque dur prévu à cet effet. On parle alors de « mémoire virtuelle », de *swap* en anglais ou encore d'« espace d'échange ».

Le système d'exploitation fait donc sa petite cuisine pour que le processeur ait toujours dans la mémoire vive les données auxquelles il veut réellement accéder. La mémoire virtuelle est ainsi un exemple d'espace de stockage auquel on ne pense pas forcément, enregistré sur le disque dur, soit sous forme d'un gros fichier contigu (avec Windows et parfois avec GNU/Linux), soit dans une partition à part (avec GNU/Linux).

On reviendra dans la partie suivante sur les problèmes que posent ces questions de format et d'espace de stockage du point de vue de la confidentialité des données.

Chapitre 2

Traces à tous les étages

Le fonctionnement normal d'un ordinateur laisse de nombreuses traces de ce que l'on fait dessus. Parfois, elles sont *nécessaires* à son fonctionnement. D'autres fois, ces informations sont collectées pour permettre aux logiciels d'être « plus pratiques ».

2.1 Dans la mémoire vive

On a vu que le premier lieu de stockage des informations sur un ordinateur est la mémoire vive.

page 18

Tant que l'ordinateur est sous tension électrique, elle contient toutes les informations dont le système a besoin. Elle conserve donc nécessairement de nombreuses traces : frappes au clavier (y compris les mots de passe), fichiers ouverts, et autres divers évènements qui ont rythmé la phase d'éveil de l'ordinateur.

En prenant le contrôle d'un ordinateur qui est allumé, il n'est pas très difficile de transférer l'ensemble des informations contenues dans la mémoire vive, par exemple vers une clé USB ou vers un autre ordinateur à travers le réseau. Et prendre le contrôle d'un ordinateur peut être aussi simple que d'y brancher un *iPod* bricolé quand la propriétaire a le dos tourné [1]. Une fois récupérées, les nombreuses informations que contient la mémoire vive, sur les personnes qui utilisent cet ordinateur par exemple, pourront alors être exploitées.

On a également vu que ces données deviennent illisibles après la mise hors tension de l'ordinateur. Néanmoins, cela prend plus ou moins de temps et cela peut suffire pour qu'une personne mal intentionnée ait le temps de récupérer ce qui s'y trouve. On appelle cela une *cold boot attack* : l'idée est de copier le contenu de la mémoire vive avant qu'elle ait eu le temps de s'effacer, de manière à l'exploiter par la suite. Il est même techniquement possible de porter à très basse température la mémoire d'un ordinateur fraîchement éteint, auquel cas on peut faire subsister son contenu plusieurs heures, voire plusieurs jours [2].

Cette attaque doit cependant être réalisée très peu de temps après la mise hors tension pour fonctionner. Par ailleurs, si on utilise quelques gros logiciels (par exemple en retouchant une énorme image avec Adobe Photoshop ou GIMP) avant d'éteindre son ordinateur, les traces qu'on a laissées précédemment en mémoire vive ont de fortes chances d'être recouvertes. Surtout, il existe des logiciels spécialement conçus pour écraser le contenu de la mémoire vive avec des données aléatoires juste avant l'extinction de l'ordinateur.

---

1. Fernand Lone Sang, Vincent Nicomette, Yves Deswarte, Loïc Duflot, 2011, *Attaques DMA peer-to-peer et contremesures* [https://www.sstic.org/media/SSTIC2011/SSTIC-actes/attaques_dma_peer-to-peer_et_contremesures/SSTIC2011-Article-attaques_dma_peer-to-peer_et_contremesures-lone-sang_duflot_nicomette_deswarte.pdf]. Maximillian Dornseif, 2004, *0wned by an iPod* [https://web.archive.org/web/20100326020818/http://md.hudora.de/presentations/#firewire-pacsec] (en anglais).

2. J. Alex Halderman *et al.*, 2008, *Lest We Remember : Cold Boot Attacks on Encryption Keys* [https://citp.princeton.edu/memory/] (en anglais).

2.2 Dans la mémoire virtuelle

page 25 Comme expliqué auparavant, le système d'exploitation utilise, dans certains cas, une partie du disque dur pour venir en aide à sa mémoire vive. Ça arrive en particulier si l'ordinateur est fortement sollicité, par exemple quand on travaille sur de grosses images, mais aussi dans de nombreux autres cas, de façon peu prévisible.

La conséquence la plus gênante de ce fonctionnement pourtant bien pratique, c'est que l'ordinateur va écrire sur le disque dur des informations qui se trouvent dans la mémoire vive, informations potentiellement sensibles, *et qui resteront ainsi lisibles après avoir éteint l'ordinateur.*

page 44 Avec un ordinateur configuré de façon standard, il est donc illusoire de croire qu'un document lu à partir d'une clé USB, même ouvert avec un logiciel portable, ne laissera jamais de traces sur le disque dur.

page 47 Pour éviter de laisser n'importe qui accéder à ces données, il est possible d'utiliser un système d'exploitation configuré pour chiffrer la mémoire virtuelle.

2.3 Veille et hibernation

La plupart des systèmes d'exploitation permettent de mettre un ordinateur « en pause ». C'est surtout utilisé avec les ordinateurs portables mais c'est également valable pour les ordinateurs de bureau.

Il y a deux grandes familles de « pause » : la veille et l'hibernation.

2.3.1 La veille

La *veille* (appelée aussi en anglais *suspend to RAM* ou *suspend*) consiste à éteindre le maximum de composants de l'ordinateur tout en gardant sous tension de quoi pouvoir le relancer rapidement.

Au minimum, la mémoire vive continuera d'être alimentée pour conserver l'intégralité des données sur lesquelles on travaillait — c'est-à-dire notamment les mots de passe et les clés de chiffrement.

page 47

En bref, un ordinateur en veille protège aussi peu l'accès aux données qu'un ordinateur allumé.

2.3.2 L'hibernation

L'*hibernation* ou *mise en veille prolongée*, appelée aussi en anglais *suspend to disk*, consiste à sauvegarder l'intégralité de la mémoire vive sur le disque dur pour ensuite éteindre complètement l'ordinateur. Lors de son prochain démarrage, le système d'exploitation détectera l'hibernation, recopiera la sauvegarde vers la mémoire vive et recommencera à travailler à partir de là.

page 25 Sur les systèmes GNU/Linux, la copie de la mémoire se fait généralement dans la mémoire virtuelle (*swap*). Sur d'autres systèmes, ça peut être dans un gros fichier, souvent *caché*.

Étant donné que c'est tout le contenu de la mémoire vive qui est alors écrit sur le disque dur, cela veut dire que tous les programmes et documents ouverts, mots de passe, clés de chiffrement et autres, pourront être retrouvés par quiconque accèdera au disque dur. Et cela, aussi longtemps que rien n'aura été réécrit par-dessus.

page 47 Ce risque est toutefois limité par le chiffrement du disque dur : la phrase de passe sera alors nécessaire pour accéder à la sauvegarde de la mémoire vive.

2.4 Les journaux

Les systèmes d'exploitation écrivent dans leurs *journaux système* un historique détaillé de ce qu'ils font.

Ces journaux (aussi appelés *logs*) sont utiles au système d'exploitation pour fonctionner, et peuvent nous permettre de corriger des problèmes de configuration ou des *bugs*.

Cependant, ces journaux conservent aussi des données qui peuvent poser des problèmes de vie privée. Par exemple, ils enregistrent :

- la date, l'heure et le pseudo de l'utilisatrice qui se connecte à chaque fois que l'ordinateur est allumé ;
- la marque et le modèle de chaque support amovible (disque externe, clé USB…) branché ;
- la date d'une impression et le nombre de pages ;
- le nom du logiciel, la date et l'heure de l'installation ou de la désinstallation d'une application.

Par défaut, tous ces journaux sont conservés sans limite de durée sur le disque dur de l'ordinateur, sauf dans le cas des systèmes *live* qui les enregistrent dans leur mémoire vive.

2.5 Sauvegardes automatiques et autres listes

En plus de ces journaux, il est possible que d'autres traces de fichiers, même supprimés, subsistent sur l'ordinateur. Même si les fichiers et leur contenu ont bien été supprimés, une partie du système d'exploitation ou d'un autre programme peut délibérément en garder une trace.

Voici quelques exemples :

- un logiciel de traitement de texte peut garder la référence à un nom de fichier supprimé dans le menu des « documents récents ». Parfois, il peut même garder des fichiers temporaires avec le contenu du fichier en question. Il existe des dizaines de programmes fonctionnant ainsi ;
- lorsqu'on utilise une imprimante, le système d'exploitation copie souvent le fichier en attente dans la « file d'impression ». Le contenu de ce fichier, une fois la file vidée, n'aura pas disparu du disque dur pour autant ;
- sous Windows, lorsqu'on connecte un lecteur amovible (clé USB, disque dur externe, carte SD ou DVD), le système commence souvent par explorer son contenu afin de proposer des logiciels adaptés à sa lecture : cette exploration automatique laisse en mémoire la liste de tous les fichiers présents sur le support employé, même si aucun des fichiers qu'il contient n'est consulté.

Il est difficile de trouver une solution adéquate à ce problème. Un fichier, même parfaitement supprimé, continuera probablement à exister sur l'ordinateur pendant un certain temps sous une forme différente. Une recherche sur les données brutes du disque permet de voir si des copies de ces données existent ou pas, à moins qu'elles n'y soient seulement référencées ou stockées sous une forme différente, comme par exemple sous forme compressée.

En fait, seuls l'écrasement de la totalité du disque et l'installation d'un nouveau système d'exploitation permettraient d'avoir la garantie que les traces d'un fichier ont bien été supprimées. Dans une autre perspective, l'utilisation d'un système *live*, dont l'équipe de développement porte une attention particulière à cette question, garantit que ces traces ne seront pas laissées ailleurs que dans la mémoire vive. Nous y reviendrons plus loin.

page 139

page 113

2.6 Les métadonnées

En plus des informations contenues dans un fichier, il existe des informations accompagnant celui-ci, qui ne sont pas forcément visibles de prime abord : date de création, nom du logiciel utilisé, de l'ordinateur, *etc.* Ces « données sur les données » s'appellent communément des « métadonnées ».

page 24

Une partie des métadonnées est enregistrée par le système de fichiers : le nom du fichier, la date et l'heure de sa création et des modifications, et souvent bien d'autres choses. Ces traces sont laissées sur l'ordinateur (ce qui peut quand même être un problème en soi), mais elles ne sont la plupart du temps pas inscrites dans le fichier.

page 24

En revanche, de nombreux formats de fichiers conservent également des métadonnées *à l'intérieur* du fichier. Elles seront donc diffusées avec le fichier lors de son éventuelle copie sur une clé USB, de son envoi par mail ou de sa publication en ligne. Ces informations pourront alors être connues de quiconque aura accès au fichier.

Les métadonnées enregistrées dépendent des formats et des logiciels utilisés. La plupart des formats de fichier audio permettent d'enregistrer le titre du morceau et l'interprète. Les traitements de texte ou les PDF enregistreront un nom d'autrice, la date et l'heure de création, et parfois même l'historique complet des dernières modifications [3], donc, potentiellement, des informations que l'on pensait avoir supprimées.

La palme revient probablement aux formats d'images comme TIFF ou JPEG : ces fichiers photos créés par un appareil numérique ou un téléphone portable contiennent des métadonnées au format EXIF. Ces dernières peuvent contenir la marque, le modèle et le numéro de série de l'appareil utilisé, mais aussi la date, l'heure et parfois même les coordonnées géographiques de la prise de vue, sans oublier une version miniature de l'image. Ce sont d'ailleurs ces métadonnées qui mettront fin à la cavale de John McAfee, fondateur et ancien patron de la société de sécurité informatique du même nom [4]. De plus, toutes ces informations ont tendance à rester même après que le fichier soit passé par un logiciel de retouche photo. Le cas de la miniature est particulièrement intéressant : de nombreuses photos disponibles sur Internet contiennent encore l'intégralité d'une photo recadrée [5] voire des visages ayant été « floutés » [6].

page 24

Pour la plupart des formats de fichiers *ouverts*, il existe toutefois des logiciels pour examiner et éventuellement supprimer les métadonnées.

page 185

3. Deblock Fabrice, 2006, *Quand les documents Word trahissent la confidentialité* [https://web.archive.org/web/20190913142445/http://www.journaldunet.com/solutions/0603/060327-indiscretions-word.shtml].

4. Big Browser, 2012, *Vice de forme – La bourde qui a mené à l'arrestation de John McAfee* [https://www.lemonde.fr/big-browser/article/2012/12/12/vice-de-forme-la-bourde-qui-a-mene-a-l-arrestation-de-john-mcafee_5986399_4832693.html].

5. Il existe même des moteurs de recherche par métadonnées : Stolen Camera Finder [https://www.stolencamerafinder.com/] (en anglais) ou CameraTrace [http://www.cameratrace.com/trace] (en anglais), par exemple.

6. Maximillian Dornseif et Steven J. Murdoch, 2004, *Hidden Data in Internet Published Documents* [http://events.ccc.de/congress/2004/fahrplan/files/316-hidden-data-slides.pdf] (en anglais).

Chapitre 3

Logiciels malveillants, mouchards et autres espions

Tout système d'exploitation laisse donc des traces, au moins lorsqu'il est en fonctionnement. Au-delà de ces traces, on peut aussi trouver dans nos ordinateurs tout un tas de *mouchards*. Ils peuvent être soit installés à notre insu (permettant par exemple de récupérer des mots de passe ou des contacts mail), soit présents de manière systématique dans les logiciels qu'on aura installés.

Ces mouchards peuvent participer à diverses techniques de surveillance, de la « lutte contre le piratage » de logiciels propriétaires, au fichage ciblé d'un individu, en passant par la collecte de données pour des pourriels (*spam*)[1], ou autres arnaques. page 39

La portée de ces dispositifs augmente fortement dès que l'ordinateur est connecté à Internet. Leur installation est alors grandement facilitée si on ne fait rien de spécial pour se protéger, et la récupération des données collectées se fait à distance.

Toutefois les gens qui récoltent ces informations sont inégalement dangereux : ça dépend des cas, de leurs motivations et de leurs moyens. Les auteurs de violences domestiques[2], les GAFAM[3] qui traquent les données des internautes à des fins publicitaires, les gendarmes de Saint-Tropez, ou la *National Security Agency* états-unienne… autant de personnes ou de structures souvent en concurrence entre elles et ne formant pas une totalité cohérente.

Pour s'introduire dans nos ordinateurs, elles n'ont pas toutes accès aux mêmes moyens ou aux mêmes outils : par exemple, l'espionnage industriel est une des raisons importantes de la surveillance plus ou moins légale[4], et, malgré les apparences[5], il ne faut pas croire que Microsoft donne toutes les astuces de Windows à la police française.

3.1 Contexte légal

Cependant, les flics et les services de renseignement français disposent maintenant des moyens de mettre en place une surveillance informatique très complète en toute légalité, en s'appuyant sur plusieurs « mouchards » présentés par la suite.

1. Le pourriel ou *spam* est une communication électronique non sollicitée, le plus souvent du courrier électronique.

2. Catherine Armitage, 2014, *Spyware's role in domestic violence* [https://www.theage.com.au/technology/technology-news/spywares-role-in-domestic-violence-20140321-358sj.html] parle de l'utilisation des *malwares* et autres outils technologiques par des auteurs de violences domestiques (en anglais).

3. GAFAM est l'acronyme de cinq grandes firmes états-uniennes — Google, Apple, Facebook, Amazon et Microsoft — qui dominent le marché du numérique.

4. Pour se faire une idée des problématiques liées à l'espionnage industriel : Wikipédia, 2014, *Espionnage industriel* [https://fr.wikipedia.org/wiki/Espionnage_industriel].

5. Microsoft, en partenariat avec Interpol, a fabriqué une boîte à outils appelée COFEE (Computer Online Forensic Evidence Extractor) mise à disposition des polices d'une quinzaine de pays. Korben, 2009, *Cofee – La clé sécurité de Microsoft vient d'apparaitre sur la toile* [https://korben.info/cofee-la-cle-securite-de-microsoft-vient-dapparaitre-sur-la-toile.html].

La loi « renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale » de 2016[6] inclut des dispositions légales qui permettent d'installer des mouchards pour enregistrer et communiquer ce qui s'affiche à l'écran ou ce que les différents périphériques (clavier, webcam, scanner, téléphone portable…) transmettent à l'ordinateur.

La « pose » des ces mouchards est autorisée, à distance ou en pénétrant dans le domicile de la personne surveillée pour y installer les outils nécessaires[7]. Le juge des libertés et de la détention peut le demander lors d'enquêtes préliminaires et de flagrance ; le juge d'instruction lors d'une information judiciaire[8]. Ces mesures ne s'appliquent pas qu'aux actes relevant du « terrorisme » (comme la « prolifération des armes de destruction massive »), mais aussi à nombre de délits dès lors qu'ils sont commis à plusieurs (en « bande organisée »). Cela peut aller de l'aide « à la circulation et au séjour irréguliers d'un étranger en France » en passant par la « destruction, dégradation et détérioration d'un bien »[9].

La loi relative au renseignement de 2015[10] donne à peu près les mêmes pouvoirs[11] aux « services spécialisés de renseignement » pour « la recherche, la collecte, l'exploitation et la mise à disposition du Gouvernement des renseignements relatifs aux enjeux géopolitiques et stratégiques ainsi qu'aux menaces et aux risques susceptibles d'affecter la vie de la Nation »[12].

3.2 Les logiciels malveillants

Les logiciels malveillants[13] (que l'on appelle également *malwares*) sont des logiciels qui ont été développés dans le but de nuire : collecte d'informations, hébergement d'informations illégales, relai de pourriels, *etc.* Les virus informatiques, les vers, les chevaux de Troie, les *spywares*, les *rootkits* (logiciels permettant de prendre le contrôle d'un ordinateur) et les *keyloggers* font partie de cette famille. Certains programmes peuvent appartenir à plusieurs de ces catégories simultanément.

page 35

3.2.1 Exploitation de failles

Afin de s'installer sur un ordinateur, certains logiciels malveillants exploitent les vulnérabilités du système d'exploitation[14] ou des applications. Ils s'appuient sur des erreurs de conception ou de programmation pour détourner le déroulement des programmes à leur avantage. Malheureusement, de telles « failles de sécurité » ont été trouvées dans de très nombreux logiciels, et de nouvelles sont trouvées constamment, tant par des gens qui cherchent à les corriger que par d'autres qui cherchent à les exploiter.

---

6. Légifrance, 2016, *loi n° 2016-731 du 3 juin 2016 renforçant la lutte contre le crime organisé, le terrorisme et leur financement, et améliorant l'efficacité et les garanties de la procédure pénale* [https://www.legifrance.gouv.fr/loda/id/JORFTEXT000032627231/].
7. Légifrance, 2019, *Code de procédure pénale*, article 706-102-1 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311624/2019-06-01/].
8. Légifrance, 2019, *Code de procédure pénale*, article 706-95-12 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038270130/2019-06-01/].
9. Légifrance, 2017, *Code de procédure pénale*, articles 706-73 et 706-73-1 [https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006071154/LEGISCTA000006138138].
10. Légifrance, 2015, *loi n° 2015-912 du 24 juillet 2015 relative au renseignement* [https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030931899].
11. Légifrance, 2017, *Code de la Sécurité Intérieure*, article L853-2 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043887476].
12. Légifrance, 2015, *Code de la Sécurité Intérieure*, article L811-2 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000030939233].
13. Toute cette partie est grandement inspirée du passage consacré à la question dans le *Surveillance Self-Defense Guide* [https://ssd.eff.org/fr/module/comment-puis-je-me-prot%C3%A9ger-contre-les-programmes-malveillants] de l'*Electronic Frontier Foundation*.
14. D'après l'*Internet Storm Center* [https://isc.sans.edu/survivaltime.html] (en anglais), en 2021, un système d'exploitation sur lequel les mises à jour de sécurité n'ont pas été installées se fait compromettre en moins d'une heure si il est connecté directement à Internet.

3.2.2 Ingénierie sociale

Un autre moyen courant est d'inciter la personne utilisant l'ordinateur à lancer le logiciel malveillant en le cachant dans un logiciel en apparence inoffensif. C'est ainsi que, sur un média social lié à la révolution syrienne, un simple lien vers une vidéo amenait en fait les internautes à télécharger un virus contenant un *keylogger*[15].

Les adversaires n'ont alors pas besoin de trouver des vulnérabilités sérieuses dans des logiciels courants. Il est particulièrement difficile de s'assurer que des ordinateurs partagés par de nombreuses personnes ou des ordinateurs qui se trouvent dans des lieux publics, comme une bibliothèque ou un cybercafé, n'ont pas été corrompus : il suffit en effet qu'une seule personne un peu moins vigilante se soit fait avoir…

3.2.3 Camouflage

En outre, la plupart des logiciels malveillants « sérieux » ne laissent pas de signes immédiatement visibles de leur présence, et peuvent même être très difficiles à détecter. Le cas sans doute le plus compliqué est celui de failles jusqu'alors inconnues, appelées « vulnérabilités zero-day »[16], et que les logiciels antivirus seraient bien en peine de reconnaître, car pas encore répertoriées. C'est exactement ce genre d'exploitations de failles « zero-day » que la compagnie VUPEN a vendues à la NSA en 2012[17].

Des logiciels malveillants peuvent être cachés dans des endroits insoupçonnés de l'ordinateur : ainsi, les processeurs Intel incluent depuis peu un moteur de gestion (Management Engine ou ME en anglais). Or, plusieurs failles de sécurité ont été découvertes en 2017 dans le microprogramme de ce moteur de gestion[18]. Elles permettent d'installer un logiciel malveillant complètement indétectable qui résiste aux mises à jour du système d'exploitation et a accès à l'ensemble du processeur et de la mémoire vive[19].

3.2.4 Capacités

Ces logiciels permettent d'effectuer de nombreuses opérations : obtenir des numéros de cartes bancaires ou des mots de passe, envoyer des pourriels, participer à attaquer un serveur en le saturant de demandes, *etc.* Ils peuvent également utiliser le micro, la webcam ou d'autres périphériques de l'ordinateur. Il existe un vrai marché spécialisé où l'on peut acheter de tels programmes, personnalisés pour différents objectifs.

Mais ils servent tout aussi bien à espionner des organisations ou des individus spécifiques[20], par exemple en exfiltrant des documents stockés sur l'ordinateur (même les documents chiffrés, s'ils ont été déchiffrés à un moment), ou en réduisant à néant des dispositifs d'anonymat sur Internet. page 47

15. Eva Galperin *et al.*, 2014, *Quantum of Surveillance : Familiar Actors and Possible False Flags in Syrian Malware Campaigns* [https://www.eff.org/files/2013/12/28/quantum_of_surveillance4d.pdf] (en anglais).
16. Wikipédia, 2016, *Vulnérabilité zero-day* [https://fr.wikipedia.org/wiki/Vuln%C3%A9rabilit%C3%A9_zero-day].
17. Grégoire Fleurot, 2013, *Espionnage : Vupen, l'entreprise française qui bosse pour la NSA* [https://www.slate.fr/france/77866/vupen-nsa-espionnage-exploits].
18. Guillaume Louel, 2017, *Nouvelle faille de sécurité de l'Intel ME !*, Hardware.fr [https://www.hardware.fr/news/15297/nouvelle-faille-securite-intel-me.html].
19. Mark Ermolov, Maxim Goryachy, 2018, *How to Hack a Turned-off Computer, or Running Unsigned Code in Intel ME*, blackhat.com [https://www.blackhat.com/docs/eu-17/materials/eu-17-Goryachy-How-To-Hack-A-Turned-Off-Computer-Or-Running-Unsigned-Code-In-Intel-Management-Engine-wp.pdf] (en anglais).
20. Par exemple, une attaque ciblée contre les institutions géorgiennes attribuée aux services secrets russes : Ministry of Justice of Georgia et al., 2012, *Cyber Espionage Against Georgian Government* [https://web.archive.org/web/20200601112146/https://dea.gov.ge/uploads/CERT%20DOCS/Cyber%20Espionage.pdf] (en anglais).



Précision

Pour donner un exemple venu des Émirats Arabes Unis, un militant des droits humains, Ahmed Mansour, a été victime d'une attaque ciblée sur son smartphone[21]. Un SMS contenant un lien vers un virus lui a été envoyé. Ce virus permettait à la personne le contrôlant d'utiliser la caméra, le micro et de surveiller les activités du téléphone de la victime à tout instant. L'attaque a été déjouée et disséquée grâce à Citizen Lab.

page 31

Les services de renseignement et les flics français ont le droit d'utiliser légalement de tels logiciels, ce qui veut très certainement dire qu'ils en disposent. Une suite de logiciels espions attribuée aux services de renseignement français a d'ailleurs été découverte notamment en Iran[22].

3.2.5 Risque et prévention

Personne ne sait combien d'ordinateurs sont infectés par des logiciels malveillants, mais certaines personnes estiment que c'est le cas pour 20 à 50 % des ordinateurs Windows[23]. Il est donc fort probable d'en trouver sur l'un des Windows que l'on croisera. Jusqu'à présent, utiliser un système d'exploitation minoritaire (tel que GNU/-Linux) diminue significativement les risques d'infection car ceux-ci sont moins visés, le développement de *malwares* spécifiques étant économiquement moins rentable.

Voici quelques moyens de limiter les risques :

- n'installer (ou n'utiliser) aucun logiciel de provenance inconnue : ne pas faire confiance au premier site web venu[24] ;
- tenir compte des avertissements des systèmes d'exploitation qui jugent un logiciel peu sûr, ou qui indiquent qu'une mise à jour de sécurité est nécessaire ;
- enfin, réduire les possibilités d'installation de nouveaux logiciels : en limitant l'utilisation du compte d'administration et le nombre de personnes y ayant accès.

3.3 Les matériels espions

page 32

Les adversaires voulant mettre la main sur les secrets contenus dans nos ordinateurs peuvent utiliser des logiciels malveillants comme on vient de le voir, mais peuvent tout aussi bien utiliser du matériel espion. Ces gadgets n'ont rien à envier à ceux de James Bond !

Il existe toute une gamme de matériel plus ou moins facilement disponible permettant l'intrusion ou l'exfiltration d'informations d'un ordinateur, à quasiment tous les niveaux. Suite à la publication de documents confidentiels de la NSA *via* Edward Snowden, un véritable catalogue d'espionnage informatique a été publié sur le journal allemand *Der Spiegel*[25].

---

21. Andréa Fradin, 2016, *« Pegasus », l'arme d'une firme israélienne fantôme qui fait trembler Apple* [https://www.nouvelobs.com/rue89/rue89-surveillance/20160826.RUE3689/pegasus-l-arme-d-une-firme-israelienne-fantome-qui-fait-trembler-apple.html].
22. Martin Untersinger, 2015, *Dino, le nouveau programme-espion développé par des francophones*, Le Monde.fr [https://www.lemonde.fr/pixels/article/2015/06/30/dino-le-nouveau-programme-espion-developpe-par-des-francophones_4664675_4408996.html].
23. SafetyDetectives, 2021, *Statistiques et tendances : antivirus et cybersécurité 2021* [https://fr.safetydetectives.com/blog/antivirus-statistics-fr/#review-4].
24. Ce conseil vaut tout autant pour les personnes utilisant GNU/Linux. En décembre 2009, le site *gnome-look.org* a diffusé un *malware* [https://lwn.net/Articles/367874/] (en anglais) présenté comme un économiseur d'écran. Ce dernier était téléchargeable sous forme de paquet Debian au milieu d'autres économiseurs et de fonds d'écran.
25. Der Spiegel, 2013, *Interactive Graphic : The NSA's Spy Catalog* [https://www.spiegel.de/international/world/a-941262.html] (en anglais).

Sans en faire un tour exhaustif, on peut découvrir pêle-mêle dans ce catalogue de faux connecteurs USB, permettant de retransmettre sous forme d'ondes radio ce qui transite par ces mêmes connecteurs, des minuscules puces installées dans les câbles reliant écran ou clavier à l'ordinateur et faisant de même, pour que des adversaires puissent capter ce qu'on tape ou voient tout en étant à bonne distance. Enfin, pléthore de matériel espion installé dans l'ordinateur, que ce soit au niveau du disque dur, des microprogrammes, *etc.*

page 20

Le tableau n'est pas très encourageant : la vérification méticuleuse de son ordinateur demanderait de démonter celui-ci avec très peu de chance de le remonter de telle manière qu'il puisse fonctionner de nouveau. Une réponse peut être de garder son ordinateur sur soi ou dans un endroit qu'on considère comme sûr. Cela dit, l'ensemble de ce matériel n'est pas à la disposition de tous types d'adversaires. De plus, rien n'indique que l'usage d'un tel matériel est devenu monnaie courante, que ce soit pour des raisons de coût, d'installation, ou autres paramètres.

Nous allons quand même nous attarder un peu sur le cas des *keyloggers*, qui peuvent entrer à la fois dans la catégorie du matériel espion et des logiciels malveillants.

3.4 Les keyloggers, ou enregistreurs de frappe au clavier

Les enregistreurs de frappe au clavier (*keyloggers*), qui peuvent être « matériels » ou « logiciels », ont pour fonction d'enregistrer furtivement tout ce qui est tapé sur un clavier d'ordinateur, afin de pouvoir transmettre ces données à l'agence ou à la personne qui les a installés [26].

Une fois mis en place, leur capacité à enregistrer touche par touche ce qui est tapé sur un clavier contourne donc tout dispositif de chiffrement, et permet d'avoir directement accès aux phrases, mots de passe et autres données sensibles.

page 47

Les *keyloggers* matériels sont des dispositifs reliés au clavier ou à l'ordinateur. Ils peuvent ressembler à des adaptateurs, à des cartes d'extension à l'intérieur de l'ordinateur (*PCIe* ou *mini PCIe*) et même s'intégrer à l'intérieur du clavier [27]. Ils sont donc difficiles à repérer si on ne les recherche pas spécifiquement…

Pour un clavier sans fil, il n'y a même pas besoin de *keylogger* pour récupérer les touches entrées : il suffit de capter les ondes émises par le clavier pour communiquer avec le récepteur, puis de casser le chiffrement utilisé, qui est assez faible dans la plupart des cas [28]. À moindre distance, il est aussi toujours possible d'enregistrer et de décoder les ondes électromagnétiques émises par les claviers avec un fil, y compris ceux qui sont intégrés dans un ordinateur portable…

page 21

Les *keyloggers* logiciels sont beaucoup plus répandus, parce qu'ils peuvent être installés à distance (*via* un réseau, par le biais d'un logiciel malveillant, ou autre), et ne nécessitent généralement pas un accès physique à la machine pour la récupération des données collectées (l'envoi peut par exemple se faire périodiquement par email). La plupart de ces logiciels enregistrent également le nom de l'application en cours, la date et l'heure à laquelle elle a été exécutée ainsi que les frappes de touches associées à cette application.

Un *keylogger* logiciel a ainsi été utilisé par la police italienne en 2012 lors d'une enquête sur une radio anarchiste [29]. Un policier états-unien a été condamné pour avoir installé

26. Electronic Frontier Foundation, 2021, *Enregistreur de frappe* [https://ssd.eff.org/fr/glossary/enregistreur-de-frappe].

27. Nombre de modèles sont en vente libre, par exemple : un adaptateur USB [https://web.archive.org/web/20210611153039/https://www.ebay.fr/itm/224463276889?hash=item34430dcb59%3Ag%3Ay8QAAOSwFpddVMrk] ou une puce à mettre dans un clavier [https://web.archive.org/web/20210611153634/https://www.ebay.fr/itm/224463702020?hash=item3443144804%3Ag%3ARWgAAOSwQKdcrmjy].

28. Tom Espiner, 2007, *Microsoft wireless keyboard hacked from 50 metres* [https://www.zdnet.com/home-and-office/networking/microsoft-wireless-keyboard-hacked-from-50-metres/] (en anglais).

29. Croce Nera Anarchica, 2018, *Resoconto udienze Scripta Manent aprile-luglio* [https://www.autistici.org/cna/2018/09/13/resoconto-udienze-scripta-manent-aprile-luglio/] (en italien).

un *keylogger* sur l'ordinateur professionnel de son épouse, qui travaillait au palais de justice[30].

La seule manière de repérer les *keyloggers* matériels est de se familiariser avec ces dispositifs et de faire régulièrement une vérification visuelle de sa machine, à l'intérieur et à l'extérieur. Même si le catalogue de la NSA publié fin 2013 rend compte de la difficulté de trouver soi-même des dispositifs d'enregistrement de frappe à peine plus gros qu'un ongle. Pour les *keyloggers* logiciels, les pistes sont les mêmes que pour les autres *logiciels malveillants*.

page 32

3.5 Les plateformes d'investigation numérique

Les flics disposent de matériels et de logiciels spécifiques pour extraire et analyser le contenu des disques, clés USB ou autres cartes SD, mais aussi le contenu de la mémoire vive[31] des ordinateurs en fonctionnement. Ils sont fournis par des sociétés spécialisées dans l'investigation numérique[32]. Leurs logiciels permettent par exemple de générer un résumé graphique de l'utilisation d'un ordinateur, de faire des recherches par mots clés, de restaurer des données effacées ou encore de craquer des mots de passe. De telles plateformes existent aussi pour les smartphones[33].

page 18

page 42

3.6 Des problèmes d'impression ?

On croyait avoir fait le tour des surprises que nous réservent nos ordinateurs… mais même les imprimantes se mettent à avoir leurs petits secrets.

3.6.1 Un peu de stéganographie

Première chose à savoir : de nombreuses imprimantes haut de gamme signent leur travail[34]. Cette signature stéganographique[35], baptisée *watermarking*, repose sur de très légers détails d'impression, souvent invisibles à l'œil nu, et insérés dans chaque document. Ils permettent d'identifier de manière certaine la marque, le modèle et dans certains cas le numéro de série de la machine qui a servi à imprimer un document. On dit bien « de manière certaine », car c'est pour cela que ces détails sont là : retrouver la machine à partir de ses travaux.

C'est d'ailleurs notamment ainsi que la personne ayant diffusé en juin 2017 des documents *top secret* de la *NSA* sur le piratage des élections des États-Unis de 2016 par des hackers russes a été retrouvée. Des marques de l'imprimante utilisée pour imprimer les documents confidentiels étaient toujours présentes lors de leur publication par le journal *The Intercept*[36].

Par ailleurs, d'autres types de traces liées à l'usure de la machine sont aussi laissées sur les documents — et ce avec toutes les imprimantes. Car avec l'âge, les têtes d'impression se décalent, de légères erreurs apparaissent, les pièces s'usent, et tout cela constitue au fur et à mesure une signature propre à l'imprimante. Tout comme la balistique permet d'identifier une arme à feu à partir d'une balle, il est possible

30. Jerome Vosgien, 2019, *Un policier installe un keylogger sur l'ordinateur de son épouse* [https://news.sophos.com/fr-fr/2014/01/13/policier-installe-keylogger-ordinateur-epouse/].

31. Cindy Casey, 2019, *RAM Analysis Memory Forensics* [https://www.bucks.edu/media/bcccmedialibrary/con-ed/itacademy/fos2019/Casey-RAM-Forensics-(1).pdf] (en anglais).

32. Wikipédia, 2021, *Informatique légale* [https://fr.wikipedia.org/wiki/Informatique_l%C3%A9gale].

33. Wikipédia, 2021, *Cellebrite* [https://fr.wikipedia.org/wiki/Cellebrite].

34. L'*Electronic Frontier Foundation* tente de maintenir une liste des constructeurs et de ces modèles d'imprimantes indiscrets [https://www.eff.org/pages/list-printers-which-do-or-do-not-display-tracking-dots] (en anglais).

35. Pour en savoir plus sur la stéganographie, nous conseillons la lecture de cet article Wikipédia, 2014, *Stéganographie* [https://fr.wikipedia.org/wiki/St%C3%A9ganographie].

36. Robert Graham, 2017, *How The Intercept Outed Reality Winner* [https://blog.erratasec.com/2017/06/how-intercept-outed-reality-winner.html] (en anglais).

d'utiliser ces défauts pour identifier une imprimante à partir d'une page qui en est sortie.

Pour se protéger en partie de cela, il est intéressant de savoir que les détails d'impression ne résistent pas à la photocopie répétée : photocopier la page imprimée, puis photocopier la photocopie obtenue, suffit à faire disparaître de telles signatures. Par contre... on en laissera sûrement d'autres, les photocopieuses présentant des défauts, et parfois des signatures stéganographiques, similaires à celles des imprimantes. Bref on tourne en rond, et le problème devient surtout de choisir *quelles* traces on veut laisser...

3.6.2 La mémoire, encore...

Certaines imprimantes sont suffisamment « évoluées » pour être plus proches d'un véritable ordinateur que d'un tampon encreur.

Elles peuvent poser des problèmes à un autre niveau, vu qu'elles sont dotées d'une mémoire vive : celle-ci, tout comme celle du PC, gardera la trace des documents qui ont été traités aussi longtemps que la machine est sous tension... ou jusqu'à ce qu'un autre document les recouvre. page 18

La plupart des imprimantes laser disposent d'une mémoire vive pouvant contenir une dizaine de pages. Les modèles plus récents ou ceux comportant des scanners intégrés peuvent, quant à eux, contenir plusieurs milliers de pages de texte...

Pire encore : certains modèles, souvent utilisés pour les gros tirages comme dans les centres de photocopies, disposent parfois de disques durs internes, auxquels l'utilisatrice n'a pas accès, et qui gardent eux aussi des traces — et cette fois, même après la mise hors tension. page 18

Chapitre 4

Quelques illusions de sécurité

Bien. On commence à avoir fait le tour des traces que nous pouvons laisser involontairement, et des informations que des personnes mal intentionnées pourraient récupérer.

Il reste maintenant à pourfendre quelques idées reçues.

4.1 Logiciels propriétaires, open source, libres

On a vu qu'un logiciel peut faire plein de choses qu'on n'a pas du tout envie qu'il fasse. Dès lors, il est indispensable de faire ce que l'on peut pour réduire ce problème. De ce point de vue, les logiciels libres sont dignes d'une confiance bien plus grande que les logiciels dits « propriétaires » : nous allons voir pourquoi.

4.1.1 La métaphore du gâteau

Pour comprendre la différence entre logiciels libres et propriétaires, on utilise souvent la métaphore du gâteau. Pour faire un gâteau, il faut une recette : il s'agit d'une liste d'instructions à suivre, d'ingrédients à utiliser et d'un procédé de transformation à effectuer. De la même façon, la recette d'un logiciel est appelée « code source ». Elle est écrite dans un langage fait pour être compréhensible par des êtres humains. Cette recette est ensuite transformée en un code compréhensible par le processeur, un peu comme la cuisson d'un gâteau nous donne ensuite la possibilité de le manger.

page 16

Les logiciels propriétaires ne sont disponibles que « prêts à consommer », comme un gâteau industriel, sans sa recette. Il est donc très difficile de connaître ses ingrédients : c'est faisable, mais le processus est long et compliqué. Au demeurant, relire une série de plusieurs millions d'additions, de soustractions, de lectures et d'écritures en mémoire, pour en reconstituer le but et le fonctionnement est loin d'être la première chose que l'on souhaite faire sur un ordinateur.

Les logiciels libres, au contraire, sont livrés avec leur recette pour quiconque veut comprendre ou modifier le fonctionnement du programme. Il est donc plus facile de savoir ce qu'on donne à manger à notre processeur, et donc ce qu'il va advenir de nos données.

4.1.2 Les logiciels propriétaires : une confiance aveugle

Un logiciel « propriétaire » est donc un peu comme une boîte étanche : on peut constater que le logiciel fait ce qu'on lui demande, possède une belle interface graphique, *etc.* Mais on ne peut pas vraiment connaître en détail comment il procède. On ne sait pas s'il se cantonne à faire ce qu'on lui demande, ou s'il fait d'autres choses en plus. Pour le savoir, il faudrait pouvoir étudier son fonctionnement, ce qui est difficile à faire sans son code source… il ne nous reste donc qu'à lui faire *aveuglément* confiance.

Windows et macOS, les premiers, sont d'immenses boîtes hermétiquement fermées dans lesquelles sont installées d'autres boîtes tout aussi hermétiques (de Microsoft Office aux anti-virus…) qui font peut-être bien d'autres choses que celles qu'on leur demande.

Notamment, elles peuvent fournir des informations que ces logiciels grapilleraient sur nous ou même permettre d'accéder à l'intérieur de l'ordinateur. Par exemple avec des *backdoors* ou « portes dérobées » [1] incluses dans le logiciel, que les personnes en ayant la clé pourraient utiliser pour pirater notre ordinateur. Comme il n'est pas possible de savoir comment est écrit le système d'exploitation, tout est imaginable en la matière.

Dès lors, faire reposer la confidentialité et l'intégrité de nos données sur des programmes auxquels on est obligée d'accorder sa confiance les yeux fermés est une illusion de sécurité. Et installer d'autres logiciels prétendant sur leur emballage veiller à cette sécurité à notre place, alors que leur fonctionnement n'est pas plus transparent, ne peut pas résoudre ce problème.

4.1.3 L'avantage d'avoir la recette : les logiciels libres

La confiance plus grande qu'on peut avoir dans un système *libre* comme GNU/Linux est principalement liée au fait de disposer de la « recette » qui permet de le fabriquer. Gardons en tête quand même qu'il n'y a rien de magique : les logiciels libres ne jettent aucun « sort de protection » sur nos ordinateurs.

Toutefois, GNU/Linux offre davantage de possibilités pour rendre un peu plus sûr l'usage des ordinateurs, notamment en permettant de configurer assez finement le système. Cela implique trop souvent des savoir-faire relativement spécialisés, mais au moins c'est possible.

Par ailleurs, le mode de production des logiciels libres est peu compatible avec l'introduction de portes dérobées : c'est un mode de production collectif, plutôt ouvert et transparent, auquel participent des gens assez variés. Il n'est donc pas facile pour des personnes mal intentionnées d'y introduire des accès secrets en toute discrétion.

Il faut toutefois se méfier des logiciels qualifiés d'*open source*. Ces derniers donnent eux aussi accès à leur « recette », mais ont des modes de développement plus fermés, plus opaques. La modification et la redistribution de ces logiciels est au pire interdite, au mieux autorisée formellement mais rendue très pénible en pratique. Comme seule l'équipe à l'origine d'un logiciel va pouvoir participer à son développement, on peut considérer qu'en pratique personne ne lira en détail son code source… et donc que personne ne vérifiera vraiment son fonctionnement.

C'est le cas par exemple de TrueCrypt, dont le développement s'est arrêté en mai 2014. Il s'agissait d'un logiciel de chiffrement dont le code source était disponible, mais dont le développement était fermé et dont la licence restreignait la modification et la redistribution. Pour ce qui nous occupe, le fait qu'un logiciel soit *open source* doit plutôt être considéré comme un argument commercial que comme un gage de confiance.

Sauf que… la distinction entre logiciels libres et *open source* est de plus en plus floue : des personnes employées par Intel, Google et compagnie, écrivent de grosses parties des logiciels libres les plus importants, et on ne va pas toujours regarder de près ce qu'elles écrivent. Par exemple, voici les statistiques des organisations employant les gens qui développent le noyau Linux (qui est libre). Elles sont exprimées en pourcentage du nombre total de lignes de code source modifiées sur une période donnée[2] :

1. Au sujet des « portes dérobées », voir l'article Wikipédia, 2014, *Porte dérobée* [https://fr.wikipedia.org/wiki/Porte_d%C3%A9rob%C3%A9e].
2. Jonathan Corbet, 2021, *Some 5.12 development statistics*, Linux Weekly News [https://lwn.net/Articles/853039/] (en anglais).

Organisation	Pourcentage
Linaro	17,4 %
Intel	11,5 %
Red Hat	5,5 %
Google	4,2 %
(Inconnue)	4,2 %
NVIDIA	4,1 %
(Aucune)	3,8 %
Realtek	3,3 %
SUSE	2,9 %
MediaTek	2,9 %
Arm	2,3 %
Marvell	2,2 %
AMD	2,1 %
Pengutronix	2,0 %
etc.	

Alors il n'est pas impossible qu'une personne qui a écrit une partie du logiciel dans un coin, et à qui la « communauté du libre » fait confiance, ait pu y intégrer des bouts de code malveillants. La NSA (une agence de renseignement états-unienne) a ainsi pu créer et faire valider un standard cryptographique dans lequel se trouvait une faille lui permettant de contourner le chiffrement de certains protocoles sécurisés[3].

page 47

Si on utilise uniquement des logiciels libres livrés par une distribution GNU/Linux non commerciale telle que Debian ou Tails, il y a peu de chances que ce cas se présente, mais c'est une possibilité. On fait alors confiance aux personnes travaillant sur la distribution pour étudier le fonctionnement des programmes qui y sont intégrés.

Néanmoins, cette confiance ne peut valoir que si on reste vigilante à ce que l'on installe sur notre système. Par exemple, sur Debian, les paquets officiels de la distribution sont « signés », ce qui permet de vérifier leur provenance. Mais si on installe des paquets ou des extensions pour Firefox trouvées sur Internet sans les vérifier, on s'expose à tous les risques mentionnés au sujet des logiciels malveillants.

page 32

En guise de conclusion : *libre ou pas, il n'existe pas de logiciel pouvant, à lui seul, assurer l'intimité de nos données*; pour ce faire, il n'existe que des pratiques, associées à l'utilisation de certains logiciels. Logiciels choisis parce que des éléments nous permettent de leur accorder un certain niveau de confiance.

4.2 Le mot de passe d'un compte ne protège pas ses données

Tous les systèmes d'exploitation récents (Windows, macOS, GNU/Linux, *etc.*) offrent la possibilité d'avoir différents comptes utilisateur ou utilisatrice sur un même ordinateur. Mais il faut savoir que les mots de passe qui protègent parfois ces comptes ne garantissent pas du tout la confidentialité des données.

Certes, il peut être pratique d'avoir son espace à soi, avec ses propres réglages (marque-pages, fond d'écran, *etc.*), mais une personne qui souhaiterait avoir accès à toutes les données qu'il y a sur l'ordinateur n'aurait aucun mal à y parvenir : en rebranchant le disque dur sur un autre ordinateur ou en le démarrant sur un autre système d'exploitation elle aurait accès à toutes les données écrites sur ce disque dur.

page 22

Aussi, si utiliser des comptes séparés et des mots de passe peut avoir quelques avantages (comme la possibilité de verrouiller l'écran quand on s'éloigne quelques minutes), il est nécessaire de garder en tête que cela ne protège pas réellement nos données.

3. Julien Lausson, 2013, *La NSA est suspectée d'avoir altéré un standard cryptographique* [https://www.numerama.com/politique/26979-la-nsa-est-suspectee-d-avoir-altere-un-standard-cryptographique.html].

4.3 À propos de l'« effacement » des fichiers

page 24

On a déjà évoqué que le contenu d'un fichier devenu inaccessible ou invisible ne s'était pas pour autant volatilisé. On va maintenant détailler pourquoi.

4.3.1 La suppression d'un fichier n'en supprime pas le contenu...

... et ça peut être très facile de le retrouver.

En effet, lorsqu'on « supprime » un fichier en le plaçant dans la *Corbeille* puis en la vidant, on ne fait que dire au système d'exploitation que le contenu de ce fichier ne nous intéresse plus. Il supprime alors son entrée dans l'index des fichiers existants. Et il a ensuite le loisir de réutiliser l'espace que prenaient ces données pour y inscrire autre chose.

Mais il faudra peut-être des semaines, des mois ou des années avant que cet espace soit *effectivement* utilisé pour de nouveaux fichiers, et que les anciennes données disparaissent réellement. En attendant, si on regarde directement ce qui est inscrit sur le disque dur, on retrouve le contenu des fichiers « supprimés ». C'est une manipulation assez simple, automatisée par de nombreux logiciels permettant de « récupérer » ou de « restaurer » des données[4].

4.3.2 Un début de solution : réécrire plusieurs fois par-dessus les données

Une fois que de nouvelles données sont réécrites sur l'espace d'un disque dur, il devient difficile de retrouver ce qui s'y trouvait auparavant. Mais cela n'est pas pour autant impossible : lorsque l'ordinateur réécrit `1` par-dessus `0`, cela donne plutôt `0,95` et lorsqu'il réécrit `1` par-dessus `1`, cela donne plutôt `1,05`[5]... un peu comme on peut lire sur un bloc-notes ce qui a été écrit sur une page arrachée, par les dépressions créées sur la page vierge située en dessous.

En revanche, cela devient très difficile, voire impossible, de les récupérer quand on réécrit plusieurs fois par-dessus avec des données aléatoires. La meilleure façon de rendre inaccessible le contenu de ces fichiers « supprimés » est donc d'utiliser des logiciels qui s'assurent de réécrire plusieurs fois par-dessus. C'est ce qu'on appelle « écraser des données » (*wipe* en anglais).

4.3.3 Quelques limites des possibilités de réécriture

Même s'il est possible de réécrire plusieurs fois à un endroit donné d'un disque dur pour rendre inaccessibles les données qu'il contenait, cela ne garantit pas pour autant leur disparition complète du disque.

Les disques « modernes »

Les disques actuels réorganisent leur contenu « intelligemment » : une partie du disque est reservée pour remplacer des endroits qui deviendraient défectueux. Ces opérations de remplacement sont difficilement détectables, et on ne peut donc jamais vraiment s'assurer que l'endroit sur lequel on réécrit est bien celui où le fichier « supprimé » était écrit initialement.

Pour les clés USB et les disques SSD (*Solid State Drive*), il est même sûr que, dans la plupart des cas, on réécrit à un endroit différent. La mémoire *flash*, utilisée par les clés USB et les disques SSD, arrête de fonctionner correctement après un certain nombre

4. C'est le cas de PhotoRec [https://www.cgsecurity.org/wiki/PhotoRec_FR] par exemple.

5. Peter Gutmann, 1996, *Secure Deletion of Data from Magnetic and Solid-State Memory* [https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html] (en anglais).

d'écritures[6], et ces derniers contiennent des puces chargées de réorganiser automatiquement leur contenu pour répartir les informations dans un maximum d'endroits différents.

En prenant en compte ces mécanismes, il devient difficile de garantir que les données que l'on souhaite détruire ont bien disparu.

Néanmoins, ouvrir un disque dur pour en examiner les entrailles demande du temps et d'importantes ressources matérielles et humaines. Cet investissement ne sera pas forcément à la portée de tout le monde, ni tout le temps.

Pour les puces de mémoire *flash* d'une clé USB ou d'un disque SSD, même si ce n'est pas non plus immédiat, l'opération est beaucoup plus simple : il suffit d'un fer à souder, et d'un appareil permettant de lire directement les puces de mémoire. Ces derniers peuvent être achetés pour environ 1 500 dollars[7].

Les systèmes de fichiers

Même si le contenu d'un fichier a été parfaitement supprimé, il peut en rester des traces ailleurs, qui peuvent être dues au système de fichiers.

page 27
page 24

En effet, les systèmes de fichiers actuels gardent une trace des modifications successives des fichiers dans un « journal ». Aussi, on dit que ces systèmes de fichiers sont « journalisés ».

page 29

La journalisation a été introduite pour améliorer la robustesse des systèmes de fichiers. Après une extinction brutale de l'ordinateur, cela permet au système de se contenter de reprendre les dernières opérations à effectuer, plutôt que de devoir parcourir l'intégralité du disque pour corriger les incohérences. Mais cela peut ajouter des traces à propos des fichiers que l'on souhaiterait voir disparaître.



Précision

Windows utilise les systèmes de fichiers NTFS et ReFS, qui sont journalisés. Sous GNU/-Linux, ext4 est le système de fichiers le plus souvent utilisé. Par défaut, il ne met dans le journal que les noms des fichiers et d'autres métadonnées, mais pas leur contenu.

Certains systèmes de fichiers ont d'autres fonctionnalités qui laissent des traces :

- les instantanés (*snapshots*) possibles avec les systèmes de fichiers modernes (NTFS, ReFS, Btrfs, *etc.*) ;
- la mise en cache dans des dossiers temporaires avec des systèmes de fichiers réseau (comme NFS) ;
- *etc.*

Ce qu'on ne sait pas

Pour ce qui est des CD-RW ou DVD±RW (ré-inscriptibles), il semble qu'aucune étude sérieuse n'ait été menée à propos de l'efficacité de la réécriture pour rendre des données irrécupérables. Les recommandations actuelles sont donc de détruire méthodiquement les supports de ce type qui auraient pu contenir des données à faire disparaître[8].

6. Wikipédia, 2020, *SSD* [https://fr.wikipedia.org/wiki/SSD].

7. Le PC-3000 Flash [https://www.acelab.eu.com/pc3000flash.php] est vendu comme un *outil professionnel de recouvrement de données sur des périphériques flash endommagés* (en anglais).

8. NIST, 2014, *Guidelines for Media Sanitization* [https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf] (en anglais).

4.3.4 Plein d'autres fois où l'on « efface »

Il faut noter qu'on ne supprime pas seulement des fichiers en les mettant à la *Corbeille*. Par exemple, quand on utilise l'option « Effacer mes traces » du navigateur Firefox, ce dernier ne fait pas mieux que de supprimer les fichiers. Certes les données sont devenues inaccessibles pour Firefox, mais elles sont toujours accessibles en regardant directement le disque dur.

Enfin, il est utile d'insister ici sur le fait que le *reformatage* d'un disque dur n'efface pas pour autant le contenu qui s'y trouvait. De même que la suppression des fichiers, cela ne fait que rendre disponible l'espace où se trouvait le contenu, mais les données restent physiquement présentes sur le disque tant qu'elles ne sont pas recouvertes. Tout comme détruire le catalogue d'une bibliothèque ne fait pas pour autant disparaître les livres présents dans les rayonnages.

On peut donc toujours retrouver des fichiers après un reformatage, aussi facilement que s'ils avaient été simplement « supprimés » [9].

4.3.5 Et pour ne laisser aucune trace ?

Malheureusement, il n'y a pas de méthode simple pour régler radicalement le problème. La solution la moins difficile pour l'instant est d'utiliser l'ordinateur après l'avoir démarré avec un système *live* configuré pour n'utiliser que la mémoire vive, comme Tails. Dans ce cas, il est possible de ne rien écrire sur le disque dur, ni sur le mémoire virtuelle (*swap*), et de ne garder les informations que dans la mémoire vive (donc uniquement tant que l'ordinateur reste allumé).

page 113
page 25

4.4 Les logiciels portables : une fausse solution

Ce que l'on appelle « logiciels portables », ce sont des logiciels qui ne sont pas installés sur un système d'exploitation donné, mais que l'on peut démarrer depuis une clé USB ou un disque dur externe — et donc, transporter avec soi afin d'en disposer sur n'importe quel ordinateur.

Toutefois, contrairement aux systèmes *live*, ces logiciels se servent du système d'exploitation installé sur l'ordinateur où on les utilise (la plupart du temps, ils sont prévus pour Windows).

L'idée qui est à leur origine est de permettre d'avoir toujours les logiciels dont on a besoin sous la main et personnalisés à notre usage. Mais « transporter son bureau partout avec soi », n'est pas forcément la meilleure manière de préserver la confidentialité de nos données.

Disons-le tout de suite : ces logiciels ne protègent pas plus les personnes qui s'en servent que les logiciels « non portables ».

4.4.1 Principaux problèmes

Ces solutions « clé en main » posent donc quelques problèmes plutôt fâcheux.

Il restera des traces sur le disque dur

Si le logiciel a été rendu « portable » correctement, il ne devrait pas laisser de traces sur le disque dur de l'ordinateur sur lequel on l'utilise. Mais dans les faits, le logiciel n'a jamais un contrôle absolu. Il dépend en effet largement du système d'exploitation sur lequel il est employé, qui peut avoir besoin d'écrire de la mémoire virtuelle (*swap*) sur le disque dur, ou d'enregistrer diverses traces de ce qu'il fait dans ses journaux et autres « documents récents ». Tout cela restera ensuite sur le disque dur.

page 28
page 29

9. PhotoRec [https://www.cgsecurity.org/wiki/PhotoRec_FR] propose aussi ce genre de fonctionnalité.

Il n'y a aucune raison d'avoir confiance en un système inconnu

On a vu auparavant que beaucoup de systèmes ne font absolument pas ce que l'on croit. Or, puisque le logiciel portable va utiliser le système installé sur l'ordinateur sur lequel on le lance, on souffrira de tous les mouchards et autres logiciels malveillants qui pourraient s'y trouver.

page 31

On ne sait pas qui les a compilés, ni comment

Les modifications apportées aux logiciels pour les rendre portables sont rarement vérifiées, alors qu'elles ne sont généralement pas faites par les autrices du logiciel elles-même. Dès lors, on peut soupçonner ces logiciels, encore plus que leurs versions non portables, de contenir des failles de sécurité, qu'elles aient été introduites par erreur ou volontairement.

Par ailleurs, on traitera plus loin des critères à prendre en considération lors du choix des logiciels que l'on installe ou télécharge.

Chapitre 5

Une piste pour protéger des données : la cryptographie

La *cryptographie* est la branche des mathématiques qui s'occupe spécifiquement de protéger des messages. Jusqu'en 1999, l'usage de techniques cryptographiques était interdit au grand public. C'est devenu légal entre autres pour permettre aux services marchands sur Internet de se faire payer sans que les clientes se fassent piquer leur numéro de carte bancaire.

La *cryptanalyse* est le domaine consistant à « casser » les techniques cryptographiques, par exemple pour permettre de retrouver un message qui avait été protégé[1].

Lorsque l'on veut protéger des messages, on distingue trois aspects :

- **confidentialité** : empêcher les regards indiscrets ;
- **authenticité** : s'assurer de la source du message ;
- **intégrité** : s'assurer que le message n'a pas subi de modifications.

On peut désirer ces trois choses en même temps, mais on peut aussi vouloir seulement l'une ou l'autre. Une personne écrivant un message *confidentiel* peut souhaiter nier en être l'autrice (et donc qu'on ne puisse pas l'*authentifier*). On peut aussi imaginer vouloir certifier la provenance (l'*authenticité*) et l'*intégrité* d'un communiqué officiel qui sera diffusé publiquement (donc loin d'être *confidentiel*).

Dans tout ce qui suit, on va parler de *messages*, mais les techniques cryptographiques s'appliquent de fait à n'importe quels nombres, donc à n'importe quelles données, une fois numérisées.

À noter, la cryptographie ne cherche pas à cacher les messages, mais à les protéger. Pour cacher des messages, il est nécessaire d'avoir recours à des techniques stéganographiques (comme celles utilisées par les imprimantes évoquées auparavant, ou encore au chiffrement répudiable), que nous ne développerons pas ici.

page 36
page 52

5.1 Protéger des données des regards indiscrets

Le chiffrement est la piste la plus sérieuse pour que des données ne puissent être comprises que par les personnes « dans le secret ». Les enfants qui utilisent des codes pour s'échanger des mots ou les militaires qui communiquent leurs ordres l'ont d'ailleurs très bien compris !

Le chiffrement d'un fichier ou d'un support de stockage permet de le rendre illisible pour toute personne qui n'a pas le code d'accès (souvent une *phrase de passe*). Il sera

1. Pour un bon aperçu des différentes méthodes — qu'on appelle des « attaques » — couramment utilisées en cryptanalyse, on peut se référer à la page Wikipédia, 2020, *Cryptanalyse* [https://fr.wikipedia.org/wiki/Cryptanalyse].

certes toujours possible d'accéder au contenu, mais les données ressembleront à une série de nombres aléatoires, et seront donc incompréhensibles et inutilisables.

Souvent on dit *crypter* et *décrypter* à la place de *chiffrer* et *déchiffrer*, ce qui peut prêter à confusion. On préfèrera cependant éviter l'emploi de l'anglicisme *crypter*, et réserver *décrypter* à l'opération consistant à déjouer un système de chiffrement (c'est-à-dire consistant à « déchiffrer » un message sans connaître le code secret de chiffrement).

5.1.1 Comment ça marche ?

Grosso modo, il y a seulement trois grandes idées pour comprendre comment on peut chiffrer des messages[2].

La première idée : la *confusion*. Il faut obscurcir la relation entre le message original (*en clair*, c'est-à-dire non chiffré) et le message chiffré. Un exemple très simple est le « chiffre de César », qui consiste à décaler chaque lettre du texte en clair de trois caractères dans l'alphabet :

texte en clair :	A	S S A U T		D A N S	U N E	H E U R E
	↓	↓ ↓ ↓ ↓ ↓		↓ ↓ ↓ ↓	↓ ↓ ↓	↓ ↓ ↓ ↓ ↓
texte chiffré :	D	V V D X W		G D Q V	X Q H	K H X U H

A + 3 lettres = D

Sauf qu'avec le chiffre de César, il est facile d'analyser la fréquence des lettres et de retrouver les mots.

Alors la deuxième grande idée, c'est la *diffusion*. Cela permet d'éclater le message pour le rendre plus difficile à reconnaître. Un exemple de cette technique, c'est la transposition par colonnes. Ainsi, pour une diffusion en trois points, on répartit le texte sur trois lignes puis on le retranscrit colonne par colonne :

1	2	3	4	5	6		1	2	3	4	5	6
A	S	S	A	U	T		A	S	S	A	U	T
D	A	N	S	U	R	diffusion en 3 points	D	A	N	S	U	R
E	H	E	U	R	E	⟶	E	H	E	U	R	E

Ce que l'on appelle *algorithmes de chiffrement*, ce sont les différentes techniques utilisées pour transformer le texte original. Quant à la *clé de chiffrement*, c'est, dans le cas du chiffre de César par exemple, le nombre de caractères de décalage (3, en l'occurrence) ou, dans la technique de diffusion, le nombre de lignes des colonnes. La valeur de cette clé est variable : on aurait tout aussi bien pu décider de faire des colonnes de 2 lignes, ou un décalage de 6 caractères.

Ce qui nous amène à la troisième grande idée : *le secret réside seulement dans la clé*. Après quelques millénaires, on a constaté que c'était une mauvaise idée de partir du principe que personne n'arriverait à comprendre l'algorithme de chiffrement : tôt ou tard, une personne finira bien par le découvrir. Il est en effet bien plus facile de garder secrète une simple clé de chiffrement ou une phrase de passe plutôt que tout un algorithme.

De nos jours, l'algorithme peut donc être détaillé en long, en large et en travers sur Wikipédia, permettant à n'importe qui de vérifier qu'il n'a pas de point faible particulier, c'est-à-dire que la seule solution pour déchiffrer un message chiffré sera de disposer de la *clé* qui a été employée avec celui-ci.

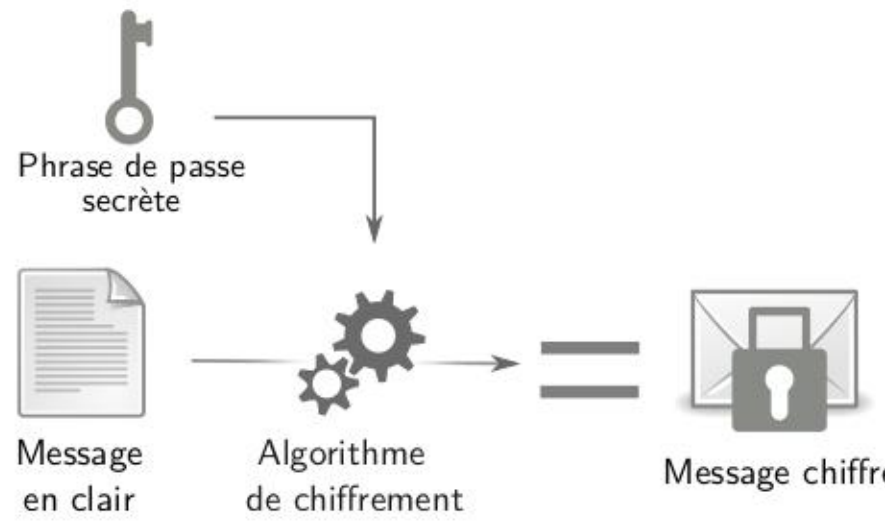
---

2. Le passage qui suit est une adaptation très partielle de la bande dessinée de Jeff Moser sur l'algorithme AES [https://www.moserware.com/2009/09/stick-figure-guide-to-advanced.html] (en anglais).

5.1.2 Vous voulez un dessin ?

Concrètement, pour assurer la *confidentialité* de nos données, on utilise deux opérations : le chiffrement, afin de protéger les données, puis le déchiffrement, afin de pouvoir les lire. Ces opérations sont assurées par un logiciel, par exemple GnuPG.

Première étape : le chiffrement



Chiffrement d'un texte en clair

Pour un exemple d'usage pratique, prenons le message suivant [3] :

```
Les spaghetti sont dans le placard.
```

Après avoir chiffré ce message en utilisant le logiciel GnuPG avec l'algorithme AES-256 et, comme phrase de passe, « *ceci est un secret* », on obtiendra par exemple [4] :

```
-----BEGIN PGP MESSAGE-----

jA0ECQMCRM0lmTSIONRg0lkBWGQI76cQOocEvdBhX6BM2AU6aYSPYymSqj8ihFXu
wV1GVraWuwEt4XnLc3F+OxT3EaXINMHdH9oydA92WDkaqPEnjsWQs/oSCeZ3WXoB
9mf9y6jzqozEHw==
=T6eN
-----END PGP MESSAGE-----
```

Voici donc l'aspect que prend un texte après chiffrement : son contenu est devenu parfaitement incompréhensible. Les données « en clair », lisibles par tout le monde, ont été transformées en un autre format, illisible pour qui ne possède pas la phrase de passe.

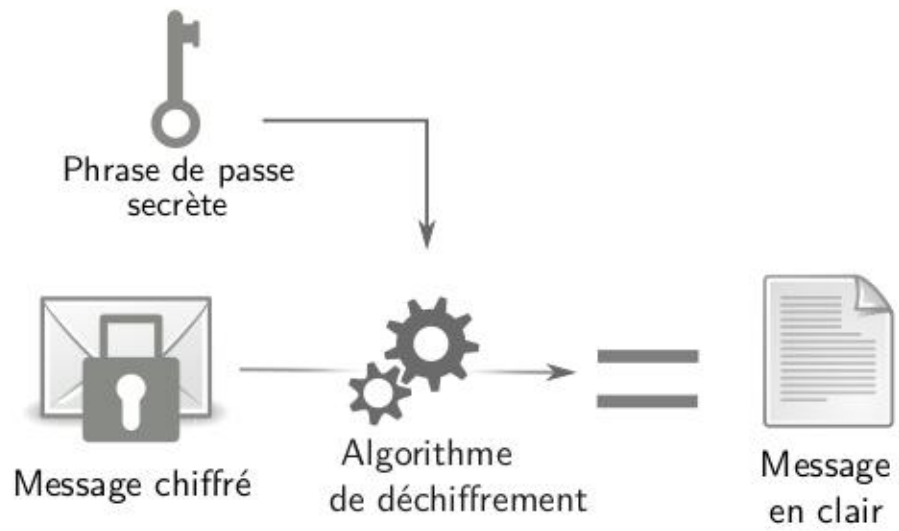
Deuxième étape : le déchiffrement

Pour le déchiffrement, il nous suffira d'utiliser de nouveau GnuPG, cette fois avec notre texte chiffré. GnuPG nous demandera la phrase de passe ayant servi à chiffrer notre message, et si cette dernière est correcte, on obtiendra enfin l'information qui nous manquait pour préparer le déjeuner.

---

3. Ce message est d'une très haute importance stratégique pour des personnes qu'on inviterait chez soi. Il est donc crucial de le chiffrer. Blague à part, si l'on ne chiffre que des messages « sensibles », tous les messages chiffrés que l'on envoie sont alors suspects ; d'où l'importance de chiffrer aussi des messages anodins.

4. Même si l'on chiffre le même message avec la même phrase de passe, le résultat est différent à chaque fois que l'on répète l'opération : afin d'empêcher quiconque de comparer des messages chiffrés (sans en connaître la phrase de passe) pour savoir s'ils correspondent ou non à un même message en clair, des données aléatoires sont introduites afin de rendre chaque message chiffré unique et distinct des autres.



Déchiffrement d'un texte chiffré

5.1.3 Pour un disque dur...

Si l'on souhaite que toutes les données que l'on met sur un support de stockage (disque dur, clé USB, *etc.*) soient chiffrées, il va falloir que le système d'exploitation se charge de réaliser « à la volée » les opérations de chiffrement et de déchiffrement.

Ainsi, chaque fois que des données devront être lues du disque dur, elles seront déchiffrées au passage afin que les logiciels qui en ont besoin puissent y accéder. À l'inverse, chaque fois qu'un logiciel demandera à écrire des données, elles seront chiffrées avant d'atterrir sur le disque dur.

page 18

Pour que ces opérations fonctionnent, il est nécessaire que la clé de chiffrement se trouve en mémoire vive aussi longtemps que le support aura besoin d'être utilisé.

Par ailleurs, la clé de chiffrement ne peut pas être changée. Une fois que cette dernière a servi à chiffrer des données inscrites sur le disque, elle devient indispensable pour pouvoir les relire. Pour pouvoir changer la clé, il faudrait donc relire puis réécrire l'intégralité des données du disque...

Pour éviter cette opération pénible, la plupart des systèmes utilisés pour chiffrer les supports de stockage ont donc une astuce : la clé de chiffrement est en fait un grand nombre aléatoire, qui est lui-même chiffré à l'aide d'une *phrase de passe*[5]. Cette version chiffrée de la clé de chiffrement est généralement inscrite sur le support de stockage au début du disque, en « *en-tête* » des données chiffrées.

Avec ce système, changer la phrase de passe devient simple, vu qu'il suffit de modifier cet *en-tête* (ce qui est généralement fait automatiquement par ces systèmes de chiffrement).

5.1.4 Résumé et limites

page 249

La cryptographie permet donc de bien protéger ses données[6], en chiffrant tout ou partie de son disque dur comme de tout autre support de stockage (clé USB, CD, *etc.*), ou de ses communications. De plus, les ordinateurs modernes sont suffisamment puissants pour que nous puissions faire du chiffrement une routine, plutôt que de le réserver à des circonstances spéciales ou à des informations particulièrement sensibles (sinon, cela identifie tout de suite ces dernières comme importantes, alors qu'il vaut mieux les dissoudre dans la masse).

---

5. Le système LUKS, utilisé sous GNU/Linux, permet même d'utiliser plusieurs versions chiffrées de la clé de chiffrement. Chacune de ces versions peut être chiffrée avec une *phrase de passe* différente, ce qui permet à plusieurs personnes d'accéder aux mêmes données sans pour autant avoir à retenir le même secret.

6. Un article de Rue89 sur les révélations de Snowden quant à l'impuissance de la NSA face au chiffrement : Marie Gutbub, 2014, *Crimes de guerre et décryptage de données : nouvelles révélations de Snowden* [https://www.nouvelobs.com/rue89/rue89-monde/20141229.RUE7224/crimes-de-guerre-et-decryptage-de-donnees-nouvelles-revelations-de-snowden.html].

On peut ainsi mettre en place une phrase de passe pour chiffrer tout un disque dur, et/ou donner à certaines personnes une partie chiffrée avec leur propre phrase de passe. Il est également possible de chiffrer individuellement tel ou tel fichier, ou un email, ou une pièce jointe, avec une phrase de passe encore différente.

Cependant, bien qu'il soit un outil puissant et essentiel pour la sécurité des informations, **le chiffrement a ses limites**, qu'il faut bien avoir à l'esprit lorsqu'on l'utilise.

Comme expliqué auparavant, lorsqu'on accède à des données chiffrées, il est nécessaire de garder deux choses en tête. Premièrement, une fois les données déchiffrées, ces dernières se trouvent *au minimum* dans la mémoire vive. Deuxièment, tant que des données doivent être chiffrées ou déchiffrées, la mémoire vive contient également la *clé de chiffrement*.

Toute personne qui dispose de la clé de chiffrement pourra lire *tout ce qui a été chiffré avec*, et pourra aussi s'en servir pour chiffrer elle-même des données.

Il faut donc faire attention aux éléments suivants :

- Le système d'exploitation et les logiciels ont accès aux données et à la clé de chiffrement autant que nous, alors cela dépend de la confiance qu'on met en eux — il s'agit donc de n'installer que des logiciels en lesquels on a confiance. page 32
- Quiconque obtient un accès physique à l'ordinateur allumé a, de fait, accès au contenu de la mémoire vive. Lorsqu'un disque chiffré est activé, celle-ci contient, en clair, les données sur lesquelles on a travaillé depuis l'allumage de l'ordinateur (même si elles sont chiffrées sur le disque). Mais elle contient surtout, comme écrit plus haut, la clé de chiffrement, qui peut donc être recopiée. Il vaut donc mieux prendre l'habitude d'éteindre les ordinateurs et de désactiver (démonter, éjecter) les disques chiffrés quand on ne s'en sert pas. page 27
- Dans certains cas, il peut être nécessaire de prévoir des solutions matérielles pour pouvoir couper le courant facilement et rapidement[7] ; ainsi les disques chiffrés redeviennent inaccessibles sans la phrase de passe — à moins d'effectuer une *cold boot attack*. page 27
- Il reste également possible qu'un enregistreur de frappe ait été installé sur l'ordinateur, et que celui-ci enregistre la phrase de passe. page 35

Aussi, les mathématiques utilisées dans les algorithmes cryptographiques ont parfois des défauts. Et beaucoup plus souvent encore, les logiciels qui les appliquent comportent des faiblesses ou des erreurs. Certains de ces problèmes peuvent, du jour au lendemain, rendre décryptables en quelques clics des données chiffrées avec ce que l'on pensait être la meilleure des protections[8]…

Par ailleurs, une certaine **limite « légale »** vient s'ajouter aux possibles attaques. En France, toute personne qui chiffre ses données est en effet censée donner le code d'accès aux autorités judiciaires lorsqu'elles le demandent, comme l'explique l'article 434-15-2 du Code pénal[9] :



> Est puni de trois ans d'emprisonnement et de 270 000 € d'amende le fait, pour quiconque ayant connaissance de la convention secrète de déchiffrement d'un moyen de cryptologie susceptible d'avoir été utilisé pour préparer, faciliter ou commettre un crime ou un délit, de refuser de remettre ladite convention aux autorités judiciaires ou de la mettre en œuvre, sur les réquisitions de ces autorités délivrées en application des titres II et III du livre I^{er} du code de procédure pénale.

7. Pour cette raison, il peut être recommandé de ne pas laisser la batterie branchée dans un ordinateur portable quand elle n'est pas utilisée. Il suffit alors d'enlever le câble secteur pour l'éteindre.

8. Le blog de Zythom, 2015, *Le disque dur chiffré* [https://zythom.fr/2015/03/le-disque-dur-chiffre/].

9. Le terme légal est « cryptologie ». Une recherche sur ce mot sur Légifrance [https://www.legifrance.gouv.fr] donnera une liste exhaustive des textes de loi concernant ce domaine.

> Si le refus est opposé alors que la remise ou la mise en œuvre de la convention aurait permis d'éviter la commission d'un crime ou d'un délit ou d'en limiter les effets, la peine est portée à cinq ans d'emprisonnement et à 450 000 € d'amende [10].

À noter là-dedans : « *susceptible* » et « *sur les réquisitions* », c'est-à-dire que la loi est assez floue pour permettre d'exiger de toute personne détentrice de données chiffrées qu'elle crache le morceau. On peut éventuellement se voir demander la phrase de passe d'un support qui ne serait pas le nôtre… et que nous n'aurions donc pas. Pour autant, la police, même en la personne d'une OPJ [11], doit avoir préalablement obtenu l'autorisation d'une magistrate [12]. De l'autre côté de la Manche, une législation douanière similaire fait planer un risque de prison ferme pour Muhammad Rabbani, directeur de l'organisation CAGE, pour avoir refusé de livrer ses mots de passe à la frontière [13].

Contrairement aux attentes de nombreuses personnes [14] [15], la justice a rejeté l'argument du « droit à ne pas s'auto-incriminer » pour se défendre de ne pas donner sa convention de déchiffrement. Elle a argué que « ces données, déjà fixées sur un support, existent indépendamment de la volonté de la personne suspectée » [16]. De plus, la Chambre criminelle de la Cour de cassation a statué « que le code de déverrouillage d'un téléphone mobile peut constituer une clé de déchiffrement, si ce téléphone est équipé d'un moyen de cryptologie » [17].

Certaines techniques permettent aussi de combiner chiffrement et stéganographie afin de rendre indétectable la présence de données chiffrées : on parle alors de « chiffrement répudiable », de « déni plausible » [18], ou de « *deniable encryption* » en anglais. Certains logiciels comme VeraCrypt [19] proposent cette fonctionnalité, qui permettrait en théorie de nier à l'autorité judiciaire l'existence de données chiffrées, et donc d'éviter de se retrouver contrainte à en révéler la phrase de passe sous le coup de l'article 434-15-2. Néanmoins, la jurisprudence à ce sujet est pour l'instant inexistante, et l'utilisation d'un chiffrement répudiable n'exclut pas que la justice parvienne par d'autres moyens à démontrer l'existence de données chiffrées. La prudence reste donc de mise.

Depuis 2014 [20], les flics ont aussi le droit de réquisitionner n'importe qui susceptible « d'avoir connaissance des mesures appliquées pour protéger les données » et « de leur remettre les informations permettant d'accéder aux données » [21].

---

10. Légifrance, 2016, *Code pénal*, article 434-15-2 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032654251/2016-06-05/].
11. Officière de police judiciaire.
12. Les Numériques, 2020, *Refuser le déverrouillage de son smartphone à la police, une infraction dans certains cas* [https://www.lesnumeriques.com/telephone-portable/refuser-le-deverrouillage-de-son-smartphone-a-la-police-une-infraction-dans-certains-cas-n155755.html].
13. Birkbeck Law Review, 2018, *In Conversation with Muhammad Rabbani, CAGE* [https://web.archive.org/web/20211102115950/http://www.bbklr.org/blog/in-conversation-with-muhammad-rabbani-cage] (en anglais).
14. Maître Éolas, 2014, *Allô oui j'écoute* [https://www.maitre-eolas.fr/post/2014/03/08/All%C3%B4-oui-j-%C3%A9coute#c173067].
15. La Quadrature du Net, 2018, *Le Conseil constitutionnel restreint le droit au chiffrement* [https://www.laquadrature.net/2018/04/04/le-conseil-constitutionnel-restreint-le-droit-au-chiffrement/].
16. Conseil constitutionnel, 2018, *Décision n° 2018-696 QPC du 30 mars 2018* [https://www.conseil-constitutionnel.fr/decision/2018/2018696QPC.htm].
17. Légifrance, 2021, *Cour de cassation, criminelle, Chambre criminelle, 3 mars 2021, 19-86.757, Inédit* [https://www.legifrance.gouv.fr/juri/id/JURITEXT000043252997].
18. Wikipédia, 2020, *Déni plausible (cryptologie)* [https://fr.wikipedia.org/wiki/D%C3%A9ni_plausible_(cryptologie)].
19. Site officiel de VeraCrypt [https://www.veracrypt.fr/] (en anglais).
20. Légifrance, 2014, *Loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme* [https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000029754374].
21. Légifrance, *Code de procédure pénale*, article 57-1 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000032655328].

Néanmoins, des personnes refusent de donner leur convention de chiffrement et le revendiquent au nom du droit à garder le silence et à ne pas s'auto-incriminer[22], au même titre que d'autres refusent de donner leur ADN, ce qui est là aussi — dans une moindre mesure — pénalement répréhensible.

5.2 S'assurer de l'intégrité de données

Nous avons vu quelques pistes pour assurer la *confidentialité* de nos données. Toutefois, il peut être aussi important de pouvoir s'assurer de leur *intégrité*, c'est-à-dire de vérifier qu'elles n'ont pas subi de modifications en cours de route (par accident ou par malveillance, afin d'y introduire des mouchards, par exemple). On peut également vouloir s'assurer de la provenance de nos données, c'est-à-dire en assurer l'*authenticité*. page 32

5.2.1 La puissance du hachoir

L'essentiel des techniques pour assurer l'intégrité ou l'authenticité reposent sur des outils mathématiques que la cryptographie a baptisés « fonctions de hachage ».

Ces dernières fonctionnent comme des *hachoirs*, capables de réduire n'importe quoi en tout petits morceaux. Et si notre hachoir fonctionne suffisamment bien pour pouvoir être utilisé en cryptographie, on sait que :

- avec les petits morceaux, impossible de reconstituer l'objet original sans essayer tous les objets de la Terre ;
- le même objet, une fois passé au hachoir, donnera toujours les mêmes petits morceaux ;
- la probabilité que deux objets différents donnent exactement les mêmes petits morceaux est astronomiquement faible.

Lorsque ces propriétés sont réunies, il nous suffit alors de comparer les petits morceaux issus de deux objets pour savoir s'ils étaient identiques.

Les petits morceaux qui sortent de notre hachoir s'appellent plus couramment une *somme de contrôle* ou une *empreinte*. Elle est généralement écrite sous une forme qui ressemble à :

```
f9f5a68a721e3d10baca4d9751bb27f0ac35c7ba
```

Notre hachoir fonctionne avec des données de n'importe quelle taille et de n'importe quelle forme : on peut tout aussi bien réduire en petits morceaux — c'est-à-dire calculer leurs empreintes — une image, un CD, un logiciel, *etc.* Ainsi, par exemple, plutôt que de comparer directement le contenu de deux DVD octet par octet, ce qui risque d'être long et fastidieux, on pourra se contenter de comparer leurs empreintes pour déterminer s'ils sont identiques.

Notre hachoir n'est pas magique pour autant. On imagine tout de même bien qu'en réduisant n'importe quoi en petits cubes de taille identique, on peut se retrouver avec les mêmes petits cubes issus de deux objets différents. Cela s'appelle une *collision*. La probabilité que de tels carambolages mathématiques se produisent par hasard est heureusement astronomiquement faible, sauf lorsqu'il existe des algorithmes pour les provoquer… ce qui est déjà arrivé pour plusieurs fonctions de hachage après quelques années de recherche, comme pour la fonction SHA-1[23], par exemple. Dans ce cas, la troisième propriété du hachoir n'est plus respectée, et il faut donc cesser de l'utiliser.

22. Le Parisien, 2018, *Un gardé à vue peut garder le silence mais doit donner les codes de son smartphone* [https://www.leparisien.fr/faits-divers/un-garde-a-vue-peut-garder-le-silence-mais-doit-donner-les-codes-de-son-smartphone-16-04-2018-7667613.php].

23. Marc Stevens *et al.*, 2017, *Announcing the first SHA-1 collision*, Google Security Blog [https://security.googleblog.com/2017/02/announcing-first-sha1-collision.html] (en anglais).

5.2.2 Vérifier l'intégrité d'un logiciel

Prenons un exemple : Ana a écrit un programme et le distribue sur des CD, que l'on peut trouver dans des clubs d'utilisatrices de GNU/Linux. Bea a envie d'utiliser le programme d'Ana, mais se dit qu'il aurait été très facile pour une administration mal intentionnée de remplacer un des CD d'Ana par un logiciel malveillant.

Elle ne peut pas aller chercher un CD directement chez Ana, qui habite dans une autre ville. Par contre, elle a rencontré Ana il y a quelque temps, et connaît sa voix. Elle lui téléphone donc, et Ana lui donne la *somme de contrôle* du contenu du CD, qu'elle a calculée avec une fonction de hachage sûre :

CD d'Ana $\xrightarrow[\text{fonction de hachage}]{}$ `94d93910609f65475a189d178ca6a45f`
`22b50c95416affb1d8feb125dc3069d0`

Bea peut ensuite la comparer avec celle qu'elle génère à partir du CD qu'elle s'est procuré, en utilisant la même fonction de hachage :

CD de Bea $\xrightarrow[\text{fonction de hachage}]{}$ `94d93910609f65475a189d178ca6a45f`
`22b50c95416affb1d8feb125dc3069d0`

Comme les sommes de contrôle sont identiques, Bea est contente, elle est sûre de bien utiliser le même CD que celui fourni par Ana.

Calculer ces sommes de contrôle ne prend pas beaucoup plus de temps que la lecture complète du CD… soit quelques minutes tout au plus.

Maintenant, mettons-nous dans la peau de Carole, qui a été payée pour prendre le contrôle de l'ordinateur de Bea à son insu. Pour cela, elle veut créer un CD qui ressemble à celui d'Ana, mais qui contient un logiciel malveillant.

Carole commence donc par se procurer le CD original d'Ana. Ensuite, elle modifie ce CD pour y introduire le logiciel malveillant. Cette première version ressemble de très près à l'original. Cela pourrait duper plus d'une personne qui ne ferait pas attention, mais elle sait que Bea vérifiera la somme de contrôle du CD avant d'installer le programme qu'il contient.

Comme Ana utilise une fonction de hachage qui n'a pas de défauts connus, il ne reste à Carole qu'à essayer un très grand nombre de variations des données de son CD, cela dans l'espoir d'obtenir une *collision*, c'est-à-dire la même somme de contrôle que celle d'Ana.

Malheureusement pour elle, et heureusement pour Bea, même avec de très nombreux ordinateurs puissants et même en y passant un temps extrêmement long, les chances de réussite de Carole resteraient astronomiquement faibles[24].

Il suffit donc de se procurer une *empreinte*, ou *somme de contrôle*, par des intermédiaires de confiance pour vérifier l'*intégrité* de données. Tout l'enjeu est ensuite de se procurer ces empreintes par un moyen de confiance, c'est-à-dire de pouvoir vérifier leur *authenticité*…

---

24. Pour donner un ordre de grandeur de la chose, avec une fonction de hachage parmi celles actuellement considérées comme sûres (SHA-256, par exemple), même si Ana disposait d'un milliard de milliards d'ordinateurs, chacun capable de calculer dix milliards de sommes de contrôle par seconde, et qu'elle les faisait calculer pendant une durée équivalente à l'âge actuel de l'univers (quinze milliards d'années), elle serait encore *très loin* d'avoir une chance raisonnable de trouver une collision !

Par contre, cela ne tient pas compte d'éventuelles avancées futures en cryptanalyse qui pourraient découvrir des faiblesses dans la fonction de hachage utilisée et proposer des algorithmes plus efficaces pour permettre à Carole de réaliser son attaque dans un temps raisonnable.

5.2.3 Vérifier un mot de passe

Un autre exemple d'utilisation des fonctions de hachage concerne la vérification de l'*authenticité* d'une demande d'accès.

Si l'accès à un ordinateur est protégé par un mot de passe, comme par exemple l'ouverture d'une session sous GNU/Linux[25], il faut que l'ordinateur puisse vérifier que le mot de passe que l'on entre est le bon. Cependant, les mots de passe ne sont pas enregistrés en clair sur l'ordinateur, sinon il serait trop facile de les obtenir.

Mais alors comment l'ordinateur s'assure-t-il que le mot de passe tapé au clavier est exact ?

Lorsque l'on choisit un mot de passe pour son ordinateur, le système enregistre, grâce à une fonction de hachage, une empreinte du mot de passe. Pour vérifier l'accès, il « hache » de la même manière le mot de passe que l'on a saisi. Et si les empreintes sont les mêmes, il considère que ce mot de passe était le bon.

Il est donc possible de vérifier que le mot de passe correspond, sans garder le mot de passe lui-même !

5.3 Symétrique, asymétrique ?

Les techniques de chiffrement mentionnées jusqu'ici reposent sur une seule clé secrète, qui permet à la fois d'effectuer le chiffrement et le déchiffrement. On parle dans ce cas de cryptographie *symétrique*.

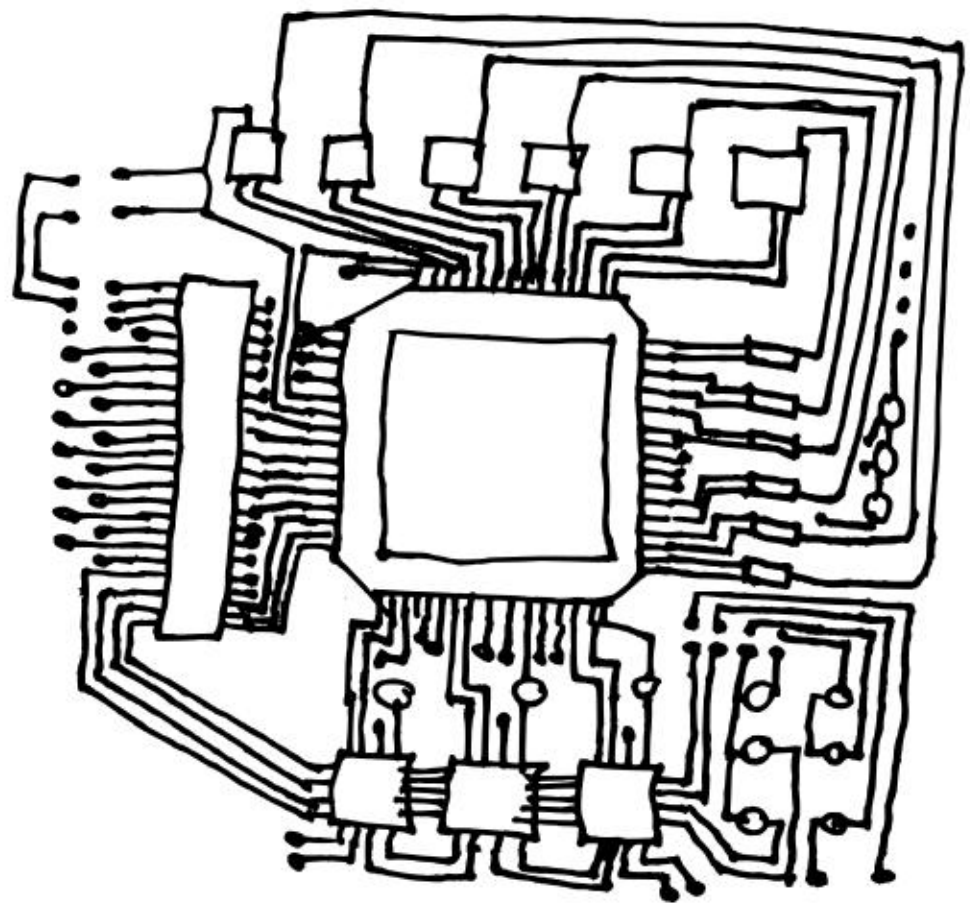
Ceci en opposition avec la cryptographie *asymétrique*, qui, dans le contexte du chiffrement, n'utilise pas la même clé pour chiffrer et pour déchiffrer un message. Aussi appelée « cryptographie à clé publique », elle est surtout utilisée pour la communication « en ligne » ; on en parlera donc en détail dans le second tome.

page 249

Une des propriétés les plus intéressantes de la cryptographie asymétrique, que l'on peut évoquer brièvement, est la possibilité de réaliser des *signatures numériques*. Comme son équivalent papier, une signature numérique permet d'apposer une marque de reconnaissance sur des données.

Ces signatures numériques qui utilisent la cryptographie asymétrique constituent la façon la plus simple de vérifier la provenance d'un logiciel. On sera donc amenées à s'en servir plus loin…

25. Rappelons-nous que ces mots de passe ne servent pas à protéger les données [page 41] !



Deuxième partie

Choisir des réponses adaptées

Introduction

Pour être honnêtes, ce premier chapitre et la compréhension du fonctionnement des ordinateurs a de quoi faire paniquer n'importe qui... Faire l'autruche n'est cependant pas une solution appropriée : on a déjà écarté l'idée qu'on n'avait rien à cacher. Le déni n'expose pas moins aux risques ou aux menaces.

Après lecture, on repense certainement aux films d'action où l'héroïne cache son matériel informatique dans un coffre de la bibliothèque qui s'ouvre quand on tire quelques livres dans une combinaison spéciale... et le découragement peut s'emparer de nous.

Heureusement, il y a une autre solution : lire la suite du guide ! Cette nouvelle partie présente des situations types, appelées *cas d'usage*, puis propose des pratiques et des outils adéquats à chaque situation.

Chapitre 6

Confiance et réduction des risques

Les notions de *confiance* et de *réduction des risques* sont utiles pour choisir comment utiliser des outils numériques. Dans ce chapitre, on évoquera le sexe, la drogue et le rock'n'roll, des contextes dans lesquels ces notions ont déjà été réfléchies. Comme le numérique, ces pratiques peuvent être fun, mais comportent souvent des risques.

6.1 Réduction des risques

Travailler sur un chantier ou à un bureau ;
partager des bijoux de piercing, des sextoys, ou sa brosse à dents ;
se connecter à Internet ou utiliser des outils numériques ;
monter dans une voiture ou faire du vélo…
Toutes ces pratiques comportent des risques… et on peut les réduire !

Comme le dit Act Up : « information = pouvoir ». En effet, le savoir et la compréhension des choses permettent de prendre plus de plaisir en prenant moins de risques, sachant que le risque zéro n'existe pas. Aussi, la notion de risque est relative, elle comprend tellement d'aspects différents qu'il faut en discuter pour pouvoir les comprendre et les cerner [1].

Diffuser de l'information relative aux risques est d'autant plus important que lorsqu'un virus est présent, autant dans l'organisme que dans un ordinateur, il n'y a pas forcément de signe visible. C'est pour cette raison que du point de vue de la santé, il est conseillé de ne pas attendre d'avoir des symptômes pour agir, et de faire régulièrement des dépistages. Ou par exemple, au niveau numérique, les mises à jour régulières permettent de réduire les risques d'infection en corrigeant les failles de sécurité.

De nombreuses personnes passent du temps à faciliter la réduction des risques : en distribuant des brochures d'information, mais aussi des capotes, des *roule ta paille* ou des bouchons d'oreille. Et dans la même logique, des gens développent des logiciels, écrivent de la documentation, animent des ateliers d'autodéfense ou d'intimité numérique.

Pour qu'utiliser le chiffrement soit aussi facile qu'enfiler un casque de chantier ;
pour en savoir autant sur le clitoris que sur la mémoire vive ;
pour que l'usage de Tor soit aussi simple que celui des bouchons d'oreille ;
parce que tout compte fait, se masturber et chercher des images de fond d'écran pendant des heures rend la vie plus agréable et ne devrait pas être risqué !

1. C'est pourquoi, dans les années 90 dans le champ des toxicomanies, on a arrêté de parler de *prévention* pour parler de *réduction des risques* [http://www.keep-smiling.com/?p=259]. Dans le champ de la sexualité, des gens ont arrêté d'utiliser *safe sex* pour utiliser plutôt *safer sex*.

6.2 Une histoire de confiance

La confiance accordée aux équipements numériques, aux logiciels et aux réseaux, c'est comme la confiance accordée aux garagistes : on peut les croire, ou pas. De la même manière, on peut avoir plus ou moins confiance en l'équipe de développement d'un logiciel[2].

Cette super application chiffre complètement toutes vos données !
Ce casque protège votre tête en cas d'accident !
T'inquiète pas, je n'ai pas pris de risque !

Les affirmations de ce genre ne sont pas suffisantes pour construire un rapport de confiance. Il convient de se poser des questions, de dépasser les évidences.

Si une application annonce chiffrer complètement les données, on peut se demander quel est le système de chiffrement et si cette méthode est approuvée par les communautés en qui nous avons confiance. On peut aussi se demander si ce ne serait pas du marketing mensonger.

De la même manière, quand on partage de la sexualité, on peut discuter de ce que l'on considère comme une prise de risque, et quelles sont nos limites, nos pratiques ou notre rapport à la réduction des risques et au dépistage.

Se poser les questions suivantes aide à évaluer la confiance qu'on pourrait avoir dans un outil :

page 39

- Pourquoi cet outil a-t-il été developpé ?
- Est-il libre ?
- Quel est son modèle économique ?
- À qui doit-il rendre des comptes ?

Mais tout ça n'est pas juste une question de risques et de confiance. On parle de simple risque quand il n'y a pas de volonté de nuire à des personnes, des groupes, des idées, *etc.* ; dans le cas contraire, c'est une menace.

Le risque, c'est de s'abimer les mains en arrachant des ronces sans gants, la menace c'est le patron qui met au placard ses salariées syndiquées ;
le risque, en conduisant ivre, c'est d'avoir un accident, la menace c'est de se faire retirer son permis de conduire ;
le risque, quand on n'a pas fait de sauvegarde, c'est de perdre toutes ses données si un disque dur plante, la menace c'est que la police perquisitionne le lieu d'activité militante où il est stocké ;
le risque c'est un bug dans un logiciel qui fait planter l'ordi, la menace c'est Cambridge Analytica qui utilise les données des comptes Facebook pour influencer les résultats des élections.

Bien sûr, c'est plus compliqué : il y a des risques de menace et des menaces peuvent engendrer des risques !

La question de la menace n'est pas uniquement individuelle, puisqu'en ne prenant pas certaines précautions, on peut exposer les personnes avec qui on communique.

---

2. On peut se poser cette question de la confiance avec à peu près toutes les spécialistes : les journalistes, les toubibs, les paysannes, les charpentières, les ingénieures, les flics, les commerçants, les tatoueuses, les maçonnes, les pilotes (d'avion, de train, de bus, *etc.*), les urbanistes, les coiffeurs, les architectes, les pharmaciennes, les profs, les artistes, les surveillantes de baignade, les aides soignantes, les infirmières, les boulangères, les politiciennes, les factrices, les psys, les agentes d'accueil (de la CAF, de la MSA, de Pôle emploi, *etc.*), les comptables, les commerciaux, les vétérinaires, les DRH (Directrices de Ressources Humaines), les scientifiques, les artisanes, les cuistots, les vigiles, les banquières, les ouvrières, les sportives, les coachs, les électroniciennes, les éducs, les assistantes sociales, *etc.*

Chapitre 7

Évaluation des risques

Quand on se demande quelles mesures mettre en place pour protéger des données ou des communications numériques, on se rend assez vite compte qu'on avance un peu à l'aveuglette.

En effet, les solutions qu'on pourrait mettre en place ont aussi leurs inconvénients : parfois elles sont très pénibles à déployer, à entretenir ou à utiliser ; parfois on a le choix entre diverses techniques, dont aucune ne répond complètement au « cahier des charges » que l'on s'est fixé ; parfois elles sont bien trop nouvelles pour qu'on ait l'assurance qu'elles fonctionnent réellement ; *etc.*

On devrait donc commencer par se poser quelques questions simples, afin d'établir un *modèle de menace*[1], c'est-à-dire l'identification et le classement par ordre de priorité des menaces potentielles.

7.1 Que veut-on protéger ?

Ce qu'on veut protéger rentre en général dans la vaste catégorie de l'*information* : par exemple, le contenu de messages électroniques, des fichiers de données (photo, tracts, carnet d'adresses) ou l'existence même d'une correspondance entre telle et telle personne.

Le mot « protéger » recouvre différents besoins :

- **confidentialité** : cacher des informations aux yeux indésirables ;
- **intégrité** : conserver des informations en bon état, et éviter qu'elles ne soient modifiées sans qu'on s'en rende compte ;
- **accessibilité** : faire en sorte que des informations restent accessibles aux personnes qui en ont besoin.

Il s'agit donc de définir, pour chaque ensemble d'informations à protéger, les besoins de confidentialité, d'intégrité et d'accessibilité. Sachant que ces besoins entrent généralement en conflit, il faudra, poser des priorités et trouver des compromis, ménager la chèvre (affamée) et le chou (très appétissant)…

7.2 Contre qui veut-on se protéger ?

Rapidement se pose la question des capacités des personnes qui en auraient après ce que l'on veut protéger : des parents intrusifs, des camarades de classe susceptibles de faire du harcèlement, des voleurs voulant récupérer des coordonnées bancaires, un ex-conjoint violent qui cherche des moyens de contrôle ou de chantage, des hiérarchies trop curieuses, la police chargée de mater un mouvement social, des fonctionnaires qui

1. Voir Electronic Frontier Foundation, 2019, *Votre plan de sécurité* [https://ssd.eff.org/fr/module/votre-plan-de-sécurité].

contrôlent les personnes migrantes[2], les GAFAM qui traquent et vendent les données personnelles, des services de renseignement mandatés pour ficher massivement une communauté ou un courant politique, *etc.*

Mais il n'est pas facile de savoir ce que les plus qualifiées d'entre elles peuvent réellement faire, de quels moyens et de quels budgets elles bénéficient. En suivant l'actualité, et par divers autres biais, on peut se rendre compte que cela varie beaucoup selon à qui on a affaire. Entre les parents, les gendarmes du coin et la *National Security Agency* (NSA) états-unienne, il y a tout un fossé sur les possibilités d'actions, de moyens et de techniques employées.

La question des moyens des adversaires est assez large.

Il y a les **moyens judiciaires** : par exemple, la possibilité qu'une commission rogatoire autorise la police à saisir du matériel informatique, ou le fait qu'il peut être exigé de donner sa clé de chiffrement.

page 50

En parallèle, des organismes disposent de beaucoup de **moyens techniques**, tels la SDAT[3] ou la DGSE[4]. Rien n'est sûr concernant leurs possibilités : quelle avance ont-ils dans le domaine du cassage de cryptographie ? Sont-ils au courant de failles dans certaines méthodes, qu'ils n'auraient pas dévoilées, et qui leur permettraient de lire les données ? Sur ces sujets, il n'y a évidemment aucun moyen d'avoir la certitude de ce que ces entités peuvent faire.

Les **moyens financiers** sont à prendre en compte. En effet, certaines technologies de surveillance coûtent cher et elles ne sont pas à la portée de tous les services de renseignement ou ne seront pas à disposition dans n'importe quelle enquête. À savoir que le budget annuel de la DGSE était de 880 millions d'euros en 2021 et que celui de la NSA était estimé à 10,8 milliards de dollars (!) en 2013, ils ne jouent pas dans la même cour.

On peut aussi se poser la question des **moyens politiques** : par exemple, dans quelle mesure l'État français peut-il collaborer avec la NSA ?

Par ailleurs, sécuriser complètement un ordinateur est de l'ordre de l'impossible. Il s'agit donc plutôt de mettre des bâtons dans les roues de celles et ceux qui pourraient en vouloir à nos informations. Plus grands sont les moyens de ces personnes, plus les bâtons doivent être nombreux et solides.

Évaluer les risques, c'est se demander quelles sont les données que l'on veut protéger et de qui. À partir de là, on peut essayer de se renseigner sur les moyens à disposition des personnes qui s'y intéresseraient et définir une *politique de sécurité* en conséquence.

---

2. Voir l'article de Ritimo : 10 menaces contre les migrant·es et les réfugié·es [https://www.ritimo.org/10-menaces-contre-les-migrant-es-et-les-refugie-es].

3. Service de la police française voué à lutter contre le terrorisme, voir Wikipédia, 2021, *Sous-direction anti-terrorriste* [https://fr.wikipedia.org/wiki/Sous-direction_anti-terroriste].

4. Service de renseignement de la France, voir Wikipédia, 2017, *Direction générale de la Sécurité extérieure* [https://fr.wikipedia.org/wiki/Direction_g%C3%A9n%C3%A9rale_de_la_S%C3%A9curit%C3%A9_ext%C3%A9rieure].

Chapitre 8

Définir une politique de sécurité

Une chaîne n'a que la solidité de son maillon le plus faible. Rien ne sert d'installer trois énormes verrous sur une porte blindée placée à côté d'une frêle fenêtre délabrée. De même, chiffrer une clé USB ne rime pas à grand-chose si les données qui y sont stockées sont utilisées sur un ordinateur qui en conservera diverses traces *en clair* sur son disque dur.

page 47
page 27

Ces exemples nous apprennent quelque chose : de telles « solutions » ciblées ne sont d'aucune utilité tant qu'elles ne font pas partie d'un ensemble de pratiques articulées de façon cohérente. Qui plus est, les informations qu'on veut protéger sont le plus souvent en relation avec des pratiques hors du champ des outils numériques. C'est donc de façon globale qu'il faut évaluer les risques et penser les réponses adéquates.

page 63

De façon globale, mais *située* : à une situation donnée correspond un ensemble singulier d'enjeux, de risques, de savoir-faire… et donc de possibilités d'action. Il n'existe pas de solution miracle convenant à tout le monde, et qui réglerait tous les problèmes d'un coup de baguette magique. La seule voie praticable, c'est d'en apprendre suffisamment pour être capable d'imaginer et de mettre en place une politique de sécurité adéquate à sa propre situation.

8.1 Une affaire de compromis

On peut toujours *mieux* protéger ses données et ses communications numériques. Les possibilités d'attaque et de surveillance sont sans limites, tout comme les dispositifs pour s'en protéger. Cependant, à chaque protection supplémentaire qu'on veut mettre en place correspond un effort en termes d'apprentissage et de temps : non seulement un effort initial pour s'y mettre, pour installer la protection, mais aussi, bien souvent, une complexité d'utilisation supplémentaire, du temps passé à taper des phrases de passe, à effectuer des procédures pénibles et répétitives, à porter son attention sur la technique plutôt que sur l'usage qu'on voudrait avoir des outils numériques.

Dans chaque situation, il s'agit donc de trouver un **compromis** convenable entre la facilité d'utilisation et le niveau de protection souhaité.

Parfois, ce compromis **n'existe** tout simplement **pas**. Les efforts nécessaires pour se protéger contre un risque plausible seraient trop pénibles, et il vaut mieux courir ce risque, ou bien, tout simplement, ne pas utiliser d'outils numériques pour stocker certaines données ou pour parler de certaines choses. D'autres moyens existent, à l'efficacité prouvée de longue date : certains manuscrits ont survécu des siècles durant, enfouis dans des jarres entreposées dans des grottes…

8.2 Comment faire ?

Il s'agit de répondre à la question suivante : quel ensemble de pratiques et d'outils me protégeraient de façon suffisante contre les risques évalués précédemment ?

page 63

Pour ce faire, on peut partir de nos pratiques actuelles et se poser les questions suivantes :

1. Face à une telle politique de sécurité, quels angles d'attaque mes adversaires utiliseraient ?
2. Quels moyens devraient être mis en œuvre par mes adversaires ?
3. Ces moyens sont-ils à la portée de mes adversaires ?

Si vous répondez « oui » à la troisième question, prenez le temps de vous renseigner sur les solutions qui permettraient de vous protéger contre ces attaques, puis imaginez les modifications de pratiques entraînées par ces solutions et la politique de sécurité qui en découle. Si ça vous semble praticable, remettez-vous dans la peau de vos adversaires, et posez-vous à nouveau les questions énoncées ci-dessus.

Réitérez ce processus de réflexion, recherche et imagination jusqu'à trouver une voie praticable, un compromis tenable.

En cas d'incertitude, il est toujours possible de demander à une personne digne de confiance et plus compétente en la matière de se mettre dans la peau des adversaires : elle sera ravie de constater que vous avez fait vous-même le gros du travail de réflexion, ce qui l'encouragera certainement à vous aider sur les points qui restent hors de votre portée.

8.3 Quelques règles

Avant de s'intéresser de plus près à l'étude de cas concrets et des politiques de sécurité qu'il serait possible de mettre en place, il existe quelques grands principes, quelques grandes familles de choix.

8.3.1 Complexe vs. simple

En matière de sécurité, une solution simple doit toujours être préférée à une solution complexe.

Tout d'abord, parce qu'une solution complexe offre plus de « surface d'attaque », c'est-à-dire plus de lieux où peuvent apparaître des problèmes de sécurité, ce qui ne manquera pas d'arriver…

Ensuite, parce que plus une solution est complexe, plus il faut de connaissances pour l'imaginer, la mettre en œuvre, la maintenir, mais aussi pour l'examiner, évaluer sa pertinence et ses problèmes. Ce qui fait qu'en règle générale, plus une solution est complexe, moins elle aura subi les regards acérés — et extérieurs — nécessaires pour établir sa validité.

Enfin, tout simplement, une solution complexe, qui ne tient pas en entier dans l'espace mental des personnes qui l'ont élaborée, a plus de chances de générer des problèmes de sécurité issus d'interactions complexes ou de cas particuliers difficiles à déceler.

Par exemple, plutôt que de passer des heures à mettre en place des dispositifs visant à protéger un ordinateur particulièrement sensible contre les intrusions provenant du réseau, autant l'en débrancher. On peut même parfois retirer physiquement la carte réseau…

page 20

8.3.2 Liste autorisée, liste bloquée

Le réflexe courant, lorsqu'on prend connaissance d'une menace, est de chercher à s'en prémunir. Par exemple, après avoir découvert que tel logiciel laisse des traces de nos activités dans tel dossier, on nettoiera régulièrement cet emplacement. Jusqu'à découvrir que le même logiciel laisse aussi des traces dans un autre dossier, et ainsi de suite.

C'est le principe de la liste bloquée[1] : une liste des dossiers où sont enregistrés les fichiers temporaires, des logiciels qui envoient des rapports, *etc.* Cette liste est complétée au fil des découvertes et des mauvaises surprises ; sur cette base, on essaie de faire au mieux pour se prémunir de chacune de ces menaces. Autrement dit, une liste bloquée fonctionne sur la base de la *confiance-sauf-dans-certains-cas*.

Le principe de la liste autorisée[2] est inverse, car c'est celui de la *méfiance-sauf-dans-certains-cas*. On interdit *tout*, *sauf* ce qu'on autorise explicitement. On interdit l'enregistrement de fichiers sur le disque dur, sauf à tel endroit, à tel moment. On interdit aux logiciels d'accéder au réseau, sauf certains logiciels bien choisis. page 131

Voilà pour les principes de base.

Toute politique de sécurité basée sur le principe de la *liste bloquée* a un gros problème : une telle liste n'est jamais complète, car elle prend uniquement en compte les problèmes qui ont déjà été repérés. C'est une tâche sans fin, désespérante, que de tenir à jour une liste bloquée ; qu'on le fasse nous-mêmes ou qu'on le délègue à des gens ayant des connaissances informatiques pointues, quelque chose sera forcément oublié.

L'ennui, c'est que malgré leurs défauts rédhibitoires, les outils basés sur une approche *liste bloquée* sont légion (comme nous allons le voir), au contraire de ceux s'appuyant sur la méthode *liste autorisée*, qui nous est par conséquent moins familière.

Mettre en œuvre l'approche *liste autorisée* requiert un effort initial qui, s'il peut être important, est bien vite récompensé. Apprendre à utiliser un système *live* qui n'écrit rien sur le disque dur sans qu'on le lui demande, ça prend un temps certain. Mais une fois que c'est fait, c'en est fini des longues séances de nettoyage de disque dur, toujours à recommencer et inefficaces car basées sur le principe de *liste bloquée*. page 113

Une autre illustration nous est fournie par les logiciels antivirus, qui visent à empêcher l'exécution de programmes mal intentionnés. Vu qu'ils fonctionnent sur le principe de la liste bloquée, leurs bases de données doivent perpétuellement être mises à jour car elles sont systématiquement en retard. Une réponse à ce problème, avec l'approche *liste autorisée*, est d'empêcher l'exécution de tout programme qui n'a pas été enregistré au préalable, ou de limiter les possibilités d'action de chaque programme. Ces techniques, nommées *Mandatory Access Control*, nécessitent aussi de maintenir des listes, mais il s'agit dans ce cas de listes *autorisées*, et le symptôme d'une liste obsolète sera le dysfonctionnement d'un logiciel, plutôt que le piratage de l'ordinateur.

Aussi, il est bien plus intéressant de se donner les moyens, lorsque c'est réalisable, de s'appuyer sur des listes autorisées les plus vastes possible, afin de pouvoir faire plein de choses chouettes avec des ordinateurs, dans une certaine confiance. Et de s'appuyer, quand la liste autorisée adéquate n'existe pas, sur des listes bloquées solides, de provenance connue, en gardant en tête le problème intrinsèque à cette méthode ; listes bloquées qu'on aidera éventuellement à compléter, en partageant nos découvertes.

8.3.3 Personne n'est infaillible

Sur Internet, il est souvent dit que « la plupart des problèmes informatiques se trouvent entre la chaise et le clavier »[3]. Derrière cette expression méprisante pour les personnes qui utilisent les outils se cache une réalité : personne n'est infaillible et l'erreur humaine est toujours une hypothèse à envisager.

---

1. Parfois aussi appelée « liste noire ».
Les expressions « liste noire » et « liste blanche » peuvent évoquer une dimension raciste, que ce soient les termes en eux-mêmes, ou leur hiérarchisation. On a donc fait le choix de remplacer ces deux termes par « liste bloquée » et « liste autorisée ». Malheureusement, la plupart des programmes, modes d'emploi et autres documentations techniques utilisent encore ces termes. C'est pourquoi nous nous trouvons obligées de les mentionner.
2. Parfois aussi appelée « liste blanche ».
3. Wiktionnaire, 2020, *Entre la chaise et le clavier* [https://fr.wiktionary.org/wiki/entre_la_chaise_et_le_clavier].

Certaines pratiques peuvent être diablement efficaces… jusqu'à ce qu'on commette une erreur. Comme on finira forcément par en faire une, il vaut mieux les prévoir plutôt que de payer les pots cassés [4].

Par exemple, imaginons une clé USB qui contient des documents confidentiels. Même en faisant vraiment attention à ne pas la laisser traîner, elle peut quand même finir par être oubliée sur une table… et être branchée et utilisée par une personne qui l'aura confondue avec une autre, dans une machine en laquelle on n'a pas confiance. Le chiffrement de la clé, avant d'y mettre les documents confidentiels, aurait permis de réduire significativement les risques.

page 47

Bref, on n'est pas des robots. Il vaut mieux se donner de solides garde-fous matériels, que de s'imposer une vigilance sans bornes et ça permet aussi de garder l'esprit tranquille.

8.3.4 Rien n'est éternel

Une fois une politique de sécurité définie, il ne faut pas oublier de la revoir de temps en temps ! Le monde de la sécurité informatique évolue très vite, et une solution considérée comme raisonnablement sûre à l'heure actuelle peut très bien être aisément attaquable l'an prochain.

N'oublions pas non plus de penser, dans nos politiques de sécurité, qu'il est important de surveiller la vie des logiciels dont on dépend : leurs problèmes, avec une incidence sur la sécurité ; leurs mises à jour, avec parfois de bonnes ou de mauvaises surprises… Tout cela prend un peu de temps, et autant le prévoir dès le départ.

page 175

4. En anglais, on utilise l'expression « better safe than sorry », qui signife littéralement : « mieux vaut la prudence que le regret. » Un équivalent de l'expression « mieux vaut prévenir que guérir » en français.

Cas d'usage

Trêve de théorie, illustrons maintenant ces notions avec quelques *cas d'usage* : à partir de situations données, nous indiquerons des pistes permettant de définir une politique de sécurité adéquate. Bon nombre des solutions techniques retenues seront expliquées dans la partie suivante, vers laquelle nous renverrons au besoin.

page 95

Vu qu'ils s'inscrivent tous dans le contexte hors-connexion de ce premier tome, ces cas d'usage auront quelque chose d'artificiel : ils partent tous du principe que les ordinateurs en jeu ne sont jamais connectés à des réseaux, et en particulier à Internet.

Chapitre 9

Cas d'usage : un nouveau départ, pour ne plus payer les pots cassés

(ou comment faire le ménage sur un ordinateur après des années de pratiques insouciantes)

9.1 Contexte

Prenons un ordinateur utilisé sans précautions particulières pendant plusieurs années. Cette machine pose sans doute un ou plusieurs des problèmes suivants :

1. son disque conserve des traces indésirables du passé ; page 27
2. le système d'exploitation est un logiciel propriétaire (exemple : Windows), et truffé de logiciels malveillants. page 31

Par ailleurs, des fichiers gênants y sont stockés de façon parfaitement transparente. En effet, cet ordinateur est utilisé pour diverses activités (parmi lesquelles certaines sont parfaitement légales) telles que :

- écouter de la musique et regarder des films pris sur Internet ;
- aider des sans-papiers à préparer leurs dossiers pour la préfecture ;
- dessiner une jolie carte de vœux pour sa grand-mère ;
- fabriquer de faux documents administratives simplifiant grandement certaines démarches (gonfler des fiches de paie, quand on en a marre de se voir refuser des locations, appart' après appart') ;
- tenir à jour la comptabilité familiale ;
- fabriquer des textes, musiques ou vidéos « terroristes ». C'est-à-dire, selon la définition européenne du terrorisme[1] : menaçant « *de causer des destructions massives [...] à une infrastructure [...] susceptible [...] de produire des pertes économiques considérables* ». Par exemple dans le but de « *contraindre indûment des pouvoirs publics ou une organisation internationale à accomplir ou à s'abstenir d'accomplir un acte quelconque* ». Par exemple, des personnes employées par Orange qui, lors d'une lutte, menaceraient de mettre hors d'état de nuire le système de facturation, et d'ainsi permettre à tout le monde de téléphoner gratuitement.

1. Union Européenne, 2017, *Directive (UE) 2017/541 du Parlement européen et du Conseil du 15 mars 2017 relative à la lutte contre le terrorisme et remplaçant la décision-cadre 2002/475/JAI du Conseil et modifiant la décision 2005/671/JAI du Conseil*, article 3 [https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32017L0541&qid=1495634630652].

9.2 Évaluer les risques

9.2.1 Que veut-on protéger ?

page 63

Appliquons au cas présent les catégories définies lorsque nous parlions d'évaluation des risques :

- confidentialité : éviter qu'un œil indésirable ne tombe trop aisément sur les informations stockées dans l'ordinateur ;
- intégrité : éviter que ces informations ne soient modifiées à notre insu ;
- accessibilité : faire en sorte que ces informations restent accessibles quand on en a besoin.

Ici, accessibilité et confidentialité sont prioritaires.

9.2.2 Contre qui veut-on se protéger ?

Cette question est importante : en fonction de la réponse qu'on lui donne, la politique de sécurité adéquate peut varier du tout au tout.

Geste généreux, conséquences judiciaires

Cet ordinateur pourrait être saisi lors d'une perquisition.

Par exemple, votre enfant a généreusement donné un gramme de *shit* à des potes, qui, après s'être fait pincer, ont informé la police de la provenance de la chose… à la suite de quoi le parquet poursuit votre enfant pour trafic de stupéfiants. D'où la perquisition.

Dans ce genre de cas, l'ordinateur a de grandes chances d'être examiné par la police, mettant en péril l'objectif de confidentialité. La gamme des moyens qui seront probablement mis en œuvre va des gendarmes de Saint-Tropez allumant l'ordinateur et cliquant partout, à l'experte judiciaire qui examinera de beaucoup plus près le contenu du disque. Il est en revanche improbable que des moyens extra-légaux soient utilisés dans cette affaire, car ils sont généralement réservés aux services spéciaux et aux militaires.

Cambriolage

Cet ordinateur pourrait être dérobé lors d'un cambriolage.

Au contraire de la police, les personnes qui ont volé l'ordinateur n'en ont sans doute pas grand-chose à faire de vos petits secrets et ne vous dénonceront pas. Au pire vous feront-elles chanter à propos de la récupération de vos données. Il est cependant improbable qu'elles mettent en œuvre de grands moyens pour les trouver sur le disque de l'ordinateur.

9.3 Définir une politique de sécurité

page 65

Posons-nous maintenant, les questions exposées dans la méthodologie en se mettant dans la peau des adversaires.

page 231

Tout ce qui suit est valable pour un ordinateur hors-ligne. D'autres situations et angles d'attaque sont imaginables s'il est connecté à un réseau, c'est ce que le second tome de ce guide étudiera.

9.3.1 Se mettre dans la peau des adversaires

Première étape : quand il leur suffit de regarder

1. Angle d'attaque le plus praticable : brancher le disque sur un autre ordinateur, examiner son contenu, y trouver tous nos petits secrets.

2. Moyens nécessaires : un autre ordinateur permettra aux gendarmes de Saint-Tropez de trouver le plus gros de nos secrets ; une experte judiciaire, elle, saurait aussi retrouver les fichiers que nous croyions avoir effacés.
3. Crédibilité de l'attaque : grande.

Il va donc falloir adapter nos pratiques. Contre ce type d'attaque, chiffrer le disque est la réponse évidente : installer et utiliser un système chiffré est désormais relativement simple. page 47 page 119

Les étapes pour y arriver seraient alors :

1. Lancer un système *live* afin d'effectuer les opérations suivantes dans un contexte relativement sûr :
   - sauvegarder temporairement, sur un disque externe ou une clé USB chiffrées, les fichiers qui doivent survivre au grand nettoyage ;
   - éjecter/démonter et débrancher ce support de stockage externe ;
   - effacer « pour de vrai » l'intégralité du disque **interne** de l'ordinateur. page 139
2. Installer un système d'exploitation libre, en précisant au programme d'installation de chiffrer le disque, mémoire virtuelle (*swap*) comprise. page 25
3. Recopier vers le nouveau système les données préalablement sauvegardées.
4. Mettre en place ce qu'il faut pour supprimer des fichiers de façon « sécurisée », afin de pouvoir…
5. Effacer le contenu des fichiers qui se trouvent sur le support de sauvegarde temporaire, qui pourra éventuellement resservir.

Ensuite, de temps à autre, faire en sorte que les données supprimées sans précautions particulières ne soient pas récupérables par la suite. Il faudra également veiller à mettre régulièrement à jour le système, afin de combler les « trous de sécurité » que pourraient utiliser des logiciels malveillants. page 32

Pour effectuer ces étapes, se référer aux recettes suivantes :

- chiffrer un disque externe ou une clé USB (voir page 145) ;
- utiliser un système *live* (voir page 113) ;
- sauvegarder des données (voir page 151) ;
- effacer « pour de vrai » (voir page 139) ;
- installer un système chiffré (voir page 119) ;
- garder un système à jour (voir page 175).

Deuxième étape : le tiroir de la commode n'était pas chiffré

1. Angle d'attaque : l'équivalent des fichiers qu'on cherche à protéger traîne peut-être dans la pièce voisine, dans le troisième tiroir de la commode, sur papier ou sur une clé USB.
2. Moyens nécessaires : perquisition, cambriolage ou autre visite impromptue.
3. Crédibilité de l'attaque : grande, c'est précisément contre ce type de situations qu'on cherche à se protéger ici.

Là encore, on constate qu'une politique de sécurité doit être pensée comme un tout. Sans un minimum de cohérence dans les pratiques, rien ne sert de s'embêter à taper des phrases de passe longues comme un jour sans pain. page 65

Il est donc temps de trier les papiers dans la commode et de nettoyer toute clé USB, CD ou DVD contenant des données que l'on compte désormais chiffrer :

- sauvegarder sur un support chiffré les données à conserver ;
- pour les clés USB et disques externes : effacer pour de vrai leur contenu ; page 139
- pour les CD et DVD : les détruire et se débarrasser des résidus ;
- décider que faire des données préalablement sauvegardées : les recopier sur le disque nouvellement chiffré ou les archiver. page 89

Troisième étape : la loi comme moyen de coercition

page 50

1. Angle d'attaque : la police a le droit d'exiger que vous lui donniez accès aux informations chiffrées, comme expliqué dans le chapitre consacré à la cryptographie.
2. Moyens nécessaires : suffisamment de persévérance dans l'enquête pour appliquer cette loi.
3. Crédibilité de l'attaque : probable, déjà utilisée à plusieurs reprises, y compris pour des affaires de stupéfiants [2].

Si la police en arrive à exiger l'accès aux données chiffrées, se posera, en pratique, la question suivante : les informations contenues dans l'ordinateur font-elles encourir plus de risques que le refus de donner la phrase de passe ? Après, c'est selon comment on le sent. Céder dans cette situation ne remet pas en cause tout l'intérêt de chiffrer son disque : cela permet tout au moins de savoir ce qui a été dévoilé, quand et à qui.

Cependant, si dévoiler sa phrase de passe est une décision personnelle, elle peut avoir des conséquences plus larges. Par exemple pour d'autres personnes dont le pseudo serait cité dans des documents stockés sur notre ordinateur, ou si dans une procédure judiciaire tout le monde donne sa phrase de passe sauf une seule personne. Dévoiler ou non sa phrase de passe n'est finalement pas une question si individuelle et elle peut donc se réfléchir à plusieurs. Il se peut aussi que *par principe* on ne veuille pas donner sa phrase de passe, alors même *qu'on n'a rien à cacher*.

page 1

Ceci dit, il peut être bon de s'organiser pour vivre de façon moins délicate une telle situation : le nouvel objectif pourrait être d'avoir un disque suffisamment « propre » pour que ce ne soit pas la catastrophe si on cède face à la loi, ou si une faille est découverte dans le système cryptographique utilisé.

Comme premier pas, il est souvent possible de faire un compromis concernant l'accessibilité des fichiers relatifs à des projets achevés, dont on n'aura plus besoin souvent. On traitera ceci dans le cas d'usage sur l'archivage, qui pourra être étudié après celui-ci.

page 89

page 246

Ensuite, c'est toute la question de la compartimentation qui se pose : toutes nos activités ne nécessitent pas forcément le même niveau de sécurité et on ne veut pas forcément qu'elles soient toutes reliées à notre identité civile ou à un même pseudo. Il serait possible d'augmenter globalement le niveau de sécurité de l'ensemble des activités pratiquées, mais il se peut que ce soit trop pénible à l'usage. On peut donc plutôt envisager de *compartimenter*. Il convient alors de préciser les besoins respectifs, en matière de confidentialité, de ces diverses activités et à partir de là, de faire le tri et décider lesquelles, plus « sensibles » que les autres, doivent bénéficier d'un traitement de faveur.

page 79

Le prochain cas d'usage étudiera de tels traitements de faveur, mais patience, mieux vaut pour l'instant terminer la lecture de celui-ci !

9.3.2 Autres angles d'attaque à envisager

Au-delà de ces situations, plusieurs autres angles d'attaque demeurent encore envisageables contre une telle politique de sécurité.

Premier angle d'attaque : une brèche dans le système de chiffrement utilisé

Comme cela a déjà été expliqué dans ces pages, tout système de sécurité finit par être cassé. Si l'algorithme de chiffrement utilisé est cassé, cela fera probablement la une des journaux, tout le monde sera au courant, et il sera possible de réagir.

page 22

Mais si c'est sa mise en œuvre dans le noyau Linux qui est cassée, ça ne passera

2. Cour de Cassation française, 2020, *Arrêt de la chambre criminelle du 13 octobre 2020* [https://www.courdecassation.fr/decision/5fca302e5b008f80d3ad3a35].

pas dans *Libération*, et il y a fort à parier que seules les personnes spécialistes de la sécurité informatique seront au courant.

Lorsqu'on ne côtoie pas de telles personnes, une façon de se tenir au courant est de s'abonner aux annonces de sécurité de Debian[3]. Les emails reçus par ce biais sont rédigés en anglais, mais il est possible de retrouver leur traduction française — lorsqu'elle existe — sur la page « Informations de sécurité »[4] du projet Debian, où ces annonces de sécurité sont recensées. La difficulté, ensuite, sera de les interpréter…

Ceci étant dit, même si le système de chiffrement utilisé est « cassé », encore faut-il que les adversaires le sachent… Les gendarmes de Saint-Tropez n'en sauront probablement rien, mais une experte judiciaire, si.

Par ailleurs, dans le rayon science-fiction, rappelons qu'il est difficile de connaître l'avance qu'ont les militaires et les agences gouvernementales comme la NSA dans ce domaine.

Deuxième angle d'attaque : cold boot attack

1. Angle d'attaque : la *cold boot attack* est décrite dans le chapitre consacré aux traces. page 27
2. Moyens nécessaires : accéder physiquement à l'ordinateur pendant qu'il est allumé ou éteint depuis peu.
3. Crédibilité de l'attaque : à notre connaissance, cette attaque n'a jamais été utilisée, du moins de façon publique, par des autorités. Sa crédibilité est donc très faible.

Il peut sembler superflu de se protéger contre cette attaque dans la situation décrite ici. Toutefois, mieux vaut prendre dès maintenant de bonnes habitudes, plutôt que d'avoir de mauvaises surprises dans quelques années. Quelles habitudes ? En voici quelques-unes qui rendent plus difficile cette attaque :

- éteindre l'ordinateur lorsqu'on ne s'en sert pas ;
- si on utilise un ordinateur fixe, prévoir la possibilité de couper le courant facilement et rapidement : interrupteur de multiprise aisément accessible par exemple ;
- si on utilise un ordinateur portable et si cela est possible, ôter la batterie (il suffit alors de débrancher le cordon secteur pour éteindre la machine) ;
- rendre l'accès au compartiment de votre ordinateur contenant la RAM plus long et difficile, par exemple en le collant/soudant.

Troisième angle d'attaque : l'œil et la vidéo-surveillance

Avec le système chiffré imaginé à la première étape, la confidentialité des données repose sur le fait que la phrase de passe soit gardée secrète. Si elle est tapée devant une caméra de vidéo-surveillance, des adversaires ayant accès à cette caméra ou à ses éventuels enregistrements pourraient découvrir ce secret, puis se saisir de l'ordinateur et avoir accès aux données. Plus simplement, dans un bar, un œil attentif pourrait voir la phrase de passe pendant qu'elle est tapée. page 72

Monter une telle attaque nécessite de surveiller les personnes utilisant l'ordinateur, jusqu'à ce que l'une d'entre elles tape la phrase de passe au mauvais endroit. Ça peut prendre du temps et c'est coûteux.

Pour se prémunir d'une telle attaque, il convient de :

- choisir une longue phrase de passe, qui rende très compliquée la mémorisation « à la volée » par une personne observatrice ; page 103

3. La liste de diffusion se nomme debian-security-announce [https://lists.debian.org/debian-security-announce/] (en anglais).
4. https://www.debian.org/security/index.fr.html

- vérifier autour de soi, à la recherche d'éventuels yeux (humains ou électroniques) indésirables, avant de taper sa phrase de passe ;
- cacher son clavier à l'aide de l'écran dans le cas d'un ordinateur portable, ou à l'aide d'une couverture[5].

Quatrième angle d'attaque : la partie non-chiffrée et le microprogramme

page 119

Comme expliqué dans la recette dédiée, un système chiffré ne l'est pas entièrement : le petit logiciel qui nous demande la phrase de passe de chiffrement du *reste* des données au démarrage est, lui, stocké en clair sur la partie du disque que l'on nomme `/boot`. Une personne malintentionnée ayant accès à l'ordinateur peut aisément et en quelques minutes modifier ce logiciel pour y installer un *keylogger*. Ce dernier conservera alors la phrase de passe lorsqu'elle sera tapée, pour venir la chercher plus tard ou, tout simplement, l'enverra par le réseau.

page 31

Si cette attaque est montée à l'avance, les adversaires pourront déchiffrer le disque quand elles se saisiront de l'ordinateur, lors d'une perquisition par exemple.

Les moyens nécessaires pour cette attaque sont, somme toute, assez limités : *a priori*, point n'est besoin d'être une superhéroïne pour avoir accès, pendant quelques minutes, à la pièce où réside l'ordinateur.

Cependant, en ce qui concerne la situation décrite pour ce cas d'usage, cette attaque ne paraît pas être la plus vraisemblable.



Précision

Une protection contre cette attaque est de stocker les programmes de démarrage, dont ce petit dossier non-chiffré (`/boot`), sur un support externe, comme une clé USB, qui sera conservé en permanence dans un endroit plus sûr que l'ordinateur. C'est l'*intégrité* de ces données, et non leur *confidentialité*, qui est alors à protéger. Cette pratique exige pas mal de compétences et de rigueur ; nous ne la développerons pas dans ce guide.

De telles pratiques mettent la barre plus haut pour les adversaires, mais il reste un mais : une fois obtenu l'accès physique à l'ordinateur, si `/boot` n'est pas accessible, et donc pas modifiable, il est possible d'effectuer le même type d'attaque sur le microprogramme (BIOS ou UEFI) de la machine. C'est légèrement plus difficile car la façon de faire dépend du modèle d'ordinateur utilisé, mais c'est possible. Nous ne connaissons aucune façon praticable de s'en protéger.

Cinquième angle d'attaque : les logiciels malveillants

page 31

Nous avons vu dans un chapitre précédent que des logiciels installés à notre insu sur un ordinateur peuvent nous dérober des données. Dans le cas présent, un tel logiciel est en mesure de transmettre la clé de chiffrement du disque à des adversaires afin qu'elles puissent avoir accès aux données chiffrées dès qu'elles auront un accès physique à l'ordinateur.

Installer un logiciel malveillant sur le système Debian dont il est question ici requiert des compétences de plus haut niveau que les attaques étudiées ci-dessus, mais aussi plus de préparation. Une telle attaque relève donc de la science-fiction, du moins en ce qui concerne la situation qui nous occupe. Dans d'autres situations, il conviendra parfois de faire preuve d'une extrême prudence quant à la provenance des données et logiciels qu'on injecte dans l'ordinateur.

page 131

Pour cela, la recette concernant l'installation de logiciels donne quelques pistes fort utiles sur la façon d'installer de nouveaux logiciels proprement. Aussi, le second tome de ce guide consacré aux réseaux, montre qu'une connexion à Internet ajoute de nombreux angles d'attaque permettant d'introduire des logiciels malveillants.

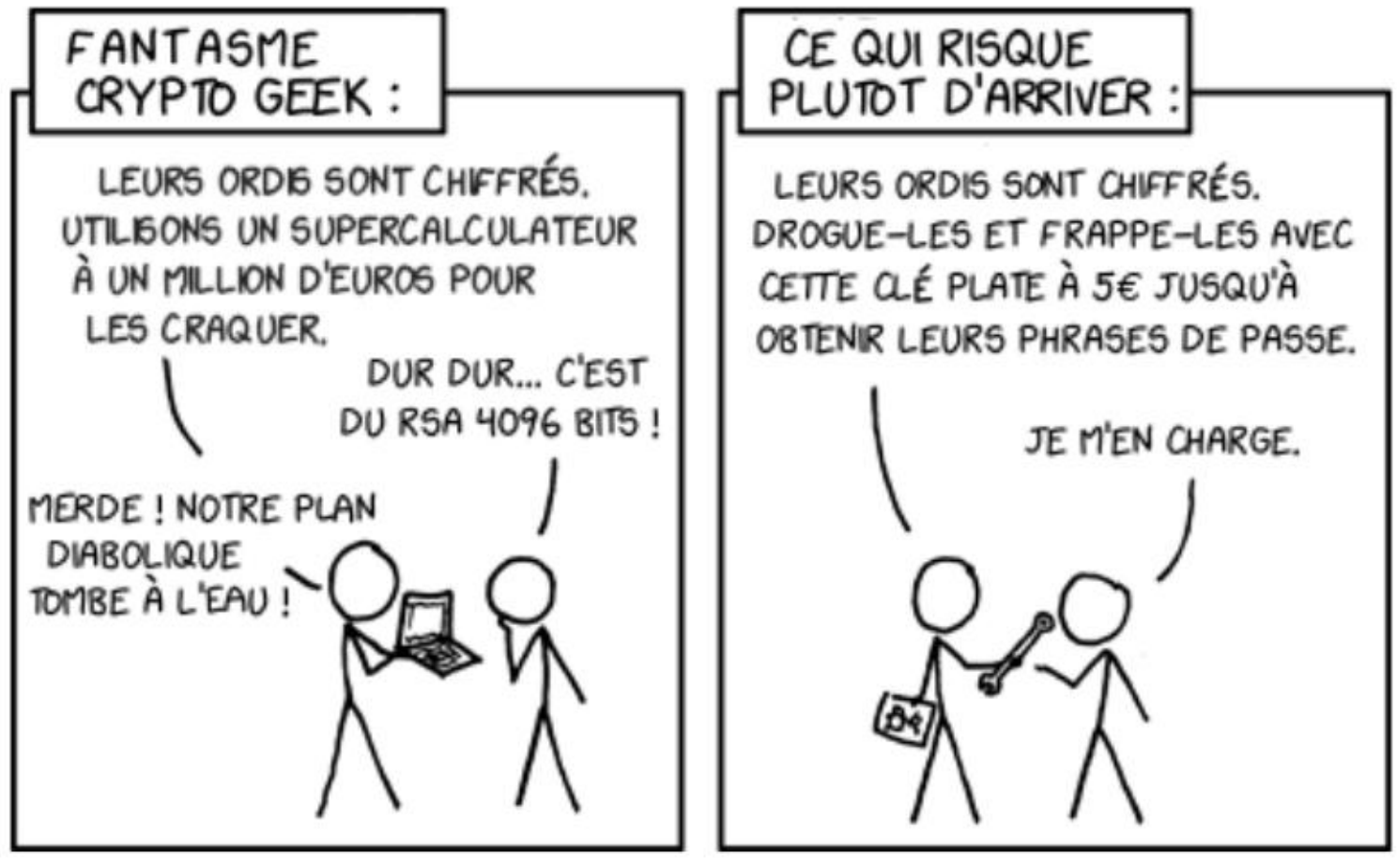
5. Dans le documentaire *Citizen Four* de Laura Poitras, on peut voir Edward Snowden mettre une couverture par dessus lui et son ordinateur pour taper sa phrase de passe.

Sixième angle d'attaque : la force brute

Attaquer un système cryptographique par « force brute », c'est-à-dire chercher la phrase de passe en testant une à une toutes les combinaisons possibles, est à la fois la plus simple et la plus lente des manières. Mais quand on ne peut pas mettre en œuvre un autre type d'attaque…

Pour notre disque chiffré lors de la première étape, ce type d'attaque demande énormément de temps (de nombreuses années) et/ou énormément d'argent, et des compétences pointues… du moins si la phrase de passe est solide.

On peut penser *a priori* que si une organisation est prête à mobiliser autant de ressources pour avoir accès à nos données, elle gagnerait amplement à mettre en place une des autres attaques listées ci-dessus, moins coûteuse et tout aussi efficace. Notamment celle d'aller demander directement la phrase de passe à la personne concernée, que ce soit de façon cordiale ou non…



Dessin issu de XKCD, traduit par nos soins (https://xkcd.com/538/).

Chapitre 10

Cas d'usage : travailler sur un document sensible

10.1 Contexte

Après avoir pris un nouveau départ, l'ordinateur utilisé pour mener ce projet à bien a été équipé d'un système chiffré. Bien. Survient alors le besoin de travailler sur un projet particulier, plus « sensible », par exemple :

page 71
page 119

- un tract doit être rédigé ;
- une affiche doit être dessinée ;
- un livre doit être maquetté puis exporté en PDF ;
- une fuite d'informations doit être organisée pour divulguer les affreuses pratiques d'une entreprise ;
- un film doit être monté et gravé sur DVD.

Dans tous ces cas, les problèmes à résoudre sont à peu près les mêmes.

Comme il serait trop pénible d'augmenter globalement, de nouveau, le niveau de sécurité de l'ordinateur, il est décidé que ce projet particulier doit bénéficier d'un traitement de faveur.

10.1.1 Conventions de vocabulaire

Par la suite, nous nommerons :

- les *fichiers de travail* : l'ensemble des fichiers nécessaires à la réalisation de l'œuvre (les images ou *rushes* utilisés comme bases, les documents enregistrés par le logiciel utilisé, *etc.*) ;
- l'*œuvre* : le résultat final (tract, affiche, *etc.*).

En somme, la matière première, et le produit fini.

10.2 Évaluer les risques

Tentons maintenant de définir les risques auxquels exposent le travail sur un document sensible.

10.2.1 Que veut-on protéger ?

Appliquons au cas présent les catégories définies lorsque nous parlions d'évaluation des risques :

page 63

- confidentialité : éviter qu'un œil indésirable ne découvre trop aisément l'œuvre et/ou les fichiers de travail ;
- intégrité : éviter que ces documents ne soient modifiés à notre insu ;

- accessibilité : faire en sorte que ces documents restent accessibles quand on en a besoin.

Ici, accessibilité et confidentialité sont prioritaires.

Accessibilité, car l'objectif principal est tout de même de réaliser l'œuvre. S'il fallait se rendre au pôle Nord pour ce faire, le projet risquerait fort de tomber à l'eau (glacée).

Et pour ce qui est de la confidentialité, tout dépend de la publicité de l'œuvre. Voyons donc ça de plus près.

Œuvre à diffusion restreinte

Si le contenu de l'œuvre n'est pas complètement public, voire parfaitement secret, il s'agit de dissimuler à la fois l'œuvre *et* les fichiers de travail.

Œuvre diffusée publiquement

Si l'œuvre a vocation à être publiée, la question de la confidentialité se ramène à celle de l'anonymat.

C'est alors, principalement, les fichiers de travail qui devront passer sous le tapis : en effet, les découvrir sur un ordinateur incite fortement à penser que ses propriétaires ont réalisé l'œuvre… avec les conséquences potentiellement désagréables que cela peut avoir.

Mais ce n'est pas tout : si l'œuvre, ou ses versions intermédiaires, sont stockées sur cet ordinateur (PDF, *etc.*), leur date de création est très probablement enregistrée dans le système de fichiers et dans des métadonnées. Le fait que cette date soit antérieure à la publication de l'œuvre peut aisément amener des adversaires à tirer des conclusions gênantes quant à sa généalogie.

page 24
page 30

10.2.2 Contre qui veut-on se protéger ?

Reprenons les menaces décrites dans le cas d'usage « un nouveau départ » : l'ordinateur utilisé pour réaliser l'œuvre peut être dérobé par de quelconques flics ou lors d'un cambriolage.

page 71

10.3 Quel système d'exploitation privilégier pour travailler sur le document ?

10.3.1 Décider des logiciels nécessaires

La première question qui se pose est : quels logiciels seront utilisés pour ce projet ?

- Si les logiciels nécessaires fonctionnent sous GNU/Linux, continuons la lecture de ce chapitre pour étudier les options qui s'offrent à nous.
- Si ces logiciels ne marchent que sous Windows (ou Mac OS), ça vaut le coup de chercher si des logiciels similaires sont disponibles sous Debian GNU/Linux. S'ils existent, les tester pour voir s'ils semblent fonctionnels pour ce projet.
- Si vraiment seuls des logiciels Windows sont satisfaisants, c'est dommage. Mais nous proposons tout de même un chemin praticable qui permet de limiter la casse. Allons donc voir à quoi ressemble cette méthode, en ignorant les paragraphes suivants, qui sont consacrés à GNU/Linux.

page 134
page 82

10.3.2 Utiliser un système *live* amnésique pour laisser le moins de traces possible

On pourrait imaginer configurer finement un système Debian chiffré pour qu'il conserve le moins de traces possible de nos activités sur le disque dur. Le problème

de cette approche, c'est qu'elle est de type « liste bloquée ». Nous en avons expliqué les limites : quel que soit le temps consacré, quelle que soit l'expertise mise au travail, même avec une compréhension particulièrement poussée des entrailles du système d'exploitation, on oublierait toujours une petite option bien cachée, il resterait toujours des traces indésirables auxquelles on n'avait pas pensé.

page 66

Un chapitre est consacré à l'installation d'un système Debian chiffré, mais l'ensemble des méthodes pour limiter les traces n'y est pas développé. Heureusement, certains systèmes *live* amnésiques fonctionnent sur le principe de la « liste autorisée » : tant qu'on ne le demande pas explicitement, aucune trace n'est laissée sur le disque dur.

page 119

page 113

En envisageant uniquement le critère « confidentialité », le système *live* bat donc l'autre à plate couture. En revanche, si son principal atout est d'être amnésique, cela peut présenter parfois un inconvénient. Ainsi, dans le cas où notre système *live* préféré ne fournit pas un logiciel indispensable au projet, il faut l'installer à chaque démarrage, ce qui peut fort heureusement être fait de manière automatique.

Si l'utilisation d'un système *live* est ainsi la solution la plus sûre, c'est aussi la solution la moins difficile à mettre en place au vu de la difficulté que représenterait l'installation d'un système Debian ne laissant que peu de traces. Dans la partie suivante, nous étudierons donc une politique de sécurité basée sur cette solution.

page suiv.

À noter qu'il est aussi possible d'installer un système Debian dans une machine virtuelle afin de satisfaire des besoins similaires, mais cette solution est moins adaptée et ne sera donc pas détaillée ici. On peut trouver de la documentation en ligne, même s'il est important de prendre pour Debian les mêmes précautions de compartimentation que celles développées dans le chapitre consacré à la création d'une machine virtuelle Windows.

page 163

10.4 Travailler sur un document sensible... sur un système *live*

page 79 Après avoir présenté le contexte dans le début de ce cas d'usage et décidé d'utiliser un système *live*, il reste à mettre cette solution en place... et à étudier ses limites.

10.4.1 Télécharger et installer le système *live*

Tous les systèmes *live* ne sont pas particulièrement destinés à des pratiques « sensibles ». Il importe donc de choisir un système spécialement conçu pour (tenter de) ne laisser aucune trace sur le disque dur de l'ordinateur sur lequel il est utilisé. Ce guide choisit de privilégier et de documenter le système *live* Tails.

Si l'on ne dispose pas encore d'une copie de la dernière version du système *live* Tails, suivre la recette pour télécharger et installer un système *live* « discret » (voir page 114).

Une fois notre périphérique Tails installé sur notre clé, on peut, si on veut, créer un espace de stockage chiffré pour enregistrer certains de nos documents ou réglages. Pour cela, se munir du système *live* précédemment installé et le démarrer (voir page 107). Suivre ensuite la recette pour créer et configurer un volume persistant dans Tails (voir page 116).

10.4.2 Installer un éventuel logiciel additionnel

Si l'on a besoin d'utiliser un logiciel qui n'est pas installé dans Tails et que l'on ne veut pas le réinstaller à chaque fois, suivre la recette pour installer un logiciel additionnel persistant dans Tails (voir page 117).

10.4.3 Utiliser le système *live*

Chaque fois que l'on souhaite travailler sur notre document, il suffit de se munir de la clé contenant notre système *live* et sa persistance chiffrée pour démarrer dessus (voir page 107). On doit alors activer le volume persistant (voir page 116).

10.4.4 Supprimer les données

Une fois notre projet terminé et imprimé ou publié en ligne (voir page 285), on peut éventuellement archiver le projet (voir page 89). Il nous faut ensuite supprimer le volume persistant (voir page 116) qui contient les données.

10.4.5 Ce n'est pas fini

Il reste à nettoyer les métadonnées (voir page 88) et à étudier les limites de notre approche (voir page 88).

10.5 Travailler sur un document sensible... sous Windows

page 79 Après avoir présenté le contexte dans le début de ce cas d'usage et, malgré tous les problèmes que pose l'utilisation de Windows, essayons maintenant de limiter un peu la casse.

10.5.1 Point de départ : une passoire et une boîte de rustines desséchées

Partons d'un ordinateur muni, de la façon la plus classique qui soit, d'un disque dur sur lequel Windows est installé. Nous ne nous appesantirons pas sur cette situation, la première partie de cet ouvrage ayant abondamment décrit les multiples problèmes qu'elle pose. Une passoire, en somme, pleine de trous de sécurité.

On peut donc imaginer coller quelques rustines sur cette passoire[1]. Faisons-en rapidement le tour.

Un disque dur, ça se démonte et ça se cache. Certes. Mais il y a les périodes où l'on s'en sert, parfois plusieurs jours ou semaines d'affilée. Cette rustine est basée sur deux hypothèses quelque peu osées :

- *Nous avons de la chance.* Il suffit en effet que l'accident (perquisition, cambriolage, *etc.*) survienne au mauvais moment pour que toute la confidentialité désirée soit réduite à néant.
- *Notre discipline est parfaitement rigoureuse.* En effet, si l'on oublie, ou qu'on ne prend pas le temps, d'aller « ranger » le disque dur quand on n'en a plus besoin, et que l'accident survient à ce moment-là, c'est perdu, fin de la partie.

Par ailleurs, des outils existent pour chiffrer des données sous Windows. Quelle que soit la confiance qu'on leur accorde, il n'en reste pas moins qu'ils s'appuient obligatoirement sur les fonctions offertes par la boîte noire qu'est Windows. On ne peut donc que s'en méfier, et, dans tous les cas, Windows, lui, aura accès à nos données *en clair*, et personne ne sait ce qu'il pourrait bien en faire.

Pour conclure ce petit tour dans la cour des miracles douteux, ajoutons que la seule « solution » possible dans le cas présent serait une approche de type liste bloquée, dont l'inefficacité a déjà été expliquée précédemment page 66

Il est maintenant temps de passer aux choses sérieuses.

10.5.2 Seconde étape : enfermer Windows dans un compartiment (presque) étanche

Ce qui commence à ressembler à une solution sérieuse, ce serait de faire fonctionner Windows dans un compartiment étanche, dans lequel on ouvrirait, quand c'est nécessaire et en connaissance de cause, une porte pour lui permettre de communiquer avec l'extérieur de façon strictement limitée.

En d'autres termes, mettre en place une solution basée sur une logique de type *liste autorisée* : rien ne pourrait entrer dans Windows ou en sortir *a priori*, et à partir de cette règle générale, on autorise des *exceptions*, au cas par cas, en réfléchissant à leur impact.

La *virtualisation*[2] permet de mettre en place ce type de systèmes. C'est un ensemble de techniques matérielles et logicielles qui permettent de faire fonctionner, sur un seul ordinateur, plusieurs systèmes d'exploitation, séparément les uns des autres, (presque) comme s'ils fonctionnaient sur des machines physiques distinctes.

Il est ainsi relativement facile, de nos jours, de faire fonctionner Windows **à l'intérieur** d'un système GNU/Linux, en lui coupant, par la même occasion, tout accès au réseau — et en particulier, en l'isolant d'Internet.

⚠ **Attention** : il est conseillé de lire l'intégralité de ce chapitre **avant** de se précipiter sur les recettes pratiques ; la description de l'hypothèse qui suit est assez longue, et ses limites sont étudiées à la fin de ce chapitre, où des contre-mesures sont envisagées. Il serait quelque peu dommage de passer quatre heures à suivre ces recettes, avant de se rendre compte qu'une tout autre solution serait, en fait, plus adéquate.

Commençons par résumer l'hypothèse proposée.

---

1. Archive INA, *La passoire des Shadoks* [https://www.youtube.com/watch?v=1Duiup2tWKA]
2. Pour plus d'informations, voir la page Wikipédia, 2020, *Virtualisation* [https://fr.wikipedia.org/wiki/Virtualisation].

L'idée est donc de faire fonctionner Windows dans un compartiment *a priori* étanche, **à l'intérieur** d'un système Debian chiffré tel que celui qui a pu être mis en place à la suite de la lecture du cas d'usage précédent. Ce qui servira de disque dur à Windows, c'est en fait un gros fichier stocké sur le disque dur de notre système Debian chiffré.

page 71

Installer le Gestionnaire de machines virtuelles

Il nous faut donc tout d'abord suivre la recette pour installer le Gestionnaire de machines virtuelles (voir page 163). Ce logiciel nous servira à lancer Windows dans un compartiment étanche.

Installer un Windows « propre » dans le Gestionnaire de machines virtuelles

Préparons une image de disque virtuel *propre* : pour cela, suivre la recette pour installer un Windows virtualisé (voir page 165). Cette recette explique comment installer Windows dans le Gestionnaire de machines virtuelles en lui coupant, **dès le départ**, tout accès au réseau.

À partir de ce moment-là, on qualifie Windows de système *invité* par le système Debian chiffré, qui, lui, est le système *hôte*.

Installer les logiciels nécessaires dans le Windows « propre »

Autant installer, dès maintenant, dans le Windows « propre », tout logiciel *non compromettant*[3] nécessaire à la réalisation des œuvres préméditées : ça évitera de le refaire au début de chaque nouveau projet… et ça évitera, souhaitons-le ardemment, d'utiliser une image Windows « sale » pour un nouveau projet, un jour où le temps presse.

Vu que le Windows *invité* n'a pas le droit de sortir de sa boîte pour aller chercher lui-même des fichiers, il est nécessaire de lui faire parvenir depuis « l'extérieur » les fichiers d'installation des logiciels nécessaires.

Une telle opération sera aussi utile, par la suite, pour lui envoyer toutes sortes de fichiers, et nous y reviendrons. Pour l'heure, vu que nous sommes en train de préparer une image de Windows « propre », servant de base à chaque nouveau projet, ne mélangeons pas tout, et contentons-nous de lui envoyer uniquement ce qui est nécessaire à l'installation des logiciels non compromettants souhaités.

Créons, sur le système hôte, un dossier nommé *Logiciels Windows*, et copions-y **uniquement** les fichiers nécessaires à l'installation des logiciels souhaités.

Puis partageons ce dossier avec le Windows *invité*. Pour cela, suivre la recette pour partager un dossier avec un système virtualisé (voir page 171).

Et en ce qui concerne l'installation des logiciels à l'intérieur du Windows *invité* : toute personne suffisamment accro à Windows pour lire ces pages est, sans aucun doute, plus compétente que celles qui écrivent ces lignes.

⚠ **Attention** : une fois cette étape effectuée, il est impératif de ne **rien** faire d'autre dans ce Windows virtualisé.

Prendre un instantané du Windows « propre »

Prenons maintenant un *instantané* de la machine virtuelle *propre* qui vient d'être préparée. C'est-à-dire : sauvegardons son état dans un coin. Par la suite, cet instantané servira de base de départ pour chaque nouveau projet.

Il faut donc suivre la recette pour prendre un instantané d'une machine virtuelle (voir page 168).

3. Par exemple, si l'on souhaite cacher le fait qu'on fabrique des films, avoir des logiciels de montage vidéo peut être compromettant.

Nouveau projet, nouveau départ

Mettons qu'un nouveau projet nécessitant l'utilisation de Windows débute ; voici la marche à suivre :

1. On restaure l'instantané de la machine virtuelle contenant l'installation de Windows propre.
2. La machine virtuelle peut maintenant être démarrée dans son compartiment étanche. Elle servira **exclusivement** pour le nouveau projet, et devient désormais une machine virtuelle *sale*.
3. Au sein de cette nouvelle machine virtuelle *sale*, une nouvelle utilisatrice Windows est créée. Le nom qui lui est attribué doit être différent **à chaque fois** qu'un nouveau projet est ainsi démarré, et cette utilisatrice servira **exclusivement** pour ce nouveau projet. Ceci, parce que les logiciels tendent à inscrire le nom de l'utilisatrice active dans les métadonnées des fichiers qu'ils enregistrent, et qu'il vaut mieux éviter de rendre possibles de fâcheux recoupements. page 30

Les détails techniques de la première étape sont expliqués dans la recette pour restaurer l'état d'une machine virtuelle à partir d'un instantané (voir page 168). En ce qui concerne la création d'une nouvelle utilisatrice sur la version de Windows utilisée, la personne lisant ces page est une fois encore certainement à même de la trouver du côté du *Panneau de configuration*.

Maintenant que nous avons un compartiment étanche, voyons comment y ouvrir des portes sélectivement, en fonction des besoins.

Comment envoyer des fichiers au Windows embastillé ? Vu que le Windows *invité* n'a pas le droit de sortir de sa boîte pour aller chercher lui-même des fichiers, il peut être nécessaire de lui en faire parvenir depuis « l'extérieur », par exemple :

- de la matière première (*rushes*, images ou textes provenant d'autres sources) ;
- un logiciel nécessaire au nouveau projet, et absent de l'image virtuelle « propre » que l'on vient de restaurer.

Nous avons déjà vu comment procéder, mais c'était dans un cas très particulier : l'installation de nouveaux logiciels dans un Windows « propre » *invité*. Partager des fichiers avec un Windows « sale » requiert davantage de réflexion et de précautions, que nous allons maintenant étudier.

La façon de faire est légèrement différente, en fonction du support sur lequel se trouvent, à l'origine, les fichiers à importer (CD, DVD, clé USB, dossier présent sur le disque dur du système chiffré), mais les précautions d'usage sont les mêmes :

- Windows doit **uniquement** avoir accès aux fichiers qu'on veut y importer, et c'est tout. Il n'est pas question de lui donner accès à un dossier qui contient, pêle-mêle, des fichiers concernant des projets qui ne devraient pas être recoupés entre eux. Si ça implique de commencer par une phase de tri et de rangement, eh bien, soit.
- Lorsque Windows a besoin de *lire* (recopier) les fichiers contenus dans un dossier, on lui donne **uniquement** accès en *lecture* à ce dossier. Moins on donne le droit à Windows d'écrire ici ou là, moins il laissera de traces gênantes.

Afin d'éviter de se mélanger les pinceaux, il est recommandé de :

- créer **un seul** dossier d'importation par projet ;
- nommer ce dossier de façon aussi explicite que possible ; par exemple : *Dossier lisible par Windows* ;
- ne jamais partager d'autres dossiers que celui-ci avec le Windows *invité*.

Des explications pratiques sont données dans la recette pour envoyer des fichiers au système virtualisé (voir page 171).

Comment faire sortir des fichiers du Windows embastillé ? Le Windows *invité* n'a pas le droit, par défaut, de laisser de traces en dehors de son compartiment étanche. Mais presque inévitablement vient le temps où il est nécessaire d'en faire sortir des fichiers, et, à ce moment-là, il nous faut l'autoriser explicitement. Par exemple :

- pour emmener à la boîte-à-copies, ou à l'imprimerie, un fichier PDF exporté ;
- pour projeter, sous forme de DVD, le film fraîchement réalisé.

Pour cela, on va exporter ces fichiers vers un dossier vide, dédié à cet usage, et stocké sur un volume chiffré qui peut être :

- une clé USB chiffrée, qu'on active sous Debian en tapant la phrase de passe correspondante ;
- le disque dur de la Debian chiffrée qui fait ici office de système *hôte*.

Ce dossier dédié sera partagé avec le Windows *invité*. Insistons sur les mots **vide** et **dédié** : Windows pourra lire et modifier tout ce que ce dossier contient, et il serait dommageable de lui permettre de lire des fichiers, quand on a seulement besoin d'exporter un fichier.

Si l'on a besoin de graver un DVD, ou pourra ensuite le faire à partir de Debian.

Afin d'éviter de se mélanger les pinceaux et de limiter la contagion, il est recommandé de :

- créer **un seul** dossier d'exportation par projet ;
- nommer ce dossier de façon aussi explicite que possible ; par exemple : *Dossier où Windows peut écrire* ;
- ne jamais partager d'autres dossiers que celui-ci avec le Windows *invité*, mis à part le dossier d'importation que le paragraphe précédent préconise.

Les recettes pour partager un dossier avec un système virtualisé (voir page 171) et pour chiffrer une clé USB (voir page 145) expliquent comment procéder pratiquement.

Quand le projet est terminé

Quand ce projet est terminé, il faut faire le ménage, mais avant toute chose :

1. l'œuvre résultante est exportée sur le support approprié (papier, DVD, *etc.*), en s'aidant du paragraphe précédent, qui explique comment faire sortir des fichiers du Windows *invité* ;
2. les fichiers de travail sont, si nécessaire, archivés (le cas d'usage suivant traitant, quelle coïncidence, de la question).

page 89

Puis vient l'heure du grand ménage, qui éliminera du système *hôte* le plus possible de traces du projet achevé :

- l'image de disque virtuel est restaurée à son état « propre » grâce à la recette pour restaurer l'état d'une machine virtuelle à partir d'un instantané (voir page 168) ;
- après avoir vérifié, une dernière fois, que tout ce qui doit être conservé a bien été archivé ailleurs, les dossiers partagés avec Windows sont effacés « pour de vrai » (voir page 141) ;
- les traces laissées sur le disque dur sont effacées « pour de vrai » (voir page 143).

Encore un nouveau projet ?

page préc.

Si un nouveau projet survient, nécessitant lui aussi d'utiliser Windows, ne réutilisons **pas** le même Windows *sale*. Retournons plutôt à l'étape « nouveau projet, nouveau départ ».

10.5.3 Troisième étape : attaques possibles et contre-mesures

L'hypothèse que nous venons de décrire est basée sur l'utilisation, comme système *hôte*, d'une Debian chiffrée. Toutes les attaques concernant cette Debian chiffrée sont donc applicables à la présente solution. Il est maintenant temps d'étudier les attaques praticables contre ce système.

page 72

Traces laissées sur notre Debian chiffrée

La plupart des traces les plus évidentes de ce projet sont séparées du reste du système : tous les fichiers de travail sont stockés dans le fichier contenant l'image de disque virtuel. Le nom de la machine virtuelle, sa configuration ainsi que ses périodes d'utilisation laisseront par contre d'autres traces sur notre système Debian.

Si la catastrophe arrive pendant la réalisation du projet Le disque dur de l'ordinateur utilisé contient les fichiers de travail à l'intérieur de l'image de disque virtuel.

Si la catastrophe arrive plus tard L'image de disque virtuel étant convenablement nettoyée lorsque le projet est achevé, si la catastrophe (céder face à la loi, découverte d'un problème dans le système cryptographique) arrive après coup, les traces résiduelles sur le disque dur seront moins évidentes, et moins nombreuses, que si l'on avait procédé de façon ordinaire.

Même si la catastrophe arrive après la fin du projet, c'est-à-dire après le nettoyage conseillé ici, il serait malvenu de se sentir immunisée, car comme le début de ce cas d'usage l'explique, l'inconvénient majeur de la méthode décrite ici est qu'elle est basée sur le principe de liste bloquée, principe abondamment décrié en ces pages… et il restera donc toujours des traces indésirables, auxquelles on n'avait pas pensé, sur le disque dur de l'ordinateur utilisé, en plus de celles qu'on connaît bien désormais : journaux, mémoires vive et « virtuelle », sauvegardes automatiques.

page 79
page 66
page 27

Si, malgré ces soucis, l'hypothèse que nous venons de décrire semble être un compromis acceptable, il est maintenant nécessaire de se renseigner sur les limites partagées par toutes les solutions envisagées dans ce cas d'usage.

page suiv.

Sinon, creusons un peu.

Aller plus loin

Admettons qu'une des attaques décrites à partir de la troisième étape du cas d'usage « un nouveau départ » semble crédible. Si elle réussissait, le contenu du disque dur chiffré du système *hôte* serait lisible, en clair, par l'attaquante. Or nos fichiers de travail sont, rappelons-le, contenus dans l'image de disque virtuel utilisée par notre Windows *invité*… qui est un bête fichier stocké sur le disque dur du système *hôte*. Ces fichiers de travail, ainsi que toute trace enregistrée par les logiciels utilisés dans Windows, deviennent alors lisibles par l'attaquante.

page 74

Nous allons envisager deux pistes permettant de limiter les dégâts. L'une est de type « liste bloquée », l'autre est de type « liste autorisée ».

Stocker l'image de disque virtuel en dehors du disque du système *hôte* Une idée est de stocker hors du disque dur du système *hôte* l'image de disque virtuel utilisée par le système Windows *invité*. Par exemple, sur un disque dur externe chiffré. Ainsi, même si le disque du système *hôte* est déchiffré, nos fichiers de travail restent inaccessibles… pourvu que le disque dur externe qui les contient ne soit pas à la portée de l'adversaire à ce moment-là.

Cette approche est de type « liste bloquée », avec tous les problèmes que ça pose. Les fichiers de travail et le système Windows ne sont pas enregistrés sur le disque dur

page 66

du système *hôte*. Mais il ne faut pas oublier que ces données seront utilisées par le Gestionnaire de machines virtuelles, qui lui fonctionne sur le système *hôte*. Comme le chapitre « traces à tous les étages » l'explique, diverses traces subsisteront donc, inévitablement, sur le disque dur **interne** de l'ordinateur utilisé.

page 27

Pour suivre cette piste :

cette page

- se renseigner sur les limites partagées par toutes les solutions envisagées dans ce cas d'usage ;

page 145

- se reporter à la recette permettant de chiffrer un disque dur externe.

Utiliser un système *live* comme système *hôte* Le pendant de cette approche « liste bloquée » est une solution de type « liste autorisée », conjuguant l'utilisation d'un système *live* et le stockage de l'image de disque virtuel sur un disque dur externe chiffré.

Pour suivre cette piste :

cette page

- se renseigner sur les limites partagées par toutes les solutions envisagées dans ce cas d'usage ;

page 145

- se reporter à la recette permettant de chiffrer un disque dur externe, et à celle qui explique comment utiliser un système *live*.

page 113

10.6 Nettoyer les métadonnées du document terminé

Une fois notre document terminé, on l'exportera dans un format adapté à l'échange de documents — par exemple un PDF pour imprimer un texte, un fichier AVI ou MKV pour publier une vidéo sur Internet, *etc.*

Considérons qu'on publie notre document sans prendre de plus amples précautions. Des adversaires à qui il déplairait vont probablement commencer par télécharger le document en quête d'éventuelles métadonnées qui le rapprocheraient des personnes qui l'ont réalisé.

page 185

Malgré les précautions qu'on a déjà prises, il est bon de nettoyer les éventuelles métadonnées présentes.

10.7 Limites communes à ces politiques de sécurité

Toute politique de sécurité étudiée dans ce cas d'usage est vulnérable à un certain nombre d'attaques, indépendamment de l'utilisation d'un système *live* ou de l'infâme Windows.

page 74

Les *angles d'attaques* du chapitre nouveau départ étudient certaines des attaques imaginables, relevant plus ou moins de la science-fiction, selon l'époque, le lieu, les protagonistes et les circonstances. Le moment est venu de les relire d'un œil nouveau.

page 13

Par ailleurs, la partie « problématiques » de ce tome abordait, de façon relativement générale, de nombreux modes de surveillance, qu'il peut être bon de réétudier à la lumière de la situation concrète qui nous occupe ; nommons en particulier les questions d'électricité, champs magnétiques et ondes radios, ainsi que les effets des divers mouchards.

page 21

page 31

Chapitre 11

Cas d'usage : archiver un projet achevé

11.1 Contexte

Un projet sensible touche à sa fin ; par exemple : un livre a été maquetté et imprimé ou un film a été monté, compressé et gravé sur DVD.

page 79

En général, il ne sera dès lors plus nécessaire de pouvoir accéder en permanence aux fichiers de travail (iconographie en haute résolution, *rushes* non compressés). Par contre, il peut être utile de pouvoir les retrouver plus tard, par exemple pour une réédition, une version mise à jour…

Vu qu'un système est d'autant plus susceptible d'être *attaqué* qu'il est fréquemment utilisé, autant extraire les informations rarement utilisées de l'ordinateur utilisé quotidiennement. De surcroît, il est plus facile de nier tout lien avec des fichiers, lorsqu'ils sont stockées sur une clé USB au fond d'un bois, que lorsqu'ils sont rangés sur le disque dur de l'ordinateur.

11.2 Est-ce bien nécessaire ?

La première question à se poser avant d'archiver de tels fichiers est la suivante : est-il *vraiment* nécessaire de les conserver ? Lorsqu'on ne dispose plus *du tout* d'une information, quiconque aura beau insister, personne ne sera en mesure de la donner, et c'est parfois la meilleure solution.

11.3 Évaluer les risques

11.3.1 Que veut-on protéger ?

Que deviennent les besoins définis lorsque nous parlions d'évaluation des risques, appliquées à ce cas ?

page 63

- confidentialité : éviter qu'un œil indésirable ne tombe trop aisément sur les informations archivées ;
- intégrité : éviter que ces informations ne soient modifiées à notre insu ;
- accessibilité : faire en sorte que ces informations restent accessibles quand on en a besoin.

Ici, l'accessibilité est secondaire par rapport à la confidentialité : toute l'idée de l'archivage est de faire un compromis, en rendant l'accès aux données plus difficile *pour tout le monde*, afin de leur offrir une meilleure confidentialité.

11.3.2 Contre qui veut-on se protéger ?

Les risques envisagés dans notre « nouveau départ » sont valables ici aussi : un

page 71

cambriolage, une perquisition ayant des motifs qui ne sont pas directement liés aux informations qu'on veut ici protéger.

Ajoutons, à ces risques, la possibilité que le livre ou le film produit déplaise à quelque commissaire, ministre, PDG (présidente-directrice générale) ou assimilée. Ça arrive. Admettons que :

- cette autorité a eu vent d'indices lui permettant de soupçonner qui a commis le chef d'œuvre ;
- cette autorité est en mesure de mandater une cohorte de flics au petit matin et au domicile des personnes soupçonnées.

Une telle intrusion inopportune débouchera au minimum, de façon tout aussi fâcheuse qu'évidente, sur la saisie de tout matériel informatique qui pourra y être découvert. Ce matériel sera ensuite remis à une experte en informatique qui pratiquera un genre d'autopsie visant à mettre au jour les données stockées sur ce matériel… ou l'ayant été.

page 42

11.4 Méthode

La méthode la plus simple à l'heure actuelle est :

1. créer une clé USB ou un disque dur externe chiffré (voir page 145) ;
2. copier les fichiers à archiver vers ce périphérique ;
3. supprimer et écraser le contenu des fichiers de travail (voir page 139).

Une fois ces opérations effectuées, la clé ou le disque dur pourra être entreposé dans un autre lieu que l'ordinateur utilisé couramment.

On pourrait envisager l'utilisation de CD ou de DVD, pour leur faible coût, mais il est plus complexe de chiffrer correctement des données sur ces supports que sur des clés USB, qui sont désormais monnaie courante et faciles à se procurer.

11.5 Quelle phrase de passe ?

page 103

Vu que les fichiers seront archivés sous forme chiffrée, il sera nécessaire de choisir une phrase de passe. Or, vu que la vocation est l'archivage, cette phrase de passe ne sera pas souvent utilisée. Et une phrase de passe rarement utilisée a toutes les chances d'être oubliée… rendant à peu près impossible l'accès aux données.

Face à ce problème, on peut envisager quelques pistes.

11.5.1 Écrire la phrase de passe quelque part

Toute la difficulté étant de savoir où l'écrire, ranger ce document pour pouvoir le retrouver… sans pour autant que d'autres puissent le retrouver et l'identifier comme une phrase de passe.

11.5.2 Utiliser la même phrase de passe que pour son système quotidien

page 119

La phrase de passe de son système quotidien, dans le cas où il est chiffré, est une phrase qu'on tape régulièrement, et dont on a toutes les chances de se souvenir.

Par contre :

- si on est forcé de révèler la phrase de passe commune, l'accès à l'archive devient également possible ;

- il est nécessaire d'avoir **très fortement** confiance dans les ordinateurs avec lesquels on accédera aux archives. Sinon, on peut se faire « piquer », à son insu, la phrase de passe, qui pourra ensuite être utilisée pour lire non seulement les informations archivées, mais aussi toutes les données stockées sur l'ordinateur d'usage quotidien.

11.5.3 Partager le secret à plusieurs

Il est possible de partager un secret à plusieurs. Cela impose de réunir plusieurs personnes afin de pouvoir accéder au contenu archivé. C'est à peser : ça peut compliquer la tâche, aussi bien pour des accès désirés qu'indésirables.

page 157

11.6 Un disque dur ? Une clé ? Plusieurs clés ?

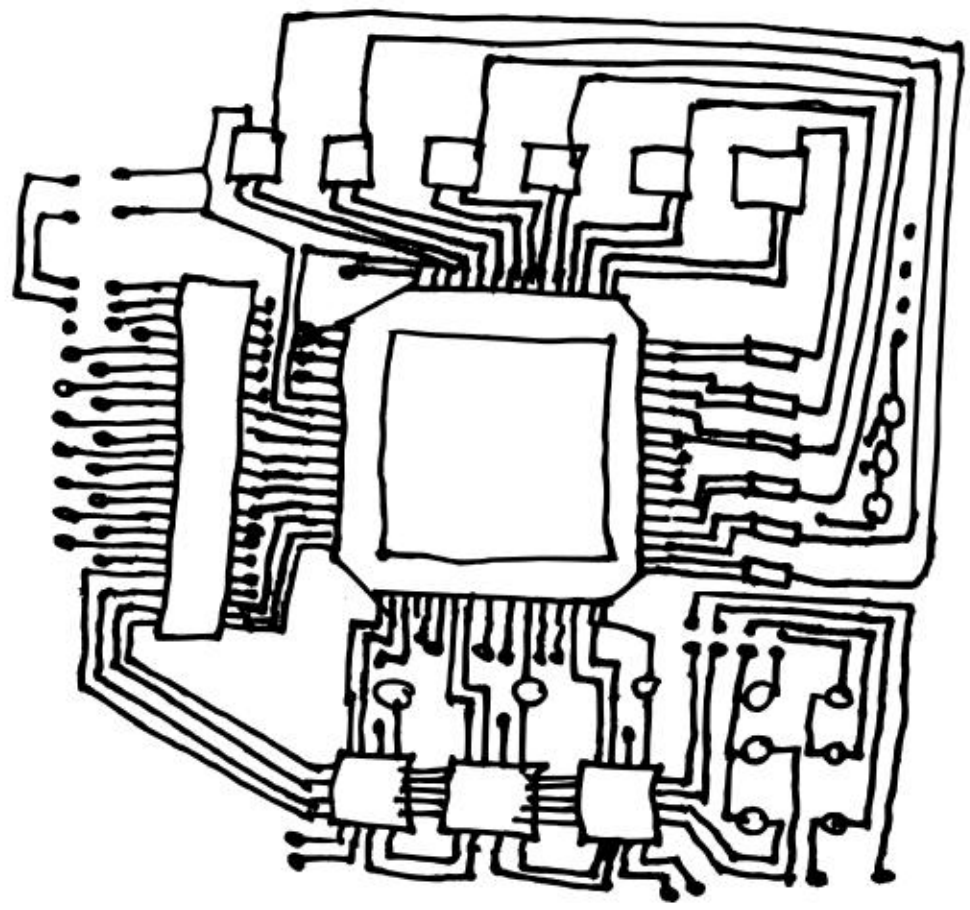
Selon les choix faits précédemment, entre autres sur la phrase de passe, on peut se demander quels supports utiliser. Sachant que sur le plan technique, le plus simple actuellement est d'avoir une seule phrase de passe par support.

Un disque dur externe peut contenir plus de données qu'une clé USB, et est donc parfois nécessaire : pour archiver un projet de vidéo, par exemple.

Archiver plusieurs projets sur un même support permet de se simplifier la tâche, mais il devient alors difficile de séparer les projets selon les niveaux de confidentialité souhaités. En effet, les personnes pouvant accéder aux archives d'un projet ont aussi accès aux autres, ce qui n'est pas forcément souhaitable. [1].

Par ailleurs, si la phrase de passe est un secret partagé, autant faciliter l'accès aux personnes partageant le secret, en ayant un support qu'elles peuvent se transmettre.

1. Le sujet de la compartimentation est développé dans le chapitre dédié aux identités contextuelles [page 246].



Troisième partie

Outils

Introduction

Dans cette troisième partie, nous expliquerons comment appliquer concrètement quelques-unes des pistes évoquées précédemment.

Cette partie est une annexe technique aux précédentes. Une fois comprises les problématiques liées à l'intimité dans le monde numérique, et une fois choisies les réponses adaptées, reste la question du « Comment faire ? » à laquelle cette annexe apporte certaines réponses.

page 59

Pour la plupart des recettes présentées dans ce guide, nous partons du principe que l'on utilise GNU/Linux avec le bureau GNOME ; ces recettes ont été écrites et testées sous Debian GNU/Linux version 11 (surnommée Bullseye) [1] et Tails version 5 [2] (*The Amnesic Incognito Live System*).

Pour autant, celles-ci sont généralement adaptables avec d'autres distributions basées sur Debian, telles qu'Ubuntu [3] ou Linux Mint [4].

Si l'on n'utilise pas encore GNU/Linux, on pourra consulter le cas d'usage un nouveau départ ou utiliser un système *live*.

page 71

page 113

Les procédures sont présentées pas à pas et expliquent, chaque fois que c'est possible, le sens des actions proposées.

L'ordre dans lequel chaque recette est détaillée est important. Sauf mention contraire, il est recommandé de ne pas sauter une étape puis de revenir en arrière. Le résultat obtenu pourrait être très différent de celui attendu.

Enfin, il est important d'utiliser la version la plus à jour de ce guide, car les logiciels évoluent. On pourra la trouver sur le site web https://guide.boum.org/.

1. https://www.debian.org/releases/bullseye/index.fr.html
2. https://tails.boum.org/index.fr.html
3. https://www.ubuntu-fr.org/
4. https://www.linuxmint.com/

Chapitre 12

Utiliser un terminal

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quinze à trente minutes.

Souvent, on utilise un ordinateur personnel en cliquant sur des menus et des icônes. Cependant, il existe une autre façon de lui « parler » : en tapant des bouts de texte que l'on appelle des « commandes ». Ce qui permet de taper ces commandes s'appelle « le terminal », « le *shell* » ou encore « la ligne de commande ».

Ce guide cherche le plus souvent possible à contourner l'utilisation de cet outil, qui est assez déroutant lorsque l'on n'y est pas habituée. Cependant, son usage s'est parfois avéré indispensable.

12.1 Qu'est-ce qu'un terminal ?

Une explication détaillée sur l'usage de lignes de commandes n'est pas l'objet de ce guide, et Internet regorge de tutoriels et de cours assurant très bien ce rôle[1]. Il semblait cependant nécessaire de poser quelques bases sur la manière de s'en servir.

Alors on va tout simplement commencer par ouvrir un terminal : sur un bureau GNOME 3, il faut ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `term` et cliquer sur *Terminal*. Apparaît alors une fenêtre qui indique :

```
IDENTIFIANT@LE-NOM-DE-LA-MACHINE:~$
```

À la fin se trouve un carré, appelé « curseur », qui correspond à l'endroit où inscrire le texte de la commande. Concrètement, avec l'identifiant *rabouane* sur une machine nommée *debian*, on aura sous les yeux :

```
rabouane@debian:~$
```

C'est à partir de cet état, appelé « invite de commande », que l'on peut taper directement les commandes que l'on veut faire exécuter à l'ordinateur.

L'effet final de ces commandes est souvent le même que celui qu'on peut obtenir en cliquant au bon endroit dans une interface graphique.

Par exemple, si dans le terminal qu'on vient d'ouvrir, on écrit `firefox` puis qu'on tape sur *Entrée* (↵ ou return), le résultat est qu'on ouvre le navigateur web *Firefox*. Par contre, on ne pourra pas entrer de nouvelle commande dans notre terminal tant que l'on n'aura pas quitté le navigateur. On aurait pu faire exactement la même

1. Entre autres, une page sur *ubuntu-fr.org* [https://doc.ubuntu-fr.org/console] qui se termine elle-même par d'autres liens.

chose avec l'interface graphique en appuyant sur la touche [⊞] ([⌘] sur un Mac) et en tapant `navig` puis en cliquant sur *Firefox ESR*.

Dans le cadre de ce guide, l'intérêt du terminal est surtout qu'il permet d'effectuer des actions qu'aucune interface graphique ne propose pour le moment.

12.2 À propos des commandes

Les commandes sont comme des ordres qu'on donne à l'ordinateur par le biais du terminal. Ces « lignes de commande » ont leur propre langage, avec leurs mots, leurs lettres, et leur syntaxe. Quelques remarques à ce sujet sont donc utiles.

12.2.1 Syntaxe

Prenons par exemple cette commande, `sfill`, qui permet à peu près les mêmes opérations que `nautilus-wipe`, un outil graphique qui sera présenté plus tard : page 143

$$\underbrace{\texttt{sfill}}_{\text{commande}} \quad \underbrace{\texttt{-l}}_{\text{option}} \quad \underbrace{\texttt{-v}}_{\text{option}} \quad \underbrace{\texttt{/home}}_{\text{argument}}$$

Dans cette ligne de commande, on peut voir, dans l'ordre :

- la *commande* que l'on appelle est `sfill`. La commande est en général un programme installé sur le système ;
- deux *options*, `-l` et `-v` qui modifient le comportement du programme `sfill`. Ces dernières peuvent être facultatives selon le programme (et commencent par un ou deux tirets pour qu'on les distingue) ;
- un *argument* `/home` qui précise ce sur quoi va travailler la commande. Il peut y en avoir plusieurs, ou aucun, tout dépend de la commande.

Chacun de ces éléments doit être séparé des autres par un (ou plusieurs) espace(s). Il y a donc un espace entre la commande et la première option, entre la première option et la suivante, entre la dernière option et le premier argument, entre le premier argument et les suivants, *etc.*

Pour connaître les options et les arguments d'une commande, pas de mystère : chacune dispose normalement d'une page de manuel. Pour y accéder, il suffit de taper dans le Terminal `man` suivi du nom de la commande, puis d'appuyer sur la touche *Entrée* ([↵] ou [return]). Ces dernières peuvent toutefois être difficiles à comprendre par leur aspect technique, et ne sont parfois disponibles qu'en anglais.

12.2.2 Insertion du chemin d'un fichier

Lors de l'utilisation d'un terminal, on a souvent besoin d'indiquer des dossiers et des fichiers. On parle de « chemin » car on décrit généralement dans quel dossier et sous-dossier un fichier se trouve. Pour séparer un dossier de ce qu'il contient, on utilise le caractère `/` (qui se prononce « slash »).

Pour donner un exemple, voici le *chemin* du document `recette.txt` qui se trouve dans le dossier `Documents` du dossier personnel du compte `alligator` :

```
/home/alligator/Documents/recette.txt
```

Comme beaucoup de commandes attendent des noms de fichiers comme arguments, cela devient vite fastidieux de taper leurs chemins complets à la main. Il y a cependant un moyen plus simple d'insérer un chemin : quand on attrape avec la souris l'icône d'un fichier, et qu'on le déplace pour le lâcher sur le terminal, son chemin s'écrit là où se trouve le curseur.

Cela ne marche cependant qu'avec les « vrais » fichiers ou dossiers. On obtiendra un nom bizarre qui ne fonctionnera pas, par exemple, pour les fichiers mis à la corbeille, l'icône du *Dossier personnel* sur le bureau ou avec les icônes de clés USB.

12.2.3 Exécution

Une fois que l'on a tapé une commande, on demande à l'ordinateur de l'« exécuter » en appuyant sur la touche *Entrée* (↵ ou return).

12.2.4 Fin ou interruption de la commande

L'exécution de la commande prend plus ou moins de temps. Lorsqu'elle est terminée, le terminal retourne toujours à l'état où il était avant qu'on lance la commande, l'« invite de commande » :

```
rabouane@debian:~$
```

On dit alors que le terminal « rend la main ».

Si on souhaite interrompre l'exécution d'une commande avant qu'elle soit terminée, on peut appuyer sur la touche Ctrl, et tout en laissant cette touche enfoncée appuyer sur la touche C. On arrête alors la commande immédiatement, un peu comme quand on ferme la fenêtre d'un programme.

12.2.5 Typographie

La plupart des symboles utilisés pour entrer les commandes complètes sont des symboles courants. Lorsqu'une commande emploie le symbole « - », il s'agit du « tiret » qu'on peut obtenir en tapant (sur un clavier français) la touche 6. Pour un « ' » (apostrophe droite), c'est la touche 4.

D'autres symboles sont rarement utilisés en dehors du terminal, mais sont disponibles sur les claviers standards. Ils sont même indiqués sur le clavier, et accessibles à l'aide de la touche Alt de droite, notée Alt Gr. Voici, en se basant sur un clavier de PC français standard, la correspondance de quelques touches avec les symboles qu'elles écrivent, et leur nom (bien peu seront en fait utilisées dans ce guide) :

Touches	Résultat	Nom du symbole
Alt Gr + 2	~	tilde
Alt Gr + 3	#	dièse
Alt Gr + 4	{	accolade gauche
Alt Gr + 5	[	crochet gauche
Alt Gr + 6	|	*pipe*
Alt Gr + 8	\	antislash
Alt Gr + 0	@	arobase
Alt Gr +)	]	crochet droit
Alt Gr + =	}	accolade droite

12.2.6 Noms à remplacer

Parfois, on précise que l'on va nommer quelque chose que l'on a trouvé pour le réutiliser plus tard. Par exemple, on dira que l'identifiant est `LOGIN`. Mettons qu'on travaille sous l'identifiant `paquerette`. Lorsqu'on écrira « taper `LOGIN` en remplaçant `LOGIN` par l'identifiant de son compte », il faudra taper en réalité `paquerette`.

12.3 Privilèges d'administration

Certaines commandes qui viennent modifier le système nécessitent des droits d'administration. Elles pourront alors accéder à l'intégralité du système sans restriction, avec les risques que cela comporte.

Pour exécuter une commande avec les droits d'administration, il faut mettre `pkexec` avant le nom de la commande. Une fenêtre demande alors un mot de passe avant d'exécuter la commande.

12.4 Mise en garde

Plus encore que pour les recettes dont on parlait plus haut, les commandes doivent être tapées très précisément. Oublier un espace, omettre une option, se tromper de symbole, être imprécis dans un argument, c'est changer le sens de la commande.

Et comme l'ordinateur effectue *exactement* ce qui est demandé, si on change la commande, il fera *exactement autre chose*...

12.5 Un exercice

On va créer un fichier vide nommé « essai », qu'on va ensuite supprimer (sans recouvrir son contenu).

Dans un terminal, entrer la commande :

```
touch essai
```

Et taper sur *Entrée* (↵ ou return) pour que l'ordinateur l'exécute.

La *commande* `touch` donne l'ordre de créer un fichier vide ; l'*argument* `essai` donne le nom de ce fichier. Aucune option n'est utilisée.

On peut alors vérifier que ce fichier a été créé en lançant la commande `ls` (qui signifie « lister ») :

```
ls
```

Une fois la commande lancée, l'ordinateur répond avec une liste. Sur celui utilisé pour les tests, cela donne :

```
Bureau
essai
```

`Bureau` est le nom d'un dossier qui existait déjà avant, et `essai` le nom du fichier qu'on vient de créer. Un autre ordinateur aurait pu répondre avec de nombreux autres fichiers en plus de `Bureau` et de `essai`.

Ce que répond la commande `ls` n'est qu'une autre manière de voir ce que l'on peut obtenir par ailleurs. En cliquant sur l'icône du *Dossier personnel* sur le bureau, on pourra noter dans le navigateur de fichiers l'apparition d'une nouvelle icône représentant le fichier `essai` que l'on vient juste de créer.

On va maintenant supprimer ce fichier. La ligne de commande pour le faire a pour syntaxe générale :

```
rm [options] NOM-DU-FICHIER-A-SUPPRIMER
```

On va utiliser l'option `-v` qui, dans le cadre de cette commande, demande à l'ordinateur d'être « bavard » (on parle de « mode verbeux ») sur les actions qu'il va effectuer.

Pour insérer le nom du fichier à supprimer, on va utiliser l'astuce donnée précédemment pour indiquer le chemin du fichier. On va donc :

- taper `rm -v` dans notre terminal,
- taper un espace afin de séparer l'option `-v` de la suite,

- dans la fenêtre du *Dossier personnel*, on va prendre avec la souris l'icône du fichier `essai` et la déposer dans le terminal.

À la fin de cette opération, on doit obtenir quelque chose comme :

```
rm -v '/home/LOGIN/essai'
```

On peut alors appuyer sur la touche *Entrée* (↵ ou return) et constater que l'ordinateur répond :

```
« /home/LOGIN/essai » supprimé
```

Cela indique qu'il a bien supprimé le fichier demandé. On peut encore vérifier son absence en lançant un nouveau `ls` :

```
ls
```

On constate l'absence de `essai` dans la liste que nous renvoie la commande. Sur le même ordinateur que tout à l'heure, cela donne maintenant :

```
Bureau
```

Et l'icône doit également avoir disparu dans le navigateur de fichiers. Apparemment, il a donc été supprimé, même si, comme expliqué dans la première partie, son contenu existe encore sur le disque. Comme c'était un fichier vide nommé « essai », on peut se dire que ce n'est pas bien grave.

page 42

12.6 Attention aux traces !

La plupart des *shells* enregistrent automatiquement les lignes de commande que l'on a tapées dans un fichier « d'historique ». C'est bien pratique pour retrouver plus tard des commandes que l'on a pu utiliser, mais cela laisse également sur le disque une trace de nos activités.

page 29

Le *shell* standard dans Debian s'appelle `bash`. Avec ce dernier, pour désactiver temporairement l'enregistrement de l'historique dans le terminal que l'on utilise, il suffit de faire :

```
unset HISTFILE
```

Par ailleurs, les commandes sont enregistrées dans le fichier caché `.bash_history` (qui se trouve dans le *Dossier personnel*). On peut donc avoir envie de le nettoyer de temps en temps.

page 141

12.7 Pour aller plus loin

Cette première expérience avec cette fenêtre pleine de petits caractères pourrait être le début d'une longue passion. Pour l'entretenir, rien de mieux que de prendre le temps de lire le tutoriel « Linux en mode texte : consolez-vous ![2] » du livre *Linux aux petits oignons* ou la partie « La console, ça se mange ?[3] » du tutoriel *Reprenez le contrôle à l'aide de Linux !*.

2. https://fr.calameo.com/read/005322362565c72e1efe8
3. https://web.archive.org/web/20210920080224/https://sdz.tdct.org/sdz/reprenez-le-controle-a-l-aide-de-linux.html#Laconsoleasemange

Chapitre 13

Choisir une phrase de passe

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Dix minutes environ.

Une « phrase de passe » (ou *passphrase* en anglais) est un secret qui sert à protéger des données chiffrées. C'est ce qu'on utilise pour chiffrer un disque dur ou des documents, voire, comme nous le verrons dans le second tome de cet ouvrage, des clés cryptographiques.

page 47

On parle de *phrase* plutôt que de *mot* de passe car un seul *mot*, aussi bizarre et compliqué soit-il, est beaucoup moins résistant qu'une simple phrase de plusieurs mots. On considère qu'une phrase de passe doit être constituée d'au moins dix mots. Mais plus il y en a, mieux c'est !

Un critère important, parfois négligé : une bonne phrase de passe est une phrase de passe dont on peut *se souvenir*[1]. Cela évite de la noter sur un papier, grave erreur qui rend caduc l'intérêt de se faire une phrase de passe béton. Mais, et c'est tout aussi important, une bonne phrase de passe doit être *aussi difficile à deviner que possible*. Évitons donc la phrase de passe formée de 15 mots composés de caractères aléatoires qu'on aura oubliée à peine 15 minutes après l'avoir trouvée, autant que les paroles d'un tube disco des années 80.

Une technique pour trouver une bonne phrase de passe, difficile à deviner, mais néanmoins facile à retenir, serait de fabriquer une phrase qui n'est pas issue d'un texte existant. En effet, que ce soit des paroles de chansons, le vers d'un poème, ou une citation d'un livre, des outils comme le projet Gutenberg[2] rendent de plus en plus facile le test de phrases de passe tirées de la littérature existante[3].

Toutefois, l'utilisation de l'expression « phrase de passe » peut conduire à vouloir choisir une phrase qui a du sens, ce qui aurait comme désavantage de perdre le côté aléatoire qui renforce la sécurité du mot de passe.

Il faut donc s'en remettre à son imagination pour créer une phrase de passe et voici quelques pistes quant aux bonnes habitudes à avoir lors du choix d'une phrase de passe :

1. Choisir dix mots au hasard qui n'ont rien à voir les uns avec les autres, par exemple en ouvrant un ou des livres aléatoirement et en gardant le premier mot sur lequel nos yeux tombent.

---

1. Randall Munroe, 2014, *Complexité du mot de passe* [https://xkcd.lapin.org/index.php?number=936].
2. Wikipédia, 2017, *Projet Gutenberg* [https://fr.wikipedia.org/wiki/Projet_Gutenberg].
3. Dan Goodin, 2013, *How the Bible and YouTube are fueling the next frontier of password cracking* [https://arstechnica.com/security/2013/10/how-the-bible-and-youtube-are-fueling-the-next-frontier-of-password-cracking/] (en anglais).

2. Souvent des logiciels nous imposent de mettre des chiffres ou des caractères spéciaux. Il est alors possible de trouver dans ces mots des choses à modifier. Sachant que cette étape n'est vraiment pas nécessaire du point de vue de la sécurité et risque surtout de rendre la phrase plus difficile à se souvenir. Il peut s'agir d'ajouter de l'argot, des mots de différentes langues, mettre des majuscules ou des espaces là où on ne les attend pas, remplacer des caractères par d'autres, laisser libre cours à notre imagination quant à l'orthographe, *etc.*
3. Se fabriquer un moyen mnémotechnique pour s'en souvenir. Exemple : broder une structure narrative avec ces mots peut aider à se souvenir de la phrase de passe.

Il est préférable d'utiliser uniquement les caractères qu'on trouve dans toutes les variantes de clavier ; autrement dit d'éviter les caractères accentués ou tout autre symbole spécifique aux langues locales. Cela peut éviter des problèmes de touches absentes ou difficiles à retrouver, et surtout de mauvais codage des caractères, si l'on est amenée à taper notre phrase de passe sur un clavier différent de celui dont on a l'habitude.



Pour aller plus loin…

Afin de générer une phrase de passe de dix mots pris au hasard, on peut aussi utiliser le gestionnaire de mots de passe KeePassXC (voir page 355).

Par défaut, cet outil inclut une liste de mots en anglais, mais il est possible de lui spécifier une autre liste de mots[4] en rajoutant cette dernière, sous la forme d'un simple fichier texte contenant un mot par ligne, dans le dossier `/usr/share/keepassxc/wordlists`. Cette opération doit être effectuée en tant que superutilisatrice.

Il faut ensuite démarrer KeePassXC et aller dans le menu *Outils* puis *Générateur de mot de passe*. Dans l'onglet *Phrase de passe*, on peut choisir la liste de mots à utiliser (si plusieurs sont disponibles) ainsi que le nombre de mots. La phrase de passe ainsi générée apparaît juste au-dessus.

Le nombre de mots nécessaires pour qu'une phrase de passe soit difficile à deviner varie selon la taille de la liste de mots. L'indicateur *Entropie*, situé à droite, en dessous de la phrase de passe, donne ainsi une mesure de cette difficulté : plus l'entropie est grande, mieux c'est. Une bonne phrase de passe requiert une entropie de 128 bits environ.

Un exemple, trouver au hasard dix mots :

> sembler bridge frein payante sortant autruche dater licences degauchir piller

Si un logiciel exige d'ajouter des symboles ou des chiffres, on peut faire des phrases, sans beaucoup se compliquer la vie. Par exemple :

> Sembler bridge frein payante. Sortant autruche, dater licences ! degauchir +piller-1984

Et on pourra imaginer une phrase, avec ces mots, qui serve de moyen mnémotechnique :

> Il peut sembler que jouer au bridge mette un frein car elle est payante. En sortant l'autruche, dater ses licences ! Dégauchir et piller, sans surveillance

4. On peut par exemple utiliser la liste de mots en français proposée par mbelivo [https://raw.githubusercontent.com/mbelivo/diceware-wordlists-fr/master/wordlist_fr_5d.txt]. Il est cependant nécessaire de l'adapter au format utilisé par KeePassXC, ce que l'on peut faire grâce à la commande suivante exécutée dans un terminal depuis le dossier où se trouve le fichier en question :
`cut -d' ' -f2 < wordlist_fr_5d.txt > wordlist_fr_5d_keepassxc.txt`

On pourra alors, au choix, utiliser la liste de mots aléatoires uniquement ou bien la phrase complète comme phrase de passe. Dans le second cas, il faudra cependant faire attention à l'utilisation de caractères spéciaux, comme mentionné plus haut.

Une fois les données chiffrées avec notre nouvelle phrase de passe, c'est une bonne idée de l'utiliser tout de suite une bonne dizaine de fois pour déchiffrer les données. On peut même la noter sur un bout de papier au moment de sa création pour être sûre de s'en souvenir quand on l'utilisera la première fois (il faut évidemment penser à détruire le papier dans un deuxième temps). Cela permettra d'apprendre un peu à ses doigts comment taper cette nouvelle phrase et ainsi la mémoriser mentalement et physiquement.

Enfin, n'oublions pas que si trouver une telle phrase de passe n'est pas sans effort, il faut en plus en trouver une différente pour chaque support que l'on chiffre. L'usage d'une même phrase de passe, ou pire d'un même mot de passe, pour une variété de choses différentes, peut s'avérer désastreux si elle est dévoilée.

De plus, on ne doit jamais utiliser comme mot de passe pour un service en ligne une phrase de passe qui sert aussi à verrouiller un secret cryptographique. En effet, si ce service en ligne se faisait pirater notre phrase de passe serait alors connue des pirates et potentiellement vendue à d'autres personnes.

page 235

Chapitre 14

Démarrer sur un CD, un DVD ou une clé USB

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Une minute à vingt minutes environ.

On va voir ici comment démarrer un ordinateur sur un média externe, par exemple un CD d'installation de Debian, ou un système *live* sur une clé USB.

Parfois, en particulier sur les ordinateurs modernes, c'est très simple. D'autres fois, c'est un peu à s'arracher les cheveux…

Quand on démarre un ordinateur, c'est le microprogramme (BIOS ou UEFI) qui s'exécute en premier. On a vu que c'est lui qui permet de choisir le périphérique (disque dur, clé USB, CD ou DVD, *etc.*) où se trouve le système d'exploitation à démarrer. page 20

14.1 Essayer naïvement

Commencer par mettre le média externe puis (re)démarrer l'ordinateur. Parfois, ça marche tout seul. Si c'est le cas, c'est gagné, lire la suite de ce chapitre est inutile !

14.2 Tenter un choix ponctuel du périphérique de démarrage

Avec les microprogrammes récents, il est souvent possible de choisir un périphérique de démarrage au cas par cas. Mais ce n'est pas toujours possible, notamment pour certains ordinateurs équipés de Windows (à partir de la version 8), pour lesquels la manipulation est plus compliquée. Il faudra, entre autres, désactiver le *Secure boot*[1] et sans doute chercher sur Internet comment démarrer sur une clé USB avec ce modèle d'ordinateur particulier.

(Re)démarrer l'ordinateur en regardant attentivement les tout premiers messages qui s'affichent à l'écran. Chercher des messages en anglais qui ressembleraient à :

- `Press [KEY] to select temporary boot device`
- `[KEY] = Boot menu`
- `[KEY] to enter MultiBoot Selection Menu`

Ces messages disent d'utiliser la touche `KEY` pour choisir un périphérique de démarrage. Cette touche est souvent F2 ou F12 ou F9 ou Échap.

Sur les Mac, il existe un équivalent de cette possibilité : immédiatement après l'allumage de l'ordinateur, il faut appuyer et maintenir la touche alt (parfois également

1. Comment désactiver le secure boot [https://doc.ubuntu-fr.org/desactiver_secure_boot].

marquée [option]). Au bout d'un moment, on doit normalement voir apparaître le *Gestionnaire de démarrage*[2].

Mais revenons à nos PC. Souvent, le microprogramme va trop vite, on n'a pas le temps de lire le message, de le comprendre et d'appuyer sur la touche. Qu'à cela ne tienne, une fois la bonne touche identifiée, redémarrer encore la machine et appuyer sur la touche en question (ne pas maintenir la touche enfoncée, mais la presser puis la relâcher plusieurs fois) dès l'allumage de l'ordinateur.

Si tout va bien, un message comme celui-ci s'affiche :

```
+----------------------------------+
| Boot Menu                        |
+----------------------------------+
|                                  |
| 1: Removable Devices             |
| 2: Hard Drive                    |
| 3: DVD-ROM                       |
| 4: Network boot                  |
|                                  |
|    <Enter Setup>                 |
|                                  |
+----------------------------------+
```

Si ça marche, c'est gagné. Choisir la bonne entrée dans ce menu, en se déplacant avec les flèches du clavier [↑] et [↓], puis appuyer sur *Entrée* ([↵] ou [return]). Souvent, il faut deviner le terme employé par le microprogramme pour désigner notre périphérique. Par exemple, pour démarrer sur une clé USB, choisir `Removable Devices` (pour « Périphériques Amovibles »). L'ordinateur va démarrer sur le périphérique sélectionné. Lire la suite est inutile !

14.3 Modifier les paramètres du microprogramme

⚠ Le microprogramme permet de configurer le fonctionnement matériel de l'ordinateur. C'est une bonne idée de ne pas faire plein de changements d'un seul coup et de noter les changements effectués sur un bout de papier. Ainsi, si l'ordinateur ne fonctionne plus, on peut revenir en arrière. En cas de doute, sortir sans sauvegarder puis recommencer.

Si choisir un périphérique de démarrage temporaire ne fonctionne pas, il va falloir rentrer dans le microprogramme pour paramétrer manuellement l'ordre de démarrage. Le microprogramme teste les périphériques dans l'ordre configuré et démarre le premier système d'exploitation trouvé. L'enjeu de la modification est de mettre notre média externe au sommet de cette liste.

Pour pimenter un peu la chose, les microprogrammes sont quasiment tous différents, de telle sorte qu'il est impossible de donner une recette qui marche systématiquement[3].

14.3.1 Entrer dans l'interface de configuration du microprogramme

Encore une fois, il s'agit de (re)démarrer l'ordinateur en regardant attentivement les premiers messages qui s'affichent à l'écran. Chercher des messages en anglais qui ressembleraient à :

- `Press [KEY] to enter setup`
- `Setup: [KEY]`
- `[KEY] = Setup`
- `Enter BIOS by pressing [KEY]`

2. http://support.apple.com/kb/HT1310?viewlocale=fr_FR
3. Des tutoriels illustrés pour quelques BIOS sont disponibles sur cette page [https://www.hiren.info/pages/bios-boot-cdrom] (en anglais).

- `Press [KEY] to enter BIOS setup`
- `Press [KEY] to access BIOS`
- `Press [KEY] to access system configuration`
- `For setup hit [KEY]`

Ces messages disent d'utiliser la touche `KEY` pour entrer dans le microprogramme. Cette touche est souvent Suppr (Delete, Del) ou F2, parfois F1, F10, F12, Échap, Tab (⇆ ou →).

Voici un tableau qui résume les touches d'accès au microprogramme pour quelques fabricants d'ordinateurs communs [4].

Fabricant	**Touches observées**
Acer	F1, F2, Suppr
Compaq	F10
Dell	F2
Fujitsu	F2
HP	F1, F2, F10, F12, Échap
IBM	F1
Lenovo	F1, *Entrée* (↵)
NEC	F2
Packard Bell	F1, F2, Suppr
Samsung	F2
Sony	F1, F2, F3
Toshiba	F1, F2, F12, Échap

Souvent, le microprogramme va trop vite, et on n'a pas le temps de lire le message, de le comprendre et d'appuyer sur la touche. Qu'à cela ne tienne, une fois la bonne touche identifiée, redémarrer encore la machine en appuyant sur la touche en question (ne pas maintenir la touche enfoncée, mais la presser puis la relâcher plusieurs fois). Parfois, l'ordinateur se perd et plante. Dans ce cas, redémarrer et réessayer…

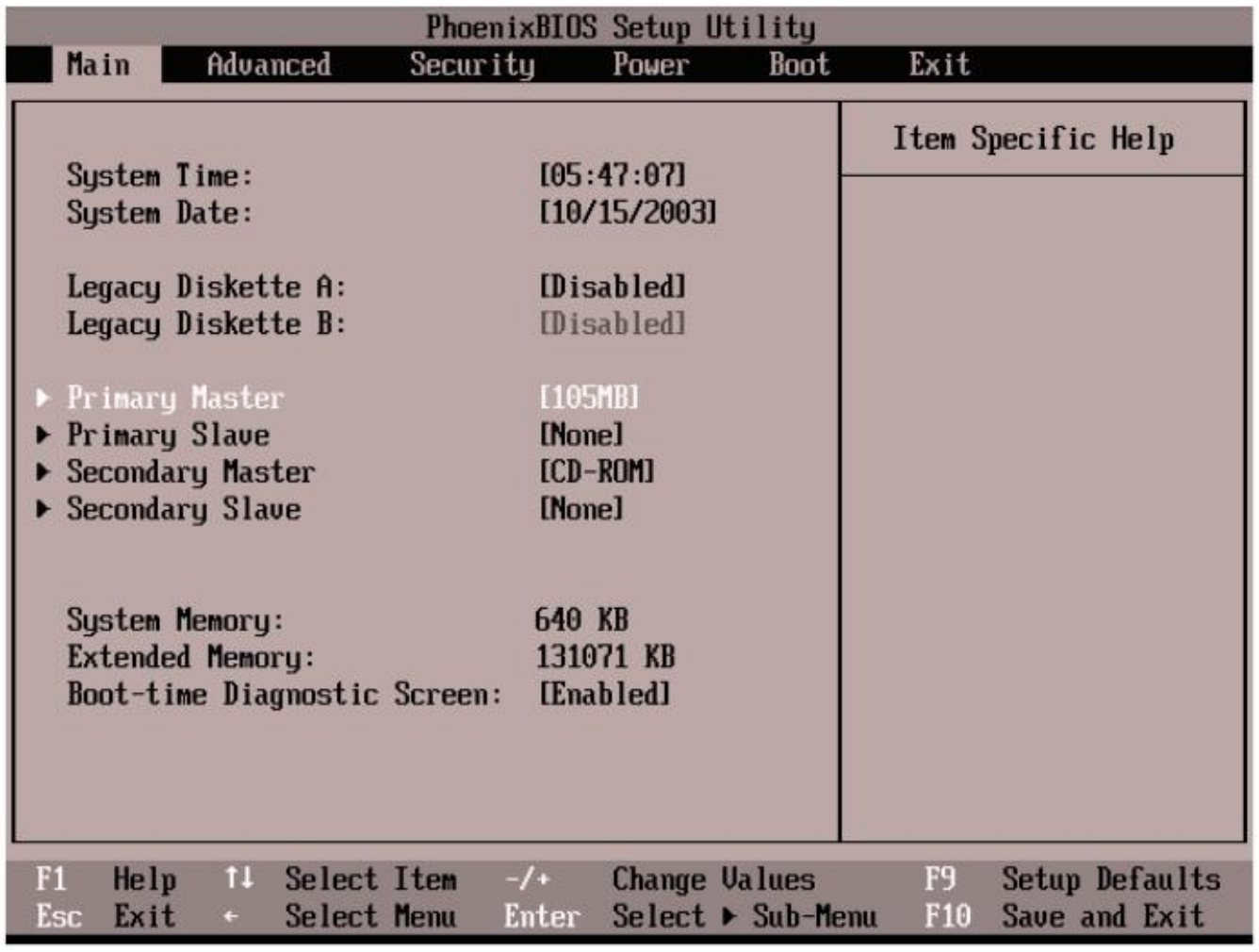
Si une image s'affiche à la place du message que l'on espère voir, il se peut que le microprogramme soit configuré pour afficher un logo plutôt que ces messages. Essayer d'appuyer sur Échap ou sur Tab (⇆ ou →) pour voir les messages.

Si l'ordinateur démarre trop rapidement pour qu'on ait le temps de lire les messages qu'il affiche, il est parfois possible d'appuyer sur la touche Pause (souvent en haut à droite du clavier) pour geler l'écran. Réappuyer sur n'importe quelle touche peut « dégeler » l'écran.

14.3.2 Utilisation de l'interface de configuration du microprogramme

Une fois dans le microprogramme, l'écran est souvent bleu ou noir, plein de menus et parfois la souris ne marche pas. En général, une zone en bas ou à droite de l'écran explique comment naviguer entre les options, comment changer d'onglet, *etc.* Elle est souvent en anglais : aide se dit « *help* », touche se dit « *key* », sélectionner se dit « *select* », valeur se dit « *value* » et modifier se dit « *modify* ». Les touches à utiliser pour se déplacer sont généralement décrites aussi, par exemple `←↑↓→: Move` (en anglais, déplacer se dit « *move* »). Il s'agit des flèches du clavier ↓ et ↑ et/ou ← et →. Parfois, la touche Tab (⇆ ou →) est utile aussi.

4. Tim Fisher, 2019, *BIOS Setup Utility Access Keys for Popular Computer Systems* [https://web.archive.org/web/20200227083303/https://www.lifewire.com/bios-setup-utility-access-keys-for-popular-computer-systems-2624463] (archive) (en anglais), ainsi que Michael Stevens Tech, 2014, *How to access/enter Motherboard BIOS* [https://web.archive.org/web/20201128221653/http://michaelstevenstech.com/bios_manufacturer.htm] (archive) (en anglais).



Un écran de BIOS

14.3.3 Modifier la séquence de démarrage

L'idée, c'est de fouiller dedans jusqu'à trouver quelque chose qui contient le mot `boot`, et qui ressemble par exemple à :

- `First Boot Device`
- `Boot Order`
- `Boot Management`
- `Boot Sequence`

S'il n'y a pas, tenter quelque chose comme `Advanced BIOS Features` ou `Advanced features`.

Une fois la bonne entrée repérée, il s'agit de trouver comment on la modifie. Par exemple `Enter: Select` ou `+/-: Value`. L'objectif est alors de mettre le CD/DVD ou la clé USB en premier, selon sur lequel on veut démarrer.

Parfois, il faut entrer dans un sous-menu. Par exemple s'il y a un menu `Boot order` et qu'il est écrit dans l'aide `Enter: Select`, appuyer sur *Entrée* (↵ ou return) une fois le menu sélectionné.

D'autres fois, les options se changent directement. Par exemple, s'il y a une option comme `First boot device` et qu'il est écrit dans l'aide `+/-: Value`, appuyer sur la touche + ou la touche − jusqu'à ce que la bonne valeur, par exemple `IDE DVDROM`, soit sélectionnée. Parfois, ce sont plutôt les touches *Page suivante* (Page Down, PgDn ou ↕) et *Page précédente* (Page Up, PgUp ou ↕) qui sont utilisées. Parfois encore, ce sont des touches comme F5 et F6. Et d'autres fois, ces touches servent à monter et à descendre le périphérique dans une liste correspondant à l'ordre de démarrage.

14.3.4 Bien choisir sa nouvelle configuration

Une fois qu'on a réussi à sélectionner le bon support pour le démarrage, il faut se demander si on veut le laisser pour toujours ou pas. Si on veut le laisser, il peut être utile de placer le disque interne en deuxième position dans la séquence de démarrage. Ainsi, si le support placé en premier est absent, l'ordinateur démarrera sur ce disque.

Si l'on ne met pas le disque interne dans la séquence de démarrage, l'ordinateur ne démarrera pas dessus, même en l'abscence de CD, de DVD ou de clé USB.

Cependant, le fait de laisser son ordinateur démarrer *a priori* sur un support externe peut avoir des conséquences fâcheuses : il devient un peu plus facile pour une personne malveillante de le faire démarrer en utilisant ce support, par exemple pour effectuer une attaque.

Certes, avec le microprogramme, on peut mettre en place un mot de passe d'accès à l'ordinateur, qui devra être entré avant tout démarrage. Mais il est inutile de compter dessus pour protéger quoi que ce soit : cette protection peut, la plupart du temps, être contournée facilement, par exemple en enlevant la pile de la carte mère pendant quelques minutes.

14.3.5 Enregistrer et quitter

Une fois la nouvelle configuration établie, il reste à enregistrer et à quitter. Encore une fois, lire l'aide à l'écran, comme `F10: Save`. Parfois, il faut appuyer une ou plusieurs fois sur Échap pour avoir le bon menu. Un message s'affiche alors pour demander (en anglais) si on est sûre de vouloir enregistrer et quitter. Par exemple :

```
+--------------------------------------+
|          Setup Confirmation          |
+--------------------------------------+
|                                      |
| Save configuration and exit now      |
|                                      |
|     <Yes>               <No>         |
|                                      |
+--------------------------------------+
```

On veut effectivement enregistrer, donc on sélectionne `Yes` et on appuie sur *Entrée* (↵ ou return).

Chapitre 15

Utiliser un système *live*

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Trente minutes à une heure, plus environ trente minutes de téléchargement.

Un système *live* est un système GNU/Linux qui fonctionne sans être installé sur le disque dur interne de l'ordinateur.

Attention, cela ne signifie pas qu'il n'y aura pas de traces sur le disque interne : par exemple, nombre de systèmes *live* utilisent la mémoire virtuelle (*swap*) s'ils en détectent un. De plus, certains systèmes *live* permettent d'accéder automatiquement au contenu du disque interne, ce qui est aussi susceptible de laisser des traces.

page 25

15.1 Des systèmes *live* discrets

Par contre, certains systèmes *live* sont spécialement conçus pour (tenter de) ne laisser aucune trace sur le disque dur de l'ordinateur sur lequel ils sont utilisés, à moins qu'on ne leur demande expressément de le faire. C'est par exemple le cas de Tails (*The Amnesic Incognito Live System* — le système *live* amnésique incognito).

Il n'y a alors (si les personnes à l'origine du système *live* ne se sont pas trompées) rien d'écrit sur le disque interne. Tout ce qui sera fait à partir du système *live* sera uniquement écrit en mémoire vive, qui s'efface plus ou moins pour de vrai quand on éteint l'ordinateur, du moins après un certain temps.

page 18

Utiliser de tels systèmes *live* est donc l'une des meilleures façons d'utiliser un ordinateur sans laisser de traces. Nous verrons ici comment obtenir un système *live*, et comment démarrer dessus.

Le moyen usuel d'utiliser un système *live* est de l'installer sur une clé USB ou de le graver sur un DVD.

Il est en général conseillé d'utiliser Tails sur une clé USB : cela permet d'utiliser certaines fonctionnalités qui ne sont pas disponibles en DVD comme les mises à jour automatiques et l'espace persistant.

Néanmoins, étant donné qu'il est possible d'écrire des données sur une clé USB alors que ça ne l'est pas sur un DVD, cela rend possible pour des personnes malveillantes de modifier notre système *live* pour, par exemple, enregistrer nos mots de passe ou nos frappes sur le clavier. Si l'on choisit pour ces raisons d'utiliser un DVD, il ne faudra pas négliger de faire les mises à jour manuellement, sous peine d'utiliser un système contenant des failles connues !

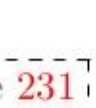
page 32

15.2 Télécharger, vérifier et installer Tails

On va expliquer ici comment télécharger la dernière version de Tails à partir de son site web officiel, puis comment en vérifier l'authenticité avant de l'installer sur une clé USB ou de la graver sur un DVD. On se base essentiellement sur l'assistant officiel disponible sur la page web https://tails.boum.org/install/index.fr.html, qui propose plusieurs documentations différentes suivant le système d'exploitation que l'on utilise.

page ci-contre

Si l'on dispose déjà d'une installation de la dernière version de Tails, il est possible de la dupliquer simplement. Suivre pour cela l'outil cloner Tails.



Attention : ce guide fournit des explications complémentaires sur la vérification de l'authenticité de l'image de Tails. Lorsqu'on arrive à la section « Vérifier votre téléchargement » de la documentation officielle de Tails, se rapporter à la partie vérifier l'authenticité du système live de ce chapitre.

cette page

15.2.1 Télécharger Tails

Tails peut être téléchargé de deux manières : soit directement *via* un navigateur web (en HTTPS), soit à l'aide de BitTorrent.

cette page

Quelle que soit la méthode utilisée, on a besoin d'une image disque[1] du système Tails et de la signature OpenPGP correspondante, qui permet de vérifier son authenticité.

Avec un navigateur web, les deux devront être téléchargées séparément alors que BitTorrent les récupérera en même temps.

Dans tous les cas, il faudra suivre l'assistant d'installation de Tails [https://tails.boum.org/install/index.fr.html] correspondant au système d'exploitation que l'on utilise.

15.2.2 Vérifier l'authenticité du système *live*

L'assistant officiel d'installation de Tails (si on n'utilise pas la méthode en ligne de commande) propose un outil automatique pour vérifier l'intégrité du fichier téléchargé. Il indique de cliquer sur un bouton *Sélectionner votre téléchargement…* et effectue ensuite une première vérification de l'image téléchargée. Il garantit notamment[2] que l'image correspond exactement à celle distribuée par le site de Tails. Cependant il **ne protège pas** contre une attaque sur le site de Tails.

page 231

page 343

page 252

L'image du système *live* que l'on vient de télécharger est signée numériquement avec OpenPGP. On va utiliser cette signature pour en vérifier l'authenticité de façon plus robuste. Si on n'a pas déjà téléchargé cette signature, on peut l'obtenir en cliquant sur le lien *signature OpenPGP* dans la section *Vérifier votre téléchargement*, puis à nouveau sur *signature OpenPGP* dans l'encadré qui apparaît.

Il faut ensuite télécharger la clé OpenPGP de signature de Tails. Pour cela, toujours dans la section *Vérifier votre téléchargement*, cliquer tout d'abord sur *signature OpenPGP* afin de faire apparaître l'encadré correspondant (s'il n'est pas déjà visible), puis cliquer sur *Clé de signature OpenPGP*. Cette clé est associée à l'adresse tails@boum.org.

page 344

Une fois téléchargée, on importe cette clé publique OpenPGP dans le trousseau du bureau. On peut alors afficher l'empreinte de cette clé en double-cliquant dessus dans *Kleopatra*. L'empreinte observée par les personnes qui ont écrit ce guide est la suivante (en admettant que c'est un exemplaire original que l'on a entre les mains) :

---

1. L'image disque est un *fichier d'archive* qui contient une copie à l'identique d'un système de stockage (CD, DVD, disque dur, clé USB, *etc.*). Elle est souvent utilisée pour transférer et dupliquer les fichiers d'installation d'un système. Une image disque peut avoir différents formats comme .img ou .iso (on parle alors d'image ISO).

2. Le modèle de menace auquel répond ce système de vérification de téléchargement de Tails est documenté sur le site de Tails [https://tails.boum.org/contribute/design/download_verification/] (en anglais).

```
A490 D0F4 D311 A415 3E2B B7CA DBB8 02B2 58AC D84F
```

Si l'empreinte observée est la même que celle-ci, on peut alors vérifier la signature numérique de l'image. *Kleopatra* peut afficher *Impossible de vérifier la donnée Signature créée le [...] Avec le certificat : Tails developers (offline long-term identity key) <tails@boum.org> (DBB8 02B2 58AC D84F).* Cela signifie que le fichier est bien signé par la clé en question, mais qu'on n'a pas confirmé l'authenticité de cette clé… ce n'est pas bien grave car on vient de vérifier son empreinte.

page 345

Si la signature est valide, il y a une très grande probabilité que le téléchargement de Tails qui vient d'être fait soit bon. Premièrement, son intégrité a été vérifiée, l'image est donc exactement la même que celle proposée par le site. De plus, elle est signée avec une clé dont l'empreinte est vérifiable dans ce guide, donc ailleurs que sur le site de Tails. La probabilité que le site et le guide aient été corrompus de la même manière étant très très faible, on peut continuer l'installation.

15.2.3 Installer Tails sur le support choisi

Retourner à l'assistant d'installation de Tails [https://tails.boum.org/install/index.fr.html] pour y trouver les instructions d'installation de Tails sur une clé USB qui correspondent à notre système d'exploitation.

Si en revanche on préfère installer Tails sur un DVD, il faudra se rendre sur la page dédiée [https://tails.boum.org/install/dvd/index.fr.html].

15.3 Cloner ou mettre à jour une clé Tails

Une fois que l'on dispose d'un DVD ou d'une clé USB avec Tails, il est possible de la dupliquer, par exemple pour créer une clé USB avec une persistance correspondant à une nouvelle identité contextuelle, pour donner une clé Tails à une connaissance, ou encore pour mettre à jour une clé USB contenant une ancienne version de Tails.

page préc.

Pour ce faire, on suit la documentation officielle de Tails, qui est disponible à partir de n'importe quel DVD ou clé Tails, même sans connexion à Internet.

Commencer par démarrer Tails. Puis, sur le bureau, double-cliquer sur l'icône *Documentation de Tails*. Chercher la section *Téléchargement, installation et mise à jour*, puis l'item *Installing by cloning from another Tails* (ou, en français, *Installer en clonant depuis un autre Tails*). Cliquer sur *For PC* (*Pour PC*), ou sur *For Mac* (*Pour Mac*) selon notre ordinateur. Suivre les étapes indiquées.

cette page

Pour mettre à jour la clé ainsi créée, il faudra par la suite suivre la page *Upgrading automatically* (*Mettre à jour automatiquement*), située sous l'item *Upgrading a Tails USB stick* (*Mettre à jour une clé USB Tails*).

15.4 Démarrer sur un système *live*

Dès que la copie ou la gravure est terminée, on peut redémarrer l'ordinateur en laissant le support du système *live* dedans, et vérifier que la copie a fonctionné. À condition bien sûr qu'on ait configuré le microprogramme de notre ordinateur pour qu'il démarre sur le bon support : voir la recette expliquant comment démarrer sur un média externe pour les détails.

page 107

Au démarrage, Tails affiche un écran qui permet de choisir, entre autres options, la langue d'affichage et la disposition du clavier.

15.5 Utiliser la persistance de Tails

cette page

Lorsqu'on utilise Tails à partir d'une clé USB, il est possible de créer un volume persistant chiffré sur l'espace libre de la clé.

Les données contenues dans ce volume persistant sont sauvegardées et restent disponibles d'une session d'utilisation de Tails à l'autre. Le volume persistant permet de sauvegarder des fichiers personnels, des clés de chiffrement, des configurations ou des logiciels qui ne sont pas installés par défaut dans Tails.

cette page

Une fois le volume persistant créé, on peut choisir de l'activer, ou non, à chaque démarrage de Tails.

cette page

On peut enfin le supprimer lorsqu'on n'a plus besoin d'accéder aux données qu'il contient.

L'utilisation d'un volume persistant n'est toutefois pas sans conséquences quant aux traces laissées. C'est pourquoi il faudra commencer par lire la page d'avertissement concernant l'usage de la persistance.

Pour cela, double-cliquer sur l'icône *Documentation de Tails* se trouvant sur le bureau. Chercher la section *Premiers pas avec Tails* et cliquer sur *Avertissements à propos du stockage persistant*, situé juste en dessous de l'item *Stockage persistant*.

15.5.1 Créer et configurer un volume persistant

L'objectif de cette recette est de créer et de configurer un volume persistant sur une clé Tails.

Pour ce faire, on va suivre la documentation officielle de Tails, qui est disponible à partir de n'importe quelle clé USB ou DVD Tails, même sans connexion à Internet.

page préc.

Commencer par démarrer Tails. Puis, sur le bureau, double-cliquer sur l'icône *Documentation de Tails*. Chercher la section *Premier pas avec Tails* et cliquer sur *Stockage persistant*. Sur cette page de documentation, suivre les sections *Créer un stockage persistant* et *Configurer le stockage persistant*.

Si l'on a déjà un volume persistant et que l'on souhaite simplement modifier ses paramètres, comme la phrase de passe par exemple, aller directement à la section *Sujets avancés* en bas de la page de sommaire de la documentation.

15.5.2 Activer et utiliser un volume persistant

L'objectif de cette recette est d'activer le volume persistant nouvellement créé sur notre clé Tails.

Pour ce faire, on va suivre la documentation officielle de Tails, qui est disponible à partir de n'importe quelle clé USB ou DVD Tails, même sans connexion à Internet.

page préc.

Commencer par démarrer Tails. Puis, sur le bureau, double-cliquer sur l'icône *Documentation de Tails*. Chercher la section *Premier pas avec Tails* et cliquer sur *Stockage persistant*. Sur cette page de documentation, suivre la section *Utiliser le stockage persistant*.

15.5.3 Supprimer un volume persistant

L'objectif de cette recette est de supprimer le volume persistant créé précédemment sur notre clé Tails.

Pour ce faire, on va suivre la documentation officielle de Tails, qui est disponible à partir de n'importe quelle clé USB ou DVD Tails, même sans connexion à Internet.

page préc.

Commencer par démarrer Tails. Sur le bureau, double-cliquer sur l'icône *Documentation de Tails*. Chercher la section *Premier pas avec Tails*, cliquer sur *Supprimer le stockage persistant* situé sous l'item *Stockage persistant*, puis suivre cette page de documentation.

15.5.4 Installer un logiciel additionnel persistant dans Tails

Tails contient des logiciels adaptés à la plupart des tâches courantes lors de l'utilisation d'Internet et de la création de documents. Toutefois, pour des projets spécifiques, on peut avoir besoin d'installer un logiciel spécifique dans Tails, comme par exemple un logiciel de conception et de simulation de circuits électroniques.

Lorsque Tails est installé sur une clé USB, il est possible de configurer un volume persistant pour qu'un ou plusieurs logiciels spécifiques soient installés de manière automatique à chaque démarrage.

Trouver le nom du paquet à installer On a besoin du nom exact du paquet à installer. Pour le trouver, suivre la recette trouver un paquet. Par exemple, notre logiciel de conception de circuits électroniques est fourni par le paquet `geda`.

page 135

Installer le logiciel additionnel Pour installer le paquet ainsi identifié, on va suivre la documentation officielle de Tails, qui est disponible à partir de n'importe quelle clé USB ou DVD Tails, même sans connexion à Internet.

Commencer par démarrer Tails. Sur le bureau, double-cliquer sur l'icône *Documentation de Tails*. Chercher la section *Premier pas avec Tails*, cliquer sur *Installer des logiciels supplémentaires* puis suivre cette page de documentation.

page 115

Chapitre 16

Installer un système chiffré

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Compter une journée, avec plusieurs périodes d'attente (parfois longues).

On a vu que tout ordinateur — hormis avec certains systèmes *live* — laisse des traces un peu partout, des fichiers ouverts, des travaux effectués, des connexions Internet, *etc.* On a vu aussi qu'une façon d'exposer un peu moins les données conservées sur l'ordinateur ainsi que les traces qu'on y laisse est de chiffrer le système sur lequel on travaille dans son ensemble.

page 27
page 47

Il est possible d'installer un système d'exploitation GNU/Linux comme Debian ou Ubuntu, sur une partie chiffrée du disque dur. À chaque démarrage, l'ordinateur va demander une phrase de passe, après quoi il débloque le chiffrement du disque, ce qui donne accès aux données, et permet donc le démarrage du système. Sans cette phrase, toute personne qui voudrait consulter le contenu de ce disque se trouvera face à des données indéchiffrables. C'est ce qu'on se propose de faire dans cette recette.

page 22

Installer un nouveau système d'exploitation peut supprimer toutes les données présentes sur le disque dur. On commencera donc par sauvegarder les données que l'on veut conserver. Puis, si on considère que le disque dur contenait des données sensibles, on pourra les effacer « pour de vrai » pour rendre leur recupération la plus difficile possible.

page 151
page 139

16.1 Limites

Attention : cette simple installation chiffrée ne règle pas tous les problèmes de confidentialité d'un coup de baguette magique. Elle ne protège les données qu'à certaines conditions.

16.1.1 Limites d'un système chiffré

Nous recommandons chaudement les lectures préalables suivantes :

- le chapitre concernant le chiffrement (et ses limites),
- le cas d'usage un nouveau départ, qui étudie, en détails, les limites pratiques d'un tel système et les attaques possibles contre lui.

page 47
page 71

Sans cela, l'installation d'un système chiffré peut procurer un sentiment erroné de sécurité, source de bien des problèmes.

16.1.2 Limites d'une nouvelle installation

Lors de l'installation d'un nouveau système, on part de zéro. Il n'y a aucun moyen simple de vérifier que le support d'installation qu'on utilise est fiable, et ne contient pas par exemple de logiciels malveillants. On ne pourra éventuellement s'en rendre compte que *par la suite* — et peut-être qu'il sera trop tard…

16.1.3 Limites dans la prise en charge du matériel

Utiliser un système d'exploitation libre comme Debian a un désavantage : les fabricants de matériel y font généralement peu attention. Il arrive donc qu'il ne soit pas facile, voire complètement impossible, d'utiliser un ordinateur ou l'un de ses périphériques avec Debian.

page 20

La situation s'améliore depuis quelques années : le fonctionnement du matériel tend à s'homogénéiser, et surtout, la diffusion des systèmes libres pousse de plus en plus les fabricants à aider, directement ou non, à ce que leur matériel fonctionne[1].

Cependant, avant de remplacer un système d'exploitation, cela peut être une bonne idée de s'assurer que le matériel nécessaire fonctionne bien à l'aide d'un système *live*. Le système Tails, par exemple, est basé sur Debian. Le matériel qui fonctionne avec l'un devrait donc fonctionner avec l'autre sans trop difficultés. Il faut toutefois garder en tête que Tails inclut les microprogrammes non-libres, alors qu'il faut les installer explicitement pour les avoir dans Debian.

page 113

cette page

16.2 Télécharger un support d'installation

Pour réaliser l'installation du système, le plus simple est d'utiliser une clé USB, un CD ou un DVD. Debian en propose plusieurs variantes, et il est donc nécessaire de commencer par choisir la méthode qui convient le mieux à notre situation.

16.2.1 Avec ou sans microprogrammes non-libres ?

Pour fonctionner, certains périphériques de l'ordinateur nécessitent que le système leur fournisse un « microprogramme » (ou *firmware*). Mais il n'en existe pas toujours de version libre...

page 20

Un micro-quoi ?

Ces microprogrammes sont des programmes qui ont la particularité de s'exécuter sur des puces électroniques à l'intérieur du périphérique et non sur le processeur de l'ordinateur. C'est par exemple le cas du programme qui contrôlera le déplacement des parties mécaniques d'un disque dur ou le fonctionnement du système de radio d'une carte Wi-Fi. On ne se rend pas forcément compte qu'ils existent car la plupart des matériels sont livrés avec le microprogramme déjà installé.

page 16

Mais pour d'autres périphériques, le système d'exploitation doit envoyer le microprogramme à un composant lors de son initialisation.

Ceux qui sont libres sont livrés avec le programme d'installation de Debian. Comme la plupart des microprogrammes ne sont pas libres, nous devons mettre nous-mêmes à disposition du programme d'installation tout microprogramme non-libre nécessaire au fonctionnement de l'ordinateur : c'est typiquement le cas pour certaines cartes Wi-Fi.

page 39

Encore une histoire de compromis

Si l'on installe notre système chiffré sur un ordinateur portable, il est très probable que des microprogrammes supplémentaires soient nécessaires pour faire marcher le Wi-Fi, voire pour avoir un affichage de bonne qualité.

---

1. Pour certains matériels, des problèmes peuvent venir de défauts dans le fonctionnement des microprogrammes intégrés. Ces problèmes sont parfois corrigés par des mises à jour que fournissent les fabricants. Cela peut donc être une bonne idée de faire les mises à jour du microprogramme (BIOS ou UEFI), de l'*Embedded Controller* ou d'autres composants avant de procéder à l'installation. Malheureusement, ces procédures diffèrent trop d'un matériel à un autre pour être détaillées dans cet ouvrage, mais peuvent en général être trouvées sur le site du constructeur...

Sur un ordinateur fixe sans Wi-Fi, il est assez plausible que notre système chiffré fonctionne correctement sans nécessairement de microprogramme non-libre.

Même s'il n'y pas à notre connaissance d'élément qui prouve son utilisation, on peut envisager que le microprogramme propriétaire d'une carte Wi-Fi nous espionne à notre insu… sauf que sans microprogramme, elle ne fonctionnera tout simplement pas. C'est encore une fois une histoire de compromis.

16.2.2 L'image d'installation par le réseau

Le plus rapide est d'utiliser une image d'installation par le réseau. Elle contient uniquement les tout premiers morceaux du système. L'installeur télécharge ensuite, depuis Internet, les logiciels à installer. Il faut donc que l'ordinateur sur lequel on souhaite installer Debian soit connecté à Internet, de préférence par un câble réseau (et non par le *Wi-Fi* qui ne fonctionnera que rarement à l'intérieur du logiciel d'installation).

Il existe plusieurs fichiers (également appelés « images ») contenant une copie de l'image d'installation, selon l'architecture du processeur. Dans la plupart des cas, il faudra télécharger celui dont le nom se termine par `amd64-i386-netinst.iso`, dit multi-architecture, qui conviendra pour les architectures 32 et 64 bits et qui fonctionnera sur la plupart des ordinateurs domestiques fabriqués après 2006 [2].

page 16

Il faut choisir entre :

- la version entièrement libre [3]
- la version contenant les microprogrammes non-libres [4].

16.2.3 L'image avec l'environnement graphique

S'il n'est pas possible de connecter à Internet l'ordinateur sur lequel on souhaite installer Debian, il est possible de télécharger un image contenant tout le système de base ainsi que l'environnement graphique habituel. Cela nécessite d'avoir accès à un graveur de DVD ou à une clé USB d'au moins 4 Go.

De la même manière que pour l'image d'installation par le réseau, il faut choisir entre [5] :

- la version entièrement libre [6]
- la version contenant les microprogrammes non-libres [7].

Seul le premier DVD est nécessaire pour réaliser l'installation. Le nom du fichier à télécharger se termine par `-amd64-DVD-1.iso` (64 bits).

16.3 Vérifier l'empreinte de l'image d'installation

Il est bon de s'assurer que le téléchargement de l'image s'est bien déroulé en vérifiant l'empreinte de l'installeur, pour s'assurer de son intégrité et de son authenticité. Nous allons procéder en deux étapes, une première nous assurant de son intégrité, et une seconde assurant son authenticité.

page 47

Pour cela, il est nécessaire de démarrer sur un système déjà installé. Si l'on a accès à un ordinateur sous GNU/Linux, par exemple celui d'une amie, tout va bien. Si on ne dispose que d'un système *live*, il est par exemple possible de mettre l'image

page 113

2. Des ordinateurs portables utilisant l'architecture de processeur [page 16] ARM apparaissent, mais les autrices de ce guide n'en ont encore jamais testé.

3. https://cdimage.debian.org/cdimage/release/current/multi-arch/iso-cd/

4. https://cdimage.debian.org/cdimage/unofficial/non-free/cd-including-firmware/current/multi-arch/iso-cd/

5. Ces DVD fonctionnent avec les ordinateurs dont le processeur utilise l'architecture `x86-64`, c'est-à-dire la grande majorité des ordinateurs fabriqués après 2012.

6. https://cdimage.debian.org/debian-cd/current/amd64/iso-dvd/

7. https://cdimage.debian.org/images/unofficial/non-free/images-including-firmware/current/amd64/iso-dvd

téléchargée sur une clé USB, puis de vérifier l'empreinte à partir du système *live*.

Pour vérifier l'intégrité et l'authenticité de l'image ISO, deux petits fichiers sont nécessaires :

- la somme de contrôle `SHA512SUMS` ;
- la signature de cette somme de contrôle `SHA512SUMS.sign`.

Les télécharger depuis la page sur laquelle on a trouvé l'image ISO ci-dessus grâce à un clic droit puis en sélectionnant *Enregistrer la cible du lien sous…*.

16.3.1 Vérifier l'intégrité de l'image d'installation

page 161

Pour cela suivre l'outil concernant les sommes de contrôle. Il sera nécessaire de calculer la somme de contrôle SHA512 de l'image d'installation (l'image ISO), puis de vérifier qu'elle correspond bien à celle contenue dans le fichier `SHA512SUMS`.

16.3.2 Vérifier l'authenticité de l'image d'installation

Si la vérification de l'intégrité s'est bien déroulée, à savoir si les deux sommes de contrôles calculées correspondent, on peut poursuivre le processus afin de vérifier son authenticité. En effet, des adversaires pourraient fournir un support d'installation corrompu et sa somme de contrôle. La vérification précédente nous permettrait simplement de constater que le fichier téléchargé est bien celui qui était disponible sur le site web, pas qu'il est celui qu'on espère avoir.

Le deuxième tome explique comment s'assurer de l'authenticité de l'installeur téléchargé, car l'empreinte est signée avec GnuPG, qui utilise la cryptographie asymétrique. Il faudra suivre les outils suivants :

- Télécharger la clé publique utilisée pour signer le support d'installation depuis https://keyserver.ubuntu.com/pks/lookup?op=get&search=0xdf9b9c49eaa9298432589d76da87e80d6294be9b et l'enregistrer avec ☰ puis *Enregistrer sous…*. Choisir `debian.asc` comme nom de fichier et *Enregistrer*.

page 343

- Importer cette clé dans le trousseau du bureau. Vérifier son empreinte :

page 135

  – si on a accès à une installation de Debian de confiance, on peut installer le paquet `debian-keyring`, puis utiliser un terminal et taper la commande suivante :

page 97

```
gpg --keyring /usr/share/keyrings/debian-role-keys.gpg
↪     --no-default-keyring --fingerprint
↪     debian-cd@lists.debian.org
```

  – si on a confiance dans le livre qu'on a dans les mains, il prétend que l'empreinte est : `DF9B 9C49 EAA9 2984 3258  9D76 DA87 E80D 6294 BE9B`.

page 345

- Vérifier la signature du fichier `SHA512SUMS`, contenue dans le fichier `SHA512SUMS.sign` préalablement téléchargé. La notification doit afficher *Signature valide mais **non fiable** de Debian CD signing key <debian-cd@lists.debian.org> sur […].*

16.4 Préparer le support d'installation

Une fois l'image du support d'installation choisie, téléchargée et vérifiée, il nous reste à l'installer sur une clé USB, un CD ou un DVD.

16.4.1 Créer une clé USB d'installation

Si l'on dispose d'une clé USB vide, ou contenant uniquement des données auxquelles on ne tient pas et qu'on a accès à un système basé sur GNU/Linux tel que Debian[8] ou Tails, c'est l'option la plus rapide.

page 113

8. Parfois, il peut arriver que l'ordinateur ne parvienne pas à démarrer sur la clé USB produite en suivant les instructions décrites ici. Cependant, de ce qu'il a été possible d'expérimenter lors

⚠ **Attention** : les données éventuellement présentes sur la clé seront perdues. Par contre, si cette clé n'était pas initialement chiffrée, il serait possible de procéder à une analyse pour retrouver les fichiers dont le contenu n'aurait pas été écrasé auparavant… page 42

Ouvrir Disques à partir de la vue d'ensemble des Activités : appuyer sur la touche ⊞ (⌘ sur un Mac), puis taper `disque` et cliquer sur *Disques*.

Une fois Disques ouvert, on peut brancher notre clé USB. Une entrée correspondant à cette dernière devrait apparaître dans la liste située à gauche. Cliquer dessus pour la sélectionner.

Cliquer ensuite sur le menu ⋮ en haut à droite (ou ☰) et sélectionner *Restaurer l'image disque…*. Dans *Image à restaurer*, sélectionner l'image ISO précédemment téléchargée. Cliquer sur *Démarrer la restauration…*.

Une fenêtre nous demande *Voulez-vous vraiment écrire l'image disque sur le périphérique ?*. Vérifier que la taille et le modèle du périphérique concerné correspondent bien à la taille et au modèle de notre clé USB. Si c'est le cas, cliquer sur *Restaurer*.

Le mot de passe d'administration nous est alors demandé, le taper et *S'authentifier* pour lancer l'écriture de la clé d'installation. Une fois la restauration terminée, cliquer sur ⏏ pour éjecter la clé.

16.4.2 Graver l'image d'installation sur un CD ou un DVD

Si l'on a pas de clé USB ou pas d'accès à un système GNU/Linux, on peut graver l'image d'installation sur un CD ou un DVD.

Le fichier téléchargé est une « image ISO », c'est-à-dire un format de fichiers que la plupart des logiciels de gravure reconnaissent comme « image CD brute ». En général, si on insère un disque vierge dans son lecteur, le logiciel de gravure s'occupe tout seul de transformer cette image en l'écrivant sur le disque vierge — en tout cas, ça marche avec Tails, et plus généralement sous Debian ou Ubuntu.

Sous Windows, si on a pas déjà installé de logiciel capable de graver des images ISO, le logiciel libre InfraRecorder[9] (en anglais) fera parfaitement l'affaire.

16.5 L'installation proprement dite

Pour installer la Debian chiffrée depuis le support d'installation (CD, DVD ou clé USB), il faut démarrer sur celui-ci en suivant la recette correspondante. page 107

À partir de là, l'installation proprement dite peut commencer : prévoir du temps devant soi et quelques mots croisés, car l'ordinateur pourra travailler longtemps sans surveillance particulière.

Vérifier, dans le cas d'une image d'installation par le réseau, que le câble reliant l'ordinateur au réseau est bien branché. Et si il s'agit d'un ordinateur portable, vérifier que le câble d'alimentation est branché, car il n'y a pas de notification de batterie faible durant l'installation.

Le programme d'installation de Debian dispose de sa propre documentation[10]. En cas de doute à la lecture des étapes décrites par la suite, cela peut valoir le coup d'y jeter un œil. Par ailleurs, pour la plupart des choix qu'il nous demande de faire, le programme d'installation nous proposera automatiquement une réponse qui fonctionne généralement…

---

de la rédaction de ce guide, les clés créées de cette manière à partir de Tails semblent fonctionner correctement.

9. http://infrarecorder.org/

10. Le manuel d'installation est disponible dans de nombreuses versions [https://www.debian.org/releases/stable/installmanual.fr.html]. On suivra celui correspondant à l'architecture du processeur [page 16].

16.5.1 Lancement de l'installeur

On démarre donc sur le support d'installation (CD, DVD ou clé USB). Un premier menu nommé *Debian GNU/Linux installer menu* apparaît. Appuyer sur la touche *Entrée* (↵ ou return) pour lancer la suite du programme d'installation.

Dans le cas où on a choisi un CD multi-architecture, l'option sélectionnée automatiquement par l'installeur sera en principe *Graphical install* et une option *32-bit install options* sera disponible ; dans ce cas, le programme d'installation a détecté que le processeur est compatible avec l'architecture `amd64`, qui apporte quelques avantages en termes de sécurité.

page 16

16.5.2 Choisir la langue et la disposition du clavier

- Après un peu de patience, un menu nommé *Select a language* apparaît : l'installeur propose de choisir une langue pour la suite de l'installation. Sélectionner *French - Français*. Pour passer à l'étape suivante, il faudra à chaque fois choisir *Continue*.
- Un menu demande le pays, pour peaufiner l'adaptation du système. Choisir son lieu géographique.
- Dans *Configurer le clavier*, le choix par défaut *Français* convient si l'on a un clavier français « azerty ».
- L'installeur charge ensuite les fichiers dont il a besoin.

16.5.3 Microprogramme et matériel réseau

Après un temps de chargement, le programme d'installation de Debian va détecter les cartes réseau présentes dans l'ordinateur.

Comme vu précédemment, certains matériels ont besoin que le système leur fournisse un microprogramme pour fonctionner.

page 120

Si le support d'installation a été préparé précédemment avec des microprogrammes nécessaires au système, on verra directement apparaître un écran nous demandant d'accepter un `SOFTWARE LICENSE AGREEMENT` ou quelque chose de similaire. Après l'avoir lu, on peut répondre *Oui* pour poursuivre l'installation.

Si le support d'installation contient uniquement des programmes libres, on pourra voir apparaître un message indiquant une liste de *fichiers de microcode manquants* : il s'agit des microprogrammes non-libres utiles pour notre ordinateur mais qui ne sont pas fournis par le support d'installation. L'installeur propose d'insérer un support amovible les contenant. Choisir *Non* permet de passer à la suite de l'installation sans installer ces microprogrammes non-libres[11]. Au contraire, choisir *Oui* demande au programme d'installation de rechercher les fichiers de microcode ou les paquets contenant ces microcodes sur les périphériques disponibles — et donc de revenir sur le choix effectué précédemment de faire une installation entièrement libre.

page 120

11. Il est possible d'installer les microcodes manquants plus tard après avoir activé les dépôts `non-free` [page 136].



Pour aller plus loin…

On peut préparer un tel périphérique en copiant les microprogrammes les plus courants regroupés par la communauté Debian sous forme d'une archive [https://cdimage.debian.org/cdimage/unofficial/non-free/firmware/bullseye/current] à décompresser dans un répertoire `firmware` situé à la racine d'une clé USB formatée en FAT.

Cette archive de *firmwares* est disponible en trois versions, correspondant à trois types de compression différents (`.cpio.gz`, `.tar.gz` ou `.zip`). Selon le ou les formats que notre système est capable de décompresser, on choisira le fichier correspondant. Si l'on ne sait pas répondre à cette question, on pourra télécharger les trois fichiers jusqu'à en trouver un que l'on peut décompresser. Comme pour l'image ISO, il est conseillé de vérifier l'intégrité (voir page 122) et l'authenticité (voir page 122) de chaque fichier téléchargé.

Si le message apparaît de nouveau, c'est que la clé ne contient pas le nécessaire [12]. Il est hors de portée de ce guide d'indiquer comment obtenir tous les microprogrammes qui peuvent s'avérer utiles. Enfin, il ne faut pas hésiter à répondre *Non*… Dans la plupart des cas, l'installation arrivera à se poursuivre sans autre problème grâce à la connexion filaire, qui permet de se passer des microprogrammes nécessaires au fonctionnement de la carte Wi-Fi.

16.5.4 Configuration du réseau et nom de la machine

- L'installeur prend alors un peu de temps pour configurer le réseau. Si notre ordinateur possède plusieurs cartes réseau, il faut choisir celle dont on va se servir pour l'installation. Le choix par défaut est généralement le bon, si il s'agit d'une carte réseau *Ethernet*.
- On nous demande ensuite le *Nom de machine*. Choisir un petit nom pour son ordinateur, en sachant que ce nom sera ensuite visible depuis le réseau, et pourra aussi s'inscrire dans les fichiers créés ou modifiés avec le système qu'on est en train d'installer. Il peut donc être pertinent de lui donner un nom générique, comme `debian`, par exemple.
- L'installeur demande alors un *Domaine*. Sans entrer dans les détails, mieux vaut laisser ce champ vide (donc effacer ce que le programme peut éventuellement avoir pré-rempli).

16.5.5 Créer les utilisateurs et choisir les mots de passe

Le programme d'installation nous demande maintenant de choisir le *mot de passe du superutilisateur (« root »)*. C'est un mot de passe qui serait nécessaire pour réaliser les tâches d'administration de l'ordinateur : mises à jour, installation de logiciels, modifications majeures du système, *etc.*

Il est toutefois plus simple de s'épargner un mot de passe supplémentaire, et de permettre que le premier compte créé sur le système ait le droit de faire des opérations d'administration [13], en redemandant le mot de passe. Pour cela, il suffit de ne pas entrer de mot de passe pour « root » : laisser simplement la case vide et choisir *Continuer*, puis à nouveau pour la *Confirmation du mot de passe*.

- Dans *Nom complet du nouvel utilisateur*, choisir le nom associé au premier compte créé sur le système. Ce nom sera souvent enregistré dans les documents créés ou modifiés dans cette session ; il peut donc être intéressant de choisir un nouveau pseudonyme.

12. Par exemple, les noms de fichier commençant par `b43` sont des microprogrammes pour un type de carte Wi-Fi, qui ne sont pas redistribués directement par Debian. Pour les faire fonctionner, il faudra tenter d'installer, une fois le système fonctionnel, l'un des paquets `firmware-b43-installer`, `firmware-b43-lpphy-installer` ou `firmware-b43legacy-installer`.

13. Ce mode est appelé *sudo*, car dans le terminal, il sera possible, en ajoutant `sudo` au début de la ligne, d'exécuter une commande en tant que « root », c'est-à-dire en tant que superutilisatrice.

- Dans *Identifiant pour le compte utilisateur*, choisir un identifiant (*login*) pour ce compte. Il est prérempli, mais peut être modifié. L'installeur prévient, pour le cas où l'on voudrait le changer, qu'il doit commencer par une lettre minuscule et être suivi d'un nombre quelconque de chiffres et de lettres minuscules.
- L'installeur demande un mot de passe pour l'utilisatrice. C'est elle qui aura le droit d'administrer l'ordinateur, si l'on a décidé de ne pas entrer un mot de passe « root » précédemment. (Ne pas oublier de trouver un moyen de se souvenir de ce mot de passe.)

16.5.6 Partitionner les disques

page 20

Si l'on a démarré sur le support d'installation en mode UEFI, il se peut que l'installeur pose la question *Forcer l'installation UEFI ?* Cela signifie qu'il a détecté un autre système déjà installé sur le disque dur et qui utilise le « mode de compatibilité BIOS » (l'ancêtre d'UEFI) pour démarrer. Comme l'on va de toute façon effacer les traces de cet ancien système et mettre Debian à la place, on peut répondre *Oui* à cette question.



Pour aller plus loin…

La probabilité d'avoir un souci en UEFI est très faible, mais certaines cartes mères ou certains microprogrammes un peu pénibles peuvent mieux fonctionner en mode compatibilité BIOS.

Si à la fin de l'installation le système ne démarre pas en UEFI, on peut relancer l'installation en répondant *Non* à cette question afin d'installer Debian en mode compatibilité BIOS.

Le support d'installation démarre ensuite l'outil de partitionnement. Il détecte les partitions présentes, et va proposer de les modifier.

- Dans le menu *Méthode de partitionnement*, choisir *Assisté — utiliser tout un disque avec LVM chiffré.*
- Dans *Disque à partitionner*, choisir le disque sur lequel installer Debian GNU/-Linux. Si l'on veut supprimer le système actuellement installé, il correspond en général au premier disque de la liste. La taille du disque est un indice permettant de ne pas se tromper, pour ne pas essayer d'installer Debian sur la clé USB contenant l'installeur par exemple.
- L'installeur propose ensuite de choisir un *Schéma de partitionnement* parmi différentes possibilités. Sélectionner *Tout dans une seule partition.*
- L'installeur prévient alors qu'il va appliquer le schéma actuel de partitionnement, ce qui sera irréversible. Vu que l'on a bien fait les sauvegardes de ce que l'on voulait garder, répondre *Oui* à *Écrire les modifications sur les disques et configurer LVM ?*
- L'installeur va alors remplacer l'ancien contenu du disque par des données aléatoires. C'est très long — plusieurs heures sur un gros disque — et ça laisse donc du temps pour faire autre chose !
- page 103 L'installeur demande alors une *Phrase secrète de chiffrement*. Choisir une bonne phrase de passe et la taper, puis confirmer la phrase de passe en la tapant une seconde fois.
- L'installeur propose alors de choisir la taille à utiliser sur le disque dans *Quantité d'espace sur le groupe de volumes pour le partitionnement assisté*. On pourra garder la valeur choisie par défaut, qui correspond à la taille maximale utilisable du disque.
- L'installeur montre une liste de toutes les partitions qu'il va créer. Il est possible de lui faire confiance en laissant *Terminer le partitionnement et appliquer les changements* séléctionné.

- L'installeur prévient qu'il va écrire des modifications sur le disque. Tout le disque a déjà été rempli de données aléatoires, donc s'il contenait des données importantes elles ont déjà été effacées. Répondre *Oui* à *Faut-il appliquer les changements sur les disques ?* L'installeur crée alors les partitions, ce qui peut prendre un petit bout de temps.

16.5.7 Installation du système de base

L'installeur va maintenant installer un système Debian GNU/Linux minimal. Le laisser faire…

16.5.8 Configurer l'outil de gestion des paquets

Selon la version de l'installeur utilisé, il peut poser différentes questions :

- Si l'installeur demande *Faut-il analyser d'autres supports d'installation* que celui utilisé pour démarrer l'installeur, le choix par défaut, *Non*, convient.
- Si l'installeur demande *Faut-il utiliser un miroir sur le réseau ?*, le choix par défaut, *Non*, convient. Cependant, si on a une bonne connexion Internet, on peut aussi choisir *Oui* : ceci permettera d'installer une version mise à jour.

Si l'on utilise une installation par le réseau (aussi appelée « *netinst* », pour *network install*) ou si l'on a répondu *Oui* à la question précédente, l'installeur demande alors depuis quel serveur il doit télécharger les paquets :

- L'installeur demande tout d'abord de choisir le *Pays du miroir de l'archive Debian*. Choisir le pays dans lequel on se trouve.
- Il demande ensuite le *Miroir de l'archive Debian* à utiliser. Le choix par défaut, *deb.debian.org*, est très bien.
- L'installeur demande si on a besoin d'un *Mandataire HTTP*. On laisse vide.
- L'installeur télécharge alors les fichiers dont il a besoin pour continuer.

16.5.9 Sélection des logiciels

La prochaine question concerne la *Configuration de popularity-contest* et demande *Souhaitez-vous participer à l'étude statistique sur l'utilisation des paquets ?* Répondre *Non*, sauf si l'on accepte de communiquer à Debian la liste des logiciels que l'on installe[14].

L'installeur demande ensuite quels sont les *Logiciels à installer*. Ses propositions conviennent en général : *environnement de bureau Debian*, *GNOME* et *utilitaires usuels du système*.



Pour aller plus loin…

La plupart des outils détaillés dans ce guide se basent sur l'environnement de bureau GNOME. Cependant, GNOME est un peu exigeant en matière de puissance, et d'autres environnements plus légers seront mieux adaptés à des ordinateurs pas très puissants : *LXDE*, *Xfce* ou *MATE*.

14. Communiquer notre liste de logiciels installés à Debian facilite le travail des personnes qui développent et maintiennent cette distribution, en leur donnant une vision de quels logiciels sont les plus utilisés. Cela permet donc aussi de leur signifier que ces logiciels sont importants pour nous et que nous tenons à ce qu'ils continuent d'être maintenus dans Debian. Cependant, la liste des logiciels que l'on utilise constitue tout de même des données personnelles : s'il y a des failles de sécurité sur les serveurs de Debian, ces données pourraient être divulguées. Qui plus est, répondre *Non* à cette question s'inscrit aussi dans la construction d'une culture politique collective de refus de communiquer nos données personnelles et d'opposition à la gouvernance par les nombres.

L'installeur télécharge alors tout le reste du système Debian GNU/Linux (ou le récupère depuis le support d'installation) et l'installe. C'est long, il y a le temps d'aller faire autre chose.

Des services du système peuvent demander à être redémarrés lors de leur mise à jour. Si jamais l'installeur propose de *Redémarrer les services automatiquement lors des mises à jour ?*, on peut répondre *Oui* afin d'éviter que le système demande une confirmation manuelle à chaque fois.

16.5.10 Installation du programme de démarrage GRUB

page 20

Si l'on a choisi d'installer Debian en mode UEFI, l'installeur procède automatiquement et sans poser de questions à l'installation du programme de démarrage GRUB, qui permet de démarrer GNU/Linux.

Dans le cas contraire, l'installeur propose de mettre en place GRUB sur une partie du disque dur appelée « secteur d'amorçage » :

- À la question *Installer le programme de démarrage GRUB sur le disque principal ?*, répondre *Oui*.
- L'installeur demande alors le *Périphérique où sera installé le programme de démarrage*. Choisir le disque dur interne, qui sera en général */dev/sda*. Si le doute persiste, un bon indice est de choisir le premier disque dans la liste dont le nom contient *ata* ou *sata*.

Lorsqu'il a terminé, l'installeur propose de redémarrer l'ordinateur en vérifiant que le support d'installation (CD, DVD, clé USB) n'est plus inséré lors du redémarrage. Choisir *Continuer*.

16.5.11 Redémarrer sur le nouveau système

L'ordinateur démarre alors sur le nouveau système. À un moment, il demande la phrase de passe sur un écran noir : « `Please unlock disk` ». La taper et appuyer sur la touche *Entrée* (↵ ou return) à la fin [15].

Après le démarrage d'un certain nombre de programmes, un écran apparaît avec la mention *debian 11* et le nom du compte entré précédemment. Il faut sélectionner ce dernier, puis entrer le mot de passe associé.

Voilà un nouveau système Debian chiffré prêt à être utilisé. Pour qui n'en aurait jamais utilisé, se balader dedans peut être une bonne idée pour s'y familiariser. La vue d'ensemble des activités, que l'on peut ouvrir en cliquant sur *Activités* en haut à gauche de l'écran ou en appuyant sur la touche ⊞ (⌘ sur un Mac) permet d'accèder aux nombreux logiciels déjà installés. Pour trouver un logiciel, on peut taper un mot décrivant sa fonction (par exemple `image` pour trouver les logiciels qui travaillent avec des images). Pour afficher tous les logiciels installés, cliquer sur ⠿ en bas à gauche. Des pages d'aide contenant de nombreux conseils et astuces sont accessibles en tapant `Aide` dans la vue d'ensemble des activités.

16.6 Paramétrage du dépôt principal de paquets Debian

Une fois l'installation terminée, suivant l'image que l'on a utilisée pour installer Debian, il peut être nécessaire d'aller dans *Software & Updates* pour y ajouter le dépôt principal de paquets Debian.

---

15. Si l'on n'est pas très à l'aise avec la frappe au clavier, il arrive souvent dans les premiers temps qu'on fasse une erreur de frappe dans la phrase. Ne pas s'inquiéter des erreurs répétées, et insister jusqu'à réussir à taper la phrase sans faute… au bout de quelque temps, elle sera « rentrée dans les doigts », et les fautes de frappe se feront plus rares. Cela dit, il ne coûte rien de vérifier qu'on n'a pas malencontreusement laissé la touche VerrMaj enfoncée, auquel cas l'on pourrait s'acharner longtemps sur le clavier sans pour autant arriver à déverrouiller le disque dur.

Pour cela afficher la vue d'ensemble des activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `software` et cliquer sur *Software & Updates*. Dans l'onglet *Debian Software*, sélectionner *Officiellement pris en charge (main)*. Puisque ce logiciel modifie à quels programmes on fait confiance, on est rassuré qu'il nous demande notre mot de passe.

Si l'on a utilisé une image DVD pour procéder à l'installation de Debian, il faut aussi désactiver ce dépôt afin que notre système ne l'utilise plus. Pour cela, dans l'onglet *Other Software*, il faut décocher toutes les lignes commençant par `cdrom:`. Sans cela, Debian voudra que l'on ait toujours le support d'installation inséré dans l'ordinateur pour pouvoir mettre à jour la liste des logiciels disponibles.

Il reste ensuite à fermer la fenêtre *Software & Updates* en cliquant sur le bouton *Fermer*. Il est possible qu'une fenêtre *Les informations sur les logiciels disponibles sont obsolètes* apparaisse, auquel cas il faudra cliquer sur *Actualiser*. Une fenêtre *Cache Refresh* (« rafraîchissement du cache », en français) apparaît pour montrer la progression du téléchargement des listes de paquets disponibles. Cette fenêtre ainsi que celle de *Software & Updates* se ferment automatiquement une fois le rafraîchissement terminé.

16.7 Quelques pistes pour continuer

Il peut maintenant être utile d'apprendre à sauvegarder des données… et à en effacer « pour de vrai ». page 151

Il est également important d'apprendre à garder son système à jour. Des problèmes affectant les logiciels sont découverts régulièrement, et il est important d'installer les corrections au fur et à mesure de leur disponibilité. page 139 page 175

16.8 Un peu de documentation sur Debian et GNU/Linux

Voici quelques références de documentations sur Debian et GNU/Linux :

- Le guide de référence officiel de Debian [16] ;
- La page d'accueil de la documentation officielle d'utilisation de Debian [17] ;
- Le cahier de l'administrateur Debian [18].

On peut trouver beaucoup de documentation sur l'utilisation de GNU/Linux. Si elles sont souvent très utiles, elles sont, comme beaucoup de choses sur Internet malheureusement, de qualité inégale. En particulier, beaucoup d'entre elles arrêteront de fonctionner lorsqu'une partie du système sera modifiée, ou seront peu soucieuses de l'intimité que l'on attend de notre système. Il faut donc faire preuve d'esprit critique et tenter de les comprendre avant de les appliquer.

Ceci dit, voici encore quelques références de wikis et des forums :

- Le wiki officiel de Debian [19] (partiellement traduit de l'anglais) ;
- Le forum en français sur Debian `debian-fr.org` [20] ;

16. https://www.debian.org/doc/manuals/debian-reference/index.fr.html
17. https://www.debian.org/doc/user-manuals.fr.html
18. https://debian-handbook.info/browse/fr-FR/stable/
19. https://wiki.debian.org/fr/FrontPage
20. https://www.debian-fr.org/

Chapitre 17

Choisir, vérifier et installer un logiciel

Cette partie propose quelques recettes à propos de la gestion de ses logiciels :

page 22

- Sur quels critères choisir un logiciel ? On doit parfois choisir un logiciel pour effectuer une certaine tâche, et il est alors possible de se perdre dans la multitude de solutions disponibles… On trouvera dans ce chapitre quelques critères permettant de prendre une décision adéquate.

cette page

- Comment trouver et installer un logiciel avec Debian ? Lorsqu'on cherche à réaliser de nouvelles tâches avec un ordinateur, cela nous amène à installer de nouveaux logiciels. On trouvera dans ce chapitre quelques conseils pour trouver ce que l'on cherche dans Debian.

page 134

- Comment installer des paquets sur Debian ? On a parfois besoin de *paquets* qui complètent des logiciels ou peuvent avoir leur propre rôle.

page 135

- Comment ajouter des dépôts Debian ? Les logiciels qui sont téléchargés par le système Debian se trouvent dans ce qu'on appelle des *dépôts*. Si les dépôts fournis avec Debian contiennent quasiment tous les logiciels dont on peut avoir besoin, il est parfois utile d'en ajouter de nouveaux.

page 136

17.1 Critères de choix

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Une demi-heure à une heure.

On doit parfois choisir un logiciel pour effectuer une certaine tâche, et il est alors possible de se perdre dans la multitude de solutions disponibles. Voici donc quelques critères permettant de prendre une décision adéquate.

L'intérêt d'utiliser des logiciels libres par rapport à des logiciels propriétaires ou même *open source* a d'ores et déjà été expliqué. La suite du texte s'attachera donc uniquement à départager les logiciels libres disponibles.

page 39

17.1.1 Distribution

Il est généralement préférable d'installer des logiciels fournis par sa distribution GNU/Linux (par exemple, Debian). Il y a deux principales raisons à ça.

page 23

Tout d'abord, une question pratique : la distribution fournit les outils pour installer et mettre à jour, de façon plus ou moins automatisée, un ensemble de logiciels ; elle nous alerte lorsque l'un des logiciels que l'on utilise peut être mis à jour, par exemple pour corriger une faille de sécurité. Mais dès lors qu'on installe un logiciel qui n'est pas fourni par sa distribution, il faut penser à le mettre à jour soi-même, se tenir informée des failles de sécurité qui y sont découvertes, gérer les dépendances entre logiciels, *etc.* Ça demande des efforts, du temps, des compétences.

D'autre part, une question de politique de sécurité : lorsqu'on a choisi sa distribution GNU/Linux, on a implicitement décidé d'accorder une certaine confiance à un ensemble de gens, à un processus de production. Installer un logiciel qui n'est pas fourni par sa distribution implique de prendre une décision similaire à propos d'un nouvel ensemble de gens, d'un nouveau processus de production. Une telle décision ne se prend pas à la légère : lorsqu'on décide d'installer un logiciel n'appartenant pas à sa distribution, on élargit l'ensemble des personnes et processus à qui on accorde de la confiance, et on augmente donc les risques. Par exemple, sans quelques précautions, on peut rapidement se retrouver à télécharger un virus.

page 61

17.1.2 Maturité

L'attrait de la nouveauté est bien souvent un piège : un logiciel en plein développement peut contenir des problèmes majeurs qui n'ont pas encore été découverts.

Mieux vaut, autant que possible, choisir un logiciel activement développé et qui a atteint une certaine maturité. Dans un logiciel développé et utilisé depuis au moins quelques années, il y a des chances que les plus gros problèmes aient déjà été découverts et corrigés… y compris les failles de sécurité.

Pour s'en rendre compte, on peut consulter l'historique des logiciels. On les trouve généralement sur leur site web en faisant une recherche avec des termes comme *historique*, *release*, *news* ou *changelog*. Si on constate qu'il y a beaucoup de mises à jours et surtout des mises à jour récentes, ça veut dire que le logiciel est toujours entretenu.

17.1.3 Processus de production et « communauté »

page 40

L'étiquette *logiciel libre* est un critère essentiellement juridique, qui ne doit jamais suffire à nous inspirer confiance.

Certes, le fait qu'un logiciel soit placé sous une licence libre ouvre la possibilité de modes de développement inspirant confiance. Mais les personnes développant ce logiciel peuvent fort bien, intentionnellement ou non, décourager toute coopération et travailler en vase clos. Que nous importe alors que le programme soit *juridiquement* libre, si, de fait, personne d'autre ne lira jamais son code source ?

Il convient donc d'étudier rapidement le processus de production des logiciels, en s'aidant des questions suivantes, qui nous permettront de surcroît de jauger le dynamisme du processus :

- Qui développe ? Une personne, des personnes, toute une équipe ?
- Le nombre de personnes qui contribuent au code source va-t-il en augmentant ou en diminuant ?
- Le développement est-il actif ? Il ne s'agit pas ici de vitesse pure, mais de réactivité, de suivi à long terme, de résistance. Le développement logiciel est une course d'endurance et non un *sprint*.

Et à propos des outils de communication collective sur lesquels s'appuie le développement (listes et salons de discussion, par exemple) :

- A-t-on facilement accès aux discussions guidant le développement du logiciel ?
- Ces discussions rassemblent-elles de nombreuses personnes ?
- Ces personnes participent-elles à son développement, ou ne font-elles que l'utiliser ?
- Quelle atmosphère y règne t-il ? Calme plat, silence de mort, joyeuse cacophonie, sérieux glaçant, bras ouverts, hostilité implicite, tendre complicité ? (Mais aussi : blagues sexistes, remarques racistes ?)
- Le volume de discussion, sur les derniers mois/années, va-t-il en diminuant ou en augmentant ? Plus que le volume brut, c'est surtout la proportion de messages obtenant des réponses qui importe : un logiciel mûr, stable et bien documenté ne sera pas forcément source de discussions, mais si plus personne n'est là pour répondre aux questions des néophytes, ça peut être mauvais signe.

- Peut-on trouver des retours d'utilisation, des suggestions d'améliorations ? Si oui, sont-elles prises en compte ?
- Les réponses sont-elles toujours données par un nombre réduit de personnes, ou existe-t-il des pratiques d'entraide plus larges ?

17.1.4 Popularité

La popularité est un critère délicat en matière de logiciels. Le fait que la grande majorité des ordinateurs de bureau fonctionnent actuellement sous Windows n'indique en rien que Windows soit le meilleur système d'exploitation disponible.

Pour autant, si ce logiciel n'est pas utilisé par beaucoup de monde, on peut douter de sa viabilité à long terme : si l'équipe de développement venait à cesser de travailler sur ce logiciel, que deviendrait-il ? Qui reprendrait le flambeau ?

On peut donc retenir, comme règle générale, qu'il faut choisir un logiciel utilisé par un nombre suffisamment important de personnes, mais pas forcément *le* logiciel le plus utilisé.

Afin de mesurer la popularité d'un logiciel, il est possible, d'une part, d'utiliser les mêmes critères que ceux décrits ci-dessus au sujet du dynamisme de la « communauté » formée autour de lui. On peut aussi regarder dans *Logiciels* l'évaluation d'une application, en ne se fiant pas uniquement à la note mais aussi au nombre de personnes ayant voté. Par exemple, on préfèrera une application qui est notée de trois étoiles avec 295 votes à une autre ayant cinq étoiles mais seulement 19 votes. D'autre part, Debian publie les résultats de son concours de popularité [1], qui permet de comparer non seulement le nombre de personnes ayant installé tel ou tel logiciel, mais aussi, voire surtout, l'évolution dans le temps de leur popularité.

17.1.5 Passé de sécurité

On peut aussi jeter un œil sur le suivi de sécurité [2] proposé par Debian. En y cherchant un logiciel par son nom, on peut avoir la liste des problèmes de sécurité qui y ont été découverts et parfois résolus.

Si ce logiciel a un historique de sécurité parfaitement vierge, ça peut impliquer : soit que tout le monde s'en fout, soit que le logiciel est écrit de façon extrêmement rigoureuse.

Si des failles de sécurité ont été découvertes dans le logiciel étudié, il y a plusieurs implications, parfois contradictoires.

Ces failles ont été découvertes et corrigées :

- donc elles n'existent plus, *a priori* ;
- donc une personne s'est préoccupé de les trouver, et une autre de les corriger : on peut supposer qu'une attention est donnée à cette question.

Mais ces failles ont existé :

- le logiciel est peut-être écrit sans que la sécurité soit un souci particulier ;
- d'autres failles peuvent subsister, non encore découvertes ou pire, non encore publiées.

Afin d'affiner notre intuition par rapport à ce logiciel, il peut être bon de se pencher sur le critère « temps ». Par exemple, il n'est pas dramatique que quelques failles aient été découvertes au début du développement d'un logiciel et si aucune n'a été découverte depuis quelques années, on peut alors mettre ça sur le compte des erreurs

1. Debian.org, 2014, *Debian Popularity Contest* [http://popcon.debian.org/] (en anglais).
2. L'équipe de sécurité de Debian maintient des informations pour chacun des paquets, visibles sur le *security tracker* [https://security-tracker.debian.org/tracker/] (en anglais), site où il est possible de faire une recherche avec le nom du logiciel.

de jeunesse. Au contraire, si de nouvelles failles sont découvertes régulièrement, depuis des années, et jusqu'à très récemment, il est fort possible que le logiciel ait encore de nombreux problèmes de sécurité totalement inconnus… ou non publiés. Tout comme un nombre relativement élevé de failles, même récentes peut indiquer une communauté de développement active et être meilleur signe qu'aucune faille de sécurité pour un logiciel dont très peu de personnes s'occupent au final.

17.1.6 Équipe de développement

Qui a écrit ce logiciel ? Qui le maintient ? Si l'on a réussi à répondre à ces questions, divers indices peuvent nous aider à déterminer la confiance qui peut être accordée à l'équipe de développement. Par exemple :

- Les mêmes personnes ont aussi écrit un autre logiciel que nous utilisons déjà intensivement ; nos impressions sur cet autre logiciel sont tout à fait pertinentes dans le cadre de cette étude.
- Des membres de l'équipe de développement ont des adresses qui finissent par `@debian.org` et ont donc le droit de modifier les logiciels fournis par Debian GNU/Linux ; si nous utilisons cette distribution, nous accordons déjà, de fait, une certaine confiance à ces personnes.
- Des membres de l'équipe de développement ont des adresses qui finissent par `@google.com`, ce qui montre que Google les paie ; s'il n'y a aucun doute à avoir sur leurs compétences techniques, on peut se demander à quel point leur travail est téléguidé par leur employeur qui, lui, n'est digne d'aucune confiance quant à ses intentions concernant nos données personnelles.

17.2 Trouver et installer un logiciel

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : De cinq minutes (si on connaît le nom du logiciel) à une demi-heure (si l'on part de zéro), plus le temps de téléchargement et d'installation (quelques secondes à plusieurs heures selon la taille des logiciels à installer et la vitesse de la connexion).

Parfois, on connaît déjà le nom du logiciel (aussi appelé *application*) que l'on souhaite installer — parce qu'on nous l'a conseillé, parce qu'on l'a trouvé sur Internet — et l'on veut savoir s'il est dans Debian. D'autres fois, on connaît seulement la tâche que l'on souhaiterait que le logiciel remplisse. Dans tous les cas, la base de données des logiciels disponibles dans Debian répondra certainement à nos questions.

page 131

Pour faire des choix éclairés, lorsque plusieurs logiciels permettent d'effectuer une même tâche, voir le chapitre qui propose des critères pour choisir un logiciel.

- Ouvrir l'application *Logiciels* : afficher la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `logic` dans la barre de recherche et cliquer sur *Logiciels*.
- Ensuite, il y a deux techniques pour chercher une application :
  - soit cliquer sur l'icône 🔍 en haut à gauche. Taper le nom de l'application dans la barre de recherche. C'est aussi possible de taper des mots-clés mais les descriptions des applications ne sont pas toujours traduites en français. Avec quelques bases d'anglais, il est souvent intéressant d'essayer des mots-clés dans cette langue.
  - soit sélectionner une catégorie dans le bas de la page (par exemple *Jeux*).
- Les résultats de la recherche s'affichent. En cliquant sur l'icône d'un logiciel, sa description apparait.

page 23

On peut installer le logiciel qui nous intéresse une fois trouvé. Il est nécessaire d'être connectée à Internet puisque les logiciels sont installés à partir de paquets qui sont téléchargés en ligne sur ce qu'on appelle des *dépôts*.

- Cliquer sur le bouton *Installer* sous le logo et le titre du logiciel.

- Puisqu'on va installer une nouvelle application, on nous demande notre mot de passe.
- *Logiciels* installe la nouvelle application.
- Quitter l'application *Logiciels*.

17.3 Trouver et installer un paquet Debian

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Dix minutes, plus le temps de téléchargement et d'installation (quelques secondes à plusieurs heures selon la taille des paquets à installer et la vitesse de la connexion).

On a parfois besoin de paquets. Les paquets permettent d'installer les logiciels, mais ils peuvent aussi les compléter ou avoir leur rôle propre. page 23

Pour installer des *paquets* on peut utiliser le logiciel *Gestionnaire de Paquet Synaptic*.

17.3.1 Trouver un paquet Debian

- Ouvrir le *Gestionnaire de paquets* : afficher la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `paquet` et cliquer sur *Gestionnaire de paquets Synaptic*.
- Puisque le gestionnaire de paquets permet de modifier les logiciels installés sur l'ordinateur, et donc de choisir à quels programmes on fait confiance, on est rassurée qu'il nous demande notre mot de passe pour s'ouvrir.
- Une fois dans le gestionnaire de paquets, commençons par recharger la liste des paquets disponibles en cliquant sur l'icône *Recharger*. Le gestionnaire de paquets télécharge alors les dernières informations sur les paquets disponibles depuis un serveur Debian.
- Ensuite, il y a deux techniques pour chercher un paquet :
  - soit cliquer sur l'icône *Rechercher* à droite dans la barre d'outils. Là, vérifier que *Description et nom* est bien sélectionné dans *Rechercher dans*. Taper des mots-clés ou un nom d'application dans la case *Rechercher* (par exemple « dictionnaire allemand openoffice »). Les descriptions des applications peu courantes sont rarement traduites en français. Avec quelques bases d'anglais, il est souvent intéressant d'essayer des mots-clés dans cette langue ;
  - soit cliquer sur *Catégorie* dans la colonne de gauche, choisir la catégorie semblant adaptée au paquet.
- Les résultats de la recherche ou les paquets de la catégorie s'affichent alors dans une liste. En cliquant sur le nom d'un paquet, sa description apparaît dans le cadre en bas. Reste maintenant à installer le paquet correspondant.

17.3.2 Sélectionner le paquet à installer

Pour l'installation proprement dite du paquet trouvé précédemment, il y a différentes façons de faire selon que l'on souhaite utiliser la version par défaut, disponible dans les dépôts officiels de sa distribution ou un paquet provenant d'un autre dépôt, par exemple pour avoir une version plus récente.

Pour installer la version par défaut

Normalement, le paquet désiré se trouve maintenant quelque part dans la liste de paquets. Une fois trouvée la ligne correspondante, on clic-droit dessus, et dans le menu qui apparaît on choisit *Sélectionner pour installation*.

Parfois, pour le bon fonctionnement de ce à quoi servira le paquet, il est nécessaire d'en installer d'autres. Par exemple, si plusieurs logiciels utilisent un même paquet,

pour que celui-ci ne soit installé qu'une seule fois il n'est pas contenu dans chacun des logiciels, mais il existe séparément et les logiciels s'y refèrent. Si le paquet à installer dépend d'autres paquets, le gestionnaire ouvre une fenêtre où il demande s'il doit *Prévoir d'effectuer d'autres changements ?* En général, ses propositions sont pertinentes, et on peut accepter en cliquant sur *Ajouter à la sélection*.

Pour installer une version particulière

Parfois, on souhaite installer une version particulière d'un paquet parmi celles disponibles, par exemple, si on a ajouté des dépôts spécifiques. Au lieu de choisir *Sélectionner pour installation* dans le menu contextuel, on sélectionne le paquet désiré d'un clic gauche sur son nom, sans cliquer sur la case à cocher. Puis on va dans le menu déroulant *Paquet*, et on choisit *Forcer la version…*. Sélectionner alors la version désirée. Si cette option est grisée, c'est qu'elle n'est pas disponible car il n'y a qu'une seule version du paquet. La suite ne change pas.

cette page

17.3.3 Appliquer les modifications

Il est possible de répéter les deux dernières étapes pour installer plusieurs paquets en même temps. Une fois qu'on a préparé ces installations, il ne reste qu'à la lancer en cliquant sur *Appliquer* dans la barre d'outils. Le gestionnaire de paquets ouvre alors une fenêtre *Résumé* où il liste tout ce qu'il va faire. Après avoir jeté un œil pour vérifier qu'on ne s'est pas trompée, on clique sur *Appliquer*.

Le gestionnaire de paquets télécharge alors les paquets depuis Internet, les vérifie, puis les installe. Il peut arriver que le gestionnaire indique que certains paquets n'ont pas pu être vérifiés : **cette information n'est pas à prendre à la légère**. Dans un tel cas, il vaut mieux annuler le téléchargement, cliquer sur *Recharger* dans le menu principal, et recommencer l'opération de sélection des paquets. Si l'indication apparaît de nouveau, cela peut être le fruit d'une attaque, d'une défaillance technique ou de soucis de configuration. Mais autant s'abstenir d'installer de nouveaux paquets avant d'avoir identifié la source du problème.

Enfin, si tout s'est bien passé, le gestionnaire de paquets affiche une fenêtre comme quoi *Les modifications ont été appliquées* et on peut donc cliquer sur *Fermer*. Pour finir, fermer le gestionnaire de paquets pour éviter qu'il ne tombe entre d'autres mains.

17.4 Ajouter des dépôts

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Un quart d'heure à une demi-heure.

Les paquets Debian qui contiennent les programmes se trouvent dans ce qu'on appelle des *dépôts*. Si les dépôts fournis avec Debian contiennent quasiment tous les logiciels dont on peut avoir besoin, il est parfois utile :

- d'installer des logiciels plus récents que ceux contenus dans la dernière version stable de Debian, dits *backports*, ou *rétroportés* en français ;
- d'installer des logiciels non-libres (*non-free*, par exemple des microprogrammes) ou fournis par des tiers (*contrib*, par exemple le navigateur Tor).

Attention : ajouter un nouveau dépôt Debian sur un ordinateur revient à décider de faire confiance aux gens qui s'en occupent. Si les dépôts de *backports* dont on parle ici sont maintenus par des membres de Debian, ce n'est pas le cas pour de nombreux autres dépôts. La décision de leur faire confiance ne doit pas se prendre à la légère : si le dépôt en question contient des logiciels malveillants, il serait possible de les installer sur l'ordinateur sans même s'en rendre compte.

page 32

17.4.1 Ouvrir *Software & Updates*

Ouvrir le *Software & Updates* : pour cela afficher la vue d'ensemble des activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `softw` et cliquer sur *Software & Updates*.

17.4.2 Désactiver les supports d'installation locaux

Comme indiqué dans le chapitre précédent, suivant l'image d'installation utilisée pour installer Debian, il se peut que le système de gestion des paquets demande à ce que l'on ait toujours ce support d'installation branché sur l'ordinateur afin de pouvoir faire la mise à jour de la liste des paquets disponibles.

page 128

Afin d'éviter cela, il faut désactiver les dépôts de ce support d'installation : dans l'onglet *Other Software*, décocher toutes les lignes commençant par `cdrom:`.

17.4.3 Configurer l'emplacement du dépôt

Pour installer les logiciels rétroportés

Cliquer sur l'onglet *Other Software*, puis sur le bouton *Add*.

Dans *Ligne APT* entrer le répertoire APT à ajouter :

```
deb http://deb.debian.org/debian/ bullseye-backports main
```

Dans ce cas, la *version du dépôt* est *bullseye-backports* et la *catégorie* est *main*.

Une fois que c'est fait, cliquer sur ✚ *Ajouter une source de mise à jour*.

Puisque ce logiciel modifie à quels programmes on fait confiance, on est rassuré qu'il nous demande notre mot de passe.

Pour installer les logiciels non-libres ou fournis par des tiers

- Dans l'onglet *Debian Software*, sélectionner en fonction de ses besoins
  - *contrib* pour ajouter les logiciels fournis par des tiers ;
  - *non-free* pour ajouter les logiciels non-libres.

Puisque ce logiciel modifie à quels programmes on fait confiance, on est rassuré qu'il nous demande notre mot de passe.

17.4.4 Mettre à jour les paquets disponibles

Il reste ensuite à fermer la fenêtre *Software & Updates* en cliquant sur le bouton *Fermer*. Il est possible qu'une fenêtre *Les informations sur les logiciels disponibles sont obsolètes* apparaisse, auquel cas il faudra cliquer sur *Actualiser*. Une fenêtre *Cache Refresh* (« rafraîchissement du cache », en français) apparaît pour montrer la progression du téléchargement des listes de paquets disponibles. Cette fenêtre ainsi que celle de *Software & Updates* se ferment automatiquement une fois le rafraîchissement terminé.

Pour installer un paquet à partir des rétroportages, suivre l'outil installer un paquet et choisir d'installer une version particulière lorsque la question se présente.

page 135

Chapitre 18

Effacer des données « pour de vrai »

On a vu dans la partie Comprendre que lorsqu'on efface un fichier, son contenu n'est pas vraiment supprimé. Cependant, il existe des programmes qui permettent d'effacer des fichiers *et leur contenu*, ou du moins qui tentent de le faire, avec les limites expliquées auparavant.

page 42
page 42

18.1 Un peu de théorie

18.1.1 La méthode de Gutmann

La documentation du paquet *secure-delete*, que nous utiliserons dans la prochaine recette, inspirée d'une publication de Peter Gutmann publiée en 1996 [1], nous dit (en anglais) :

Le processus d'effacement fonctionne comme suit :

1. *la procédure d'écrasement (en mode sécurisé) remplace le contenu du fichier [...]. Après chaque passage, le cache du disque est vidé ;*
2. *le fichier est tronqué, de sorte qu'un attaquant ne sache pas quels blocs du disque appartenaient au fichier ;*
3. *le fichier est renommé, de sorte qu'un attaquant ne puisse tirer aucune conclusion sur le contenu du fichier supprimé à partir de son nom ;*
4. *finalement, le fichier est supprimé. [...]*[2]

Pour un disque dur magnétique de moins de 20 ans [3] : il suffit d'écraser les données quelques fois avec des données aléatoires.

Le NIST (*National Institute of Standards and Techonology*, organisme gouvernemental états-unien définissant les protocoles de sécurité utilisés, entre autres, par les administrations de ce pays) a publié une étude de 2006 [4] de la NSA, qui semble conclure que sur les disques durs magnétiques récents, les données sont tellement collées les unes aux autres qu'il devient pratiquement impossible de se livrer à des analyses magnétiques pour retrouver les traces de données effacées.

Par conséquent, nous nous contenterons dans les recettes qui suivent de quelques réécritures aléatoires.

Cependant, cette méthode n'est pas adaptée aux disques SSD. Or, les disques SSD tendent de nos jours à remplacer les disques durs…

page 42

Il s'agira une fois de plus de faire le bon compromis, au cas par cas, entre la rapidité

page 65

1. Peter Gutmann, 1996, *Secure Deletion of Data from Magnetic and Solid-State Memory* [https://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html] (en anglais).
2. Source : fichier `README.gz` de *secure-delete* installé sur une Debian dans `/usr/share/doc/secure-delete`.
3. Utilisant la technologie PRML [https://fr.wikipedia.org/wiki/PRML], apparue en 1990 [https://www.datadoctor.biz/datarecoverybook/chapter-2.html] (en anglais).
4. NIST, 2006, *Guidelines for Media Sanitization* [https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-88.pdf] (en anglais).

et le niveau de protection souhaité, en fonction de la taille des données à écraser, de l'âge du disque dur, et de la confiance qu'on accorde au NIST.

18.1.2 Pour les clés USB, disques SSD et autres mémoires *flash*

Pour les clés USB ou autre mémoire *flash* - comme les cartes SD, ou disques SSD - une étude datant de 2011 [5] a montré que la situation était réellement problématique.

Cette étude démontre qu'il est impossible, quel que soit le nombre de réécritures, d'avoir la garantie que tout le contenu d'un fichier donné a bien été recouvert. Même si cela rend inaccessibles les données en branchant simplement la clé, elles sont toujours visibles pour quiconque regarderait directement dans les puces de mémoire *flash*.

La seule méthode qui a fonctionné de façon systématique était de réécrire plusieurs fois l'*intégralité* de la clé USB. Dans la plupart des cas, deux passages ont suffi, mais sur certains modèles, vingt réécritures ont été nécessaires avant que les données ne disparaissent pour de bon.

page 145 Partant de ces constats, la réponse préventive semble être de chiffrer systématiquement les clés USB, opération rendant vraiment plus difficile l'extraction des informations directement depuis les puces de mémoire *flash*. Et pour nettoyer a posteriori, l'écrasement entier, malgré ses limites, protège tout de même contre les attaques purement logicielles.

La seule solution pour rendre illisible les données de ces supports est de les détruire physiquement.

18.1.3 D'autres limites de l'effacement « sécurisé »

⚠ Il peut encore rester des informations sur le fichier permettant de le retrouver, notamment si l'on utilise un système de fichiers journalisé comme *ext4*, Btrfs, HFS+, ReFS, NTFS, un système d'écriture, de compression ou de sauvegarde (que ce soit sur disque, par exemple avec RAID [6] ou *via* un réseau). Voir à ce sujet la première partie.

page 43

18.2 Sur d'autres systèmes

page 39 On a vu qu'il est illusoire, si l'on utilise un système d'exploitation propriétaire, de rechercher une réelle intimité. Bien qu'il existe des logiciels supposés effacer des fichiers avec leur contenu sous Windows et macOS, il est donc bien plus difficile de leur faire confiance.

18.3 Allons-y

On peut effacer le contenu :

- de fichiers individuels (voir page suivante) ;
- de tout un périphérique (voir page ci-contre) ;
- de fichiers déjà supprimés (voir page 143).

---

5. Michael Wei *et al.*, 2011, *Reliably Erasing Data From Flash-Based Solid State Drives* [https://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf] (en anglais).

6. RAID signifie « regroupement redondant de disques indépendants » (*Redundant Array of Independent Disks* en anglais). C'est un système qui répartit des données sur plusieurs disques afin d'améliorer soit les performances, la sécurité ou la tolérance aux pannes (Wikipédia, 2021, *RAID (informatique)*)[https://fr.wikipedia.org/wiki/RAID_(informatique)]

18.4 Supprimer des fichiers... et leur contenu

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Cinq minutes de préparation, puis quelques secondes à plusieurs heures d'attente en fonction de la taille du fichier à effacer et de la méthode utilisée.

Voici donc la méthode à suivre pour se débarrasser de fichiers, en prenant soin de rendre illisible ce qu'ils contenaient.

Attention : cette méthode ne fonctionne qu'avec les disques durs mécaniques. Après avoir recouvert le contenu de fichiers sur une clé USB (ou tout autre support de stockage utilisant de la mémoire *flash* comme une carte SD ou un disque SSD) il y a de fortes chances qu'il se trouve encore inscrit dans une région inaccessible du périphérique !

18.4.1 Installer les logiciels nécessaires

Si ce n'est pas déjà fait, il nous faut installer le paquet `nautilus-wipe` (voir page 135), puis redémarrer l'ordinateur.

Ce paquet est présent par défaut dans Tails.

18.4.2 Supprimer des fichiers et leur contenu à partir du navigateur de fichiers

Dans Tails

Afin de supprimer des fichiers et leur contenu en utilisant Tails, consulter la documentation en cliquant sur l'icône *Documentation de Tails* se trouvant sur le bureau. Dans l'index qui s'ouvre, chercher la section *Chiffrement et vie privée* et cliquer sur la page *Effacer des fichiers de façon sécurisée et nettoyer l'espace disque*.

Avec une Debian chiffrée

Afin de supprimer des fichiers et leur contenu depuis le navigateur de fichiers, naviguer jusqu'au fichier, faire un clic-droit sur celui-ci et sélectionner *Écraser*. Une fenêtre s'ouvre nous demandant de confirmer la suppression, et proposant également quelques *Options*.

Nous pouvons choisir le nombre de passes à effectuer afin de recouvrir les données de notre périphérique ainsi que quelques options de comportement lors de l'effacement des données. Les options par défaut sont suffisantes pour les disques durs magnétiques.

Cliquer ensuite sur *Écraser*. Une fois l'effacement terminé, une fenêtre *L'écrasement a réussi* s'ouvre, précisant que *Le(s) élément(s) ont été écrasé(s) avec succès.*

18.5 Effacer « pour de vrai » tout un disque

Avant de se débarrasser d'un disque dur, de le recycler, de réinstaller un système propre, ou encore d'envoyer un ordinateur en panne au service après-vente, il peut être judicieux de mettre des bâtons dans les roues des gens qui voudraient récupérer les données qu'il contenait. Pour cela, la meilleure solution est encore de réécrire l'intégralité du disque avec des données aléatoires.

page 71

Avant d'utiliser cette recette, il faut réfléchir à deux fois et sauvegarder soigneusement les données à conserver. Si elle est bien appliquée, elle rend en effet les données très difficiles à récupérer, même en analysant le disque dans un laboratoire.

page 151

18.6 Effacer tout le contenu d'un disque

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Cinq minutes de préparation, puis plusieurs heures d'attente en fonction de la taille du disque.

page suiv.

Pour effacer un volume complet (disque ou partition), on va utiliser la commande `shred` de façon à ce qu'elle recouvre la totalité des données trois fois avec des données aléatoires. Cette commande permet donc, en plus de l'effacement des fichiers, de recouvrir l'espace effacé de telle manière qu'il devient quasiment impossible de retrouver ce qu'il contenait auparavant.

page 113

Pour recouvrir le contenu d'un disque, il est nécessaire de ne pas être en train de l'utiliser… s'il contient le système d'exploitation habituellement utilisé, il faut donc mettre le disque dur dans un autre ordinateur ou utiliser un système *live*. `shred` étant un outil standard, n'importe quel système *live* devrait faire l'affaire.

La commande est très simple. Elle exige seulement de connaître l'emplacement du périphérique (son chemin) que l'on veut effacer, puis de faire preuve de patience car le processus prend plusieurs heures.

18.6.1 Trouver le chemin du périphérique

Avant tout, il faut savoir repérer sans se tromper le chemin utilisé par le système d'exploitation pour désigner le support de stockage qu'on veut effacer.

Si l'on souhaite effacer un disque interne, commencer par débrancher tous les disques durs externes, clés USB, lecteurs de cartes mémoire ou autres périphériques de stockage branchés sur l'ordinateur. D'une part, cela évitera de les effacer par erreur ; d'autre part, cela rendra la recherche du disque interne plus facile.

Bien sûr, il ne faut pas faire cela si c'est justement le contenu d'un disque externe que l'on souhaite rendre inaccessible.

Ouvrir l'utilitaire de gestion des disques

Ouvrir Disques : afficher la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `disque` et cliquer sur *Disques*.

Chercher le chemin du périphérique

La partie située à gauche indique la liste des disques connus du système. On peut cliquer sur l'un d'entre eux afin de voir plus d'informations apparaître sur la partie droite. Les icônes, la taille indiquée ainsi que le nom des disques devraient permettre d'identifier celui que l'on cherche.

Si cela ne suffit pas, il est possible de jeter un œil à l'organisation des partitions, en regardant le tableau qui apparaît dans la partie droite :

- si le disque à effacer contenait un système GNU/Linux non chiffré, il doit y avoir au moins deux partitions, l'une avec un système de fichiers *Swap*, l'autre en général *Ext3* ou *Ext4* ;
- si le disque à effacer contenait un système GNU/Linux chiffré, il doit y avoir au moins deux partitions, l'une avec un système de fichiers *Ext2*, l'autre *LUKS* ;
- si le disque à effacer contenait un système Windows, il doit y avoir une ou plusieurs partitions notées *NTFS* ou *FAT*.

Par ailleurs, le périphérique correspondant au disque interne est généralement le premier de la liste.

Une fois le disque trouvé et sélectionné, on pourra lire le chemin du disque dans la partie de droite en bas, à côté de l'étiquette *Périphérique*.

Le chemin du périphérique commence par `/dev/` suivi de trois lettres et éventuellement d'un chiffre, les premiers caractères étant dans la plupart des cas `sd`, `hd`, ou `mmcblk` : par exemple, `/dev/sdx1`. Noter le chemin quelque part, sans le chiffre (par exemple `/dev/sdx`) : il faudra l'écrire tout à l'heure à la place de `LE-PÉRIPHÉRIQUE`.

⚠ **Attention** : ce chemin n'est pas nécessairement toujours le même. Il vaut mieux recommencer cette courte procédure après avoir redémarré l'ordinateur, branché ou débranché une clé USB ou un disque dur. Cela évitera les mauvaises surprises… comme perdre le contenu d'un autre disque dur.

18.6.2 Lancer la commande shred

Ouvrir un Terminal : ouvrir la vue d'ensemble activités en appuyant sur la touche page 97
(⌘ sur un Mac), puis taper `term` et cliquer sur *Terminal*.

Saisir la commande suivante en veillant à remplacer `LE-PÉRIPHÉRIQUE` par le chemin de périphérique déterminé précédemment :

```
pkexec shred -n 3 -v LE-PÉRIPHÉRIQUE
```

Si l'on préfère utiliser la méthode originale de Gutmann (plus longue, et peut-être plus sûre), il faut remplacer `-n 3` par `-n 25` dans la ligne de commande.

Une fois la commande tapée et vérifiée, appuyer sur la touche *Entrée* (↵ ou return). Un mot de passe est demandé, car cette commande nécessite les privilèges page 99
d'administration, le saisir. La commande `shred` va alors écrire dans le terminal ce qu'elle fait (puisqu'on le lui a demandé en ajoutant à la commande `shred` l'option `-v`, qui signifie, dans le cadre de *cette* commande, que l'ordinateur doit être « verbeux » — c'est-à-dire « bavard ») :

```
shred: /dev/sdb: pass 1/3 (random)...
shred: /dev/sdb: pass 2/3 (random)...
shred: /dev/sdb: pass 3/3 (random)...
```

À la fin de la procédure, le terminal affiche à nouveau le signe `$`, qui symbolise l'invite de commande. On peut alors fermer le terminal.

18.6.3 Réutiliser le disque

Attention, cette méthode efface non seulement les données d'un volume complet mais, à la fin de l'opération, le disque n'a plus ni table de partitions, ni système de fichiers. page 23
Pour le réutiliser, il est nécessaire de créer entièrement au moins une nouvelle partition et son système de fichiers, avec l'application Disques par exemple. page 24

18.7 Rendre irrécupérables des données déjà supprimées

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Cinq minutes de préparation, puis de plusieurs minutes à plusieurs heures d'attente, selon la taille du disque à nettoyer et selon la méthode utilisée.

Lorsque des fichiers ont *déjà* été effacés sans précautions particulières, les données qu'ils contenaient se trouvent toujours sur le disque. L'objectif de cette recette est de recouvrir les données qui subsisteraient, en écrasant l'espace libre d'un disque dur. Cette méthode ne supprime donc aucun fichier visible dans le navigateur de fichiers.



Attention : comme les autres façons d'effacer un fichier « pour de vrai », cela ne marche pas avec certains systèmes de fichiers « intelligents » qui, pour être plus efficaces, ne vont pas montrer tout l'espace libre au logiciel chargé d'y recouvrir les traces. Il ne faut pas non plus faire confiance à cette méthode pour les clés USB, les cartes SD ou les disques SSD et préférer recouvrir plusieurs fois l'intégralité des données qu'ils contiennent.

page 43
page 142

Dans Tails

Le paquet `nautilus-wipe` est déjà installé par défaut dans Tails. Il nous suffit donc de consulter la documentation, en cliquant sur l'icône *Documentation de Tails* se trouvant sur le bureau. Puis, dans l'index qui s'ouvre, chercher la section *Chiffrement et vie privée* et cliquer sur la page *Effacer des fichiers de façon sécurisée et nettoyer l'espace disque*.

Avec une Debian chiffrée

Si ce n'est pas déjà fait, il nous faut installer le paquet `nautilus-wipe` (voir page 135), puis redémarrer l'ordinateur.

Il nous faut ensuite ouvrir un navigateur de fichiers, puis naviguer jusqu'au disque que l'on veut nettoyer. Effectuez ensuite un clic-droit dans la partie droite du navigateur de fichiers et sélectionnez *Écraser l'espace disque disponible*. Une fenêtre s'ouvre nous demandant de confirmer la suppression de l'espace disque disponible, et proposant également quelques *Options*.

Nous pouvons choisir le nombre de passes effectuées afin de recouvrir les données de notre périphérique, ainsi que quelques options de comportement lors de l'effacement des données. Les options par défaut sont suffisantes pour les disques magnétiques actuels.

Cliquer ensuite sur *Écraser l'espace disque disponible*. L'effacement peut prendre du temps. Dans certains cas, le mot de passe d'administration est demandé.

Remarquons qu'un dossier appelé *tmp.XXXXXXXXXX* est créé dans le dossier. Nautilus Wipe va créer ce fichier à l'intérieur et en augmenter la taille autant que possible, afin d'utiliser tout l'espace libre disponible, puis l'écrasera de manière sécurisée. Une fois l'effacement terminé, une fenêtre *L'écrasement a réussi* s'ouvre, précisant que *L'espace disque disponible sur la partition ou le périphérique « … » a été écrasé avec succès*.

Chapitre 19

Partitionner et chiffrer un disque dur

Nous allons maintenant aborder le chiffrement d'un périphérique, afin d'y stocker des données de manière confidentielle.

Une fois un disque chiffré, les données qu'il contient ne sont accessibles que lorsqu'on a tapé une phrase de passe permettant de le déchiffrer. Pour plus d'informations là-dessus, on peut consulter la partie sur la cryptographie.

page 47

Lorsque la phrase de passe est saisie, le système a accès aux données du périphérique en question, il ne faut donc pas taper cette phrase de passe n'importe où, mais seulement sur les ordinateurs et les systèmes dans lesquels on a suffisamment confiance.

page 65

En effet, non seulement ceux-ci auront accès aux données déchiffrées, mais des traces de la présence du périphérique seront également gardées sur l'ordinateur. C'est pourquoi nous vous conseillons plutôt de l'utiliser sur un système GNU/Linux chiffré ou un système *live* amnésique.

page 27
page 119
page 113

Il peut s'agir d'un disque dur, d'un disque SSD, d'une clé USB, d'une carte SD ou encore d'une partie seulement d'un de ces périphériques. On peut en effet découper un disque dur ou une clé USB en plusieurs morceaux indépendants, qu'on appelle des partitions.

page 23

Ci-dessous, on parlera de disque pour désigner, sauf mention contraire, aussi bien un disque dur interne qu'un disque dur externe, ou tout type de périphérique à mémoire *flash*, comme une clé USB, un disque SSD, ou une carte SD.

Si on veut avoir un endroit sur le disque où mettre des données qui ne seront pas confidentielles, et auxquelles on pourra accéder sur des ordinateurs non dignes de confiance, il est possible de découper le disque en deux partitions :

1. une partition non chiffrée, où l'on ne met que des données non confidentielles, comme de la musique, et que l'on peut utiliser depuis tous les ordinateurs sans taper la phrase de passe ;
2. une partition chiffrée, avec des données confidentielles, qu'on n'ouvre que sur les ordinateurs auxquels on fait confiance.

19.1 Vue d'ensemble

19.1.1 Chiffrer un disque avec LUKS et `dm-crypt`

On va expliquer comment chiffrer un disque avec les méthodes standard sous GNU/-Linux, appelées `dm-crypt` et LUKS, qui sont des logiciels libres. Ce système est maintenant bien intégré avec les environnements de bureau, et la plupart des opérations sont donc possibles sans avoir besoin d'outils particuliers.

page 40

19.1.2 D'autres logiciels que l'on déconseille

page 39

Pour chiffrer un disque, on déconseille d'utiliser des logiciels propriétaires, auxquels on ne peut pas faire confiance, comme par exemple : FileVault, BitLocker, Stormshield Endpoint Security ou encore Symantec PGP Whole Disk Encryption. Il existe aussi des logiciels libres, comme VeraCrypt [https://www.veracrypt.fr/] qui peuvent fonc-

page 22

tionner sur un un système d'exploitation propriétaire. Cependant, si l'on utilise un logiciel, même libre, sur un système d'exploitation propriétaire, on fait implicitement confiance à ce dernier puisqu'il a forcément accès aux données déchiffrées.

19.1.3 Aperçu des étapes

Si le disque a déjà servi, ça peut être une bonne idée de commencer par recouvrir ses données (voir page 141).

Si le disque à chiffrer ne dispose pas d'espace libre, commencer par le formater (voir cette page). Cela peut impliquer d'effacer toutes les données qui se trouvent dessus.

Ensuite, si l'on souhaite chiffrer une partie seulement du disque, il faut d'abord créer une partition en clair (voir page ci-contre).

Si l'on a déjà de l'espace non partitionné sur son disque, on peut directement passer à l'étape de chiffrement (voir page 148).

À la suite de quoi, il ne reste plus qu'à l'initialiser pour contenir des données chiffrées (voir page 148).

Et le voilà enfin prêt à être utilisé (voir page 148).

19.2 Préparer un disque à chiffrer

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Environ dix minutes.

Ci-dessous, on parlera toujours de disque pour désigner aussi bien un disque interne ou externe, que pour une clé USB, une carte SD ou un disque SSD, sauf si on précise le contraire.

La procédure que l'on explique ici implique d'effacer toutes les données qui se trouvent sur le disque[1]. Si l'on a déjà de l'espace non partitionné sur son disque, on peut directement passer à l'étape de chiffrement (voir page 148).

19.2.1 Installer les paquets nécessaires

Pour chiffrer un disque, nous avons besoin des paquets suivants : `secure-delete`, `dosfstools` et `cryptsetup`. Avec Debian 11, il faut donc installer le paquet (voir page 135) `secure-delete`, les deux autres étant installés par défaut. Si l'on utilise Tails, ces trois paquets sont déjà installés.

19.2.2 Formater le disque avec l'utilitaire Disques

Formater implique d'effacer toutes les données qui se trouvent sur le disque.

Pour ouvrir l'application Disques à partir de la vue d'ensemble des Activités : taper sur la touche ⊞ (⌘ sur un Mac), puis taper `disques` et cliquer sur *Disques*.

Dans la fenêtre de l'application Disques la partie de gauche liste les disques connus du système ; la partie de droite permet d'effectuer des actions.

1. Il est cependant possible de *redimensionner* une partition déjà existante tout en gardant les fichiers qui s'y trouvent.

Choisir le périphérique

À gauche, il y a la liste des disques. Si l'ordinateur utilisé contient un système chiffré, il y a aussi les volumes chiffrés de notre système.

Les icônes, la taille indiquée ainsi que le nom des disques doivent nous permettre d'identifier celui que l'on cherche.

Une fois le disque repéré, le sélectionner dans la liste. Les informations qui s'affichent dans la partie droite de la fenêtre doivent permettre de confirmer qu'on a sélectionné le disque voulu.

Démonter les volumes

Si le volume est monté, une icône carrée ■ est visible dans la partie de droite, sous la représentation graphique du disque dans la rubrique *Volumes*. Cliquer sur ce bouton afin de démonter le volume.

Si ce disque contient plusieurs volumes, les démonter un par un : les sélectionner dans la représentation graphique de la rubrique *Volumes* puis les démonter comme expliqué précédemment.

Reformater le disque

⚠ **Attention** : formater un disque revient à supprimer tous les fichiers qui s'y trouvent.

Dans la barre supérieure du logiciel, cliquer sur l'icône ⋮, puis sur *Formater le disque…*. Une fenêtre s'ouvre et propose d'effacer ou non les données sur le support, et de formater le disque. En fonction du contexte, et des limites abordées précédemment, page 42 choisir si les données doivent être effacées ou non. Laisser *Compatible avec tous les systèmes et périphériques* dans *Partitionnement*, puis cliquer sur le bouton *Formater…*.

Disques demande si l'on veut vraiment formater le périphérique. C'est le moment de vérifier que l'on a choisi le bon périphérique avant de faire une bêtise. Si c'est bien le cas, confirmer en cliquant sur *Formater*.

Le formatage peut prendre un peu de temps, une barre d'avancement apparaît dans l'application Disques. Attendre que la tâche soit terminée avant de démonter ou débrancher le disque.

19.3 Créer une partition non chiffrée

↻ *Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.*

🕓 *Durée : Deux minutes.*

Si on le souhaite, c'est le moment de créer une partition non chiffrée où l'on mettra des données qui ne sont pas confidentielles, et que l'on pourra utiliser depuis tous les ordinateurs sans avoir à taper de phrase de passe.

Si l'on désire chiffrer le disque en entier, on peut directement passer à l'étape suivante (voir page suivante).

Toujours dans l'application Disques, sélectionner le disque voulu, puis dans la partie droite cliquer sur la zone *Espace disponible* du schéma des *Volumes*. En-dessous, cliquer ensuite sur le symbole ✚.

Choisir la taille voulue pour la partition non chiffrée dans le champs dédié. L'espace laissé libre nous servira pour la partition chiffrée. Cliquer sur *Suivant*.

On peut choisir un nom pour cette partition. Dans *Type*, choisir *Compatible avec tous les systèmes et périphériques (FAT)*. Une fois cela fait, cliquer sur *Créer*.

19.4 Créer une partition chiffrée

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Dix minutes + entre quelques minutes et plusieurs heures pour remplir l'espace libre, selon la taille de la partition.

19.4.1 Créer la partition chiffrée

Toujours dans Disques avec le disque cible sélectionné, cliquer dans la partie droite sur la zone *Espace disponible* du schéma des *Volumes*. Cliquer ensuite en-dessous sur le symbole ✚.

Choisir la taille de la partition : garder la taille maximale puisqu'on veut créer une seule partition chiffrée dans cet espace disponible. Cliquer sur *Suivant*.

Il est possible de donner un nom à la future partition chiffrée. Il n'est pas nécessaire d'activer l'option Effacer. L'effacement se fera à l'étape suivante, via le remplissage par des données aléatoires, qui sera plus fiable. Dans la section *Type* choisir *Disque interne à utiliser avec les systèmes Linux uniquement (Ext4)* puis cocher *Volume protégé par motde passe (LUKS)*. Cliquer sur *Suivant*. Choisir une bonne phrase de passe (voir page 103) pour le volume chiffré et la taper dans les deux champs appropriés. Enfin, cliquer sur *Créer*.

19.4.2 Remplir la partition de données aléatoires

Pour finir, on va remplir l'espace vide du disque chiffré avec des données aléatoires. Cela permet de cacher l'endroit où vont se trouver nos données, et donc de compliquer la vie des personnes qui voudraient tenter de les déchiffrer.

Sur le schéma des *Volumes*, repérer *Partition [...] LUKS* et sélectionner le *Système de Fichiers* situé en dessous. Sous le schéma, cliquer sur ▶.

En bas de la fenêtre, dans *Contenu*, un lien apparaît après *Monté sur*. Cliquer sur ce lien pour ouvrir le dossier, puis suivre l'outil servant à rendre irrécupérables des données déjà supprimées (voir page 143).

Le processus dure de quelques minutes à quelques heures, selon la taille du disque et sa vitesse (par exemple, deux heures pour une clé USB de 4 Go).

19.4.3 Débrancher *proprement* le disque

Dans le navigateur de fichiers, cliquer sur le symbole ⏏, puis débrancher physiquement le disque (le cas échéant).

Le disque chiffré est maintenant utilisable.

19.5 Utiliser un disque dur chiffré

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Deux minutes, quelques heures… ou jamais, si la phrase de passe nous échappe.

Afin de permettre au système d'accéder aux données qui se trouvent sur un disque chiffré, il est nécessaire d'indiquer une phrase de passe (ça tombe bien, c'est ce qu'on voulait !) Mais cette opération est plus ou moins simple selon les environnements.

19.5.1 Avec Debian (ou autre GNU/Linux)

Sur un système GNU/Linux avec un environnement de bureau configuré pour ouvrir automatiquement les médias externes, une fenêtre apparaît pour demander la phrase de passe lorsqu'on branche un disque externe contenant des données chiffrées.

Si ce n'est pas le cas, cette fenêtre apparaît quand on demande au système d'ouvrir la partition chiffrée, par exemple à partir de *Fichiers* en cliquant sur le nom du disque dans la colonne de gauche.

Pour fermer la partition chiffrée, il suffit de démonter le disque comme on le fait habituellement.

19.5.2 Avec d'autres systèmes

Nous ne connaissons pas de moyen simple d'accéder à la partition chiffrée du disque ni sous Windows, ni sous macOS. Même si des solutions peuvent exister[2], il est bon de rappeler qu'il s'agit de systèmes d'exploitation propriétaires, en lesquels il n'y a aucune raison d'avoir confiance. page 39

Pour mettre sur le disque des données auxquelles on veut accéder sur des ordinateurs en lesquels on n'a pas confiance, le mieux à faire est alors probablement de prévoir sur ce disque une deuxième partition, non chiffrée, comme expliqué précédemment. page 147

2. Pour les anciennes versions de Windows (jusqu'à Vista), il était possible d'utiliser FreeOTFE (https://sourceforge.net/projects/freeotfe.mirror/) (en anglais).

Chapitre 20

Sauvegarder des données

Réaliser des sauvegardes est une opération relativement simple dans son principe : faire une copie des fichiers qu'on ne voudrait pas perdre, sur un autre support de stockage que celui où se trouvent les données.

Bien entendu, si on prend le soin de mettre nos données de travail sur des disques durs ou des clés USB chiffrées, il est nécessaire que ces copies soient chiffrées, elles aussi.

Deux autres points à ne pas négliger pour mettre en place une bonne *politique de sauvegarde* :

- définir une méthode pour effectuer **régulièrement** ses sauvegardes,
- tester de temps à autre si les sauvegardes sont toujours bien lisibles.

Ce dernier aspect est vraiment à ne pas négliger. Perdre les données originales est souvent pénible. S'apercevoir ensuite que les sauvegardes ne permettent pas de *restaurer* ce qu'on a perdu transforme la situation en catastrophe.

Il est aussi pertinent de stocker les sauvegardes dans un lieu différent des données originales, pour éviter que tout soit détruit en même temps (incendie, dégât des eaux…)

20.1 Cas particulier du stockage persistant de Tails

Lorsqu'on utilise Tails, il existe une méthode pour sauvegarder l'intégralité du volume persistant d'une clé Tails.

Pour ce faire, on va suivre la documentation officielle de Tails, qui est disponible à partir de n'importe quelle clé USB ou DVD Tails, même sans connexion à Internet. page 115

Démarrer Tails. Sur le bureau, cliquer sur l'icône *Documentation de Tails*. Chercher la section *Premiers pas avec Tails* et dans la section *Stockage persistant chiffré* cliquer sur *Créer une sauvegarde de votre stockage persistant* et suivre cette page de documentation.

20.2 Avec le gestionnaire de fichiers et un stockage chiffré

Réaliser des sauvegardes est avant tout une question de rigueur et de discipline. Dans les cas simples, on peut se passer de logiciels spécialement prévus pour réaliser des sauvegardes, et se contenter simplement d'effectuer des copies vers un support de stockage chiffré avec le gestionnaire de fichiers.

20.2.1 Effectuer les sauvegardes

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : pour la première fois, le temps de chiffrer le support de stockage et de décider des fichiers à sauvegarder ; et ensuite cela dépend de la quantité de données à sauvegarder.

page 145 Le chiffrement de nos sauvegardes sera assuré par le chiffrement du support de stockage externe, clé USB ou disque dur.

Pour effectuer les copies avec régularité et sans trop y passer de temps, il est recommandé :

- d'avoir quelque part une liste des fichiers et dossiers à sauvegarder ;
- de se fabriquer un petit calendrier des jours ou semaines où l'on fera ses sauvegardes, avec des cases que l'on cochera après les avoir faites.

Une bonne pratique consiste à créer un dossier (sur le support de stockage des sauvegardes) avec la date de la sauvegarde et de copier les données dedans. Cela permet de garder facilement plusieurs sauvegardes si on le souhaite, et de supprimer tout aussi facilement les sauvegardes précédentes.

Précision

Lors du choix des fichiers à sauvegarder, penser aux données de certains programmes (comme celles du logiciel de messagerie électronique Thunderbird[1]) qui sont parfois dans des dossiers cachés. Dans *Fichiers*, ils peuvent être affichés en cliquant sur ☰ puis *Afficher les fichiers cachés*.

20.2.2 Restaurer une sauvegarde

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : selon la quantité de données à restaurer.

En cas de perte des données originales, la restauration se fait aussi simplement que la sauvegarde : en effectuant des copies dans l'autre sens.

20.2.3 S'assurer que les sauvegardes sont toujours lisibles

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Environ cinq minutes, puis attendre que la vérification se fasse.

Si l'on a effectué nos sauvegardes sur un support de stockage externe, il faut commencer par le brancher sur l'ordinateur.

La méthode évidente pour s'assurer que les sauvegardes sont toujours lisibles est sans doute de simuler une restauration. Procéder ainsi a un inconvénient… de taille : il faut avoir assez d'espace libre à notre disposition pour recopier l'ensemble des données sauvegardées vers un dossier temporaire que l'on supprime ensuite.

page 97 Voici une autre méthode, peut-être moins facile à mettre en œuvre, mais qui n'a pas cette contrainte. Elle nécessite d'utiliser un Terminal.

1. Vincent, Goofy *et al.*, 2021, *Profils – là où Thunderbird conserve vos messages et autres données utilisateur* [https://support.mozilla.org/fr/kb/profils-thunderbird-conserve-donnees-utilisateur].

Commencer la commande en tapant (**sans** faire *Entrée*, ↵ ou return) :

```
tar -cPf /dev/null
```

Ensuite, ajouter un espace et indiquer le dossier contenant les sauvegardes, en attrapant l'icône du dossier avec la souris et en l'amenant sur la fenêtre du terminal. Après avoir relâché le bouton, ce qui est affiché doit ressembler à :

```
tar -cPf /dev/null '/media/externe/sauvegardes'
```

La lecture se lance dès qu'on a appuyé sur *Entrée* (↵ ou return). La ligne suivante devrait rester vide jusqu'à la fin de l'opération.

Si des messages d'erreur sont apparus dans l'intervalle, tels que « *Erreur d'entrée/-sortie* » ou « *Input/output error* », cela signifie que la sauvegarde est corrompue. Il faut alors faire une nouvelle sauvegarde sur un nouveau support (clé USB ou disque dur), la vérifier, puis se débarasser du support de stockage défectueux.

Après de la patience et le retour du `$` de l'invite de commande, on peut fermer le terminal.

Note : ces deux méthodes partagent le défaut de ne pas vérifier l'intégrité des données. page 53 Mettre en place un mécanisme pour le faire est difficile sans recourir à des logiciels de sauvegarde plus complexes.

20.3 En utilisant Déjà Dup

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Cinq minutes pour installer le logiciel.

On peut également préférer utiliser un logiciel spécialisé dans la réalisation des sauvegardes. L'un d'entre eux, nommé « Déjà Dup », a comme avantage d'être facile à utiliser et de réaliser des sauvegardes chiffrées. Ces sauvegardes sont également « incrémentales », c'est-à-dire que seuls les nouveaux fichiers et les modifications sont sauvegardées, les fichiers inchangés depuis la sauvegarde précédente ne sont pas copiés une nouvelle fois ; aussi il est possible d'accéder aux fichiers tels qu'ils étaient à chacune des sauvegardes.

Ce qui le rend aussi simple peut être une limite : quand on configure le logiciel, on choisit les dossiers à sauvegarder et le support sur lequel on veut les conserver. Mais on ne peut pas avoir plusieurs configurations qui permettraient de sauvegarder certains dossiers sur un disque dur avec une phrase de chiffrement et d'autres données sur un serveur, par exemple, avec une autre phrase de passe. Déjà Dup est donc idéal pour sauvegarder le contenu de son dossier personnel de manière régulière, mais pas beaucoup plus.

Par ailleurs, il n'est pas livré avec l'environnement par défaut, il est donc nécessaire d'installer le logiciel (voir page 134) *Sauvegardes Déjà Dup* pour pouvoir s'en servir.

20.3.1 Effectuer une sauvegarde

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quinze minutes environ pour la configuration, de quelques minutes à plusieurs heures pour la sauvegarde, selon la taille de ce qu'on veut copier.

Ouvrir *Sauvegardes* à partir de la vue d'ensemble des Activités : taper sur la touche ⊞ (⌘ sur un Mac), puis taper `sauv` et cliquer sur *Sauvegardes*.

Au premier lancement, deux boutons nous accueillent, l'un intitulé *Créer ma première sauvegarde*, l'autre pour *Restaurer à partir d'une précédente sauvegarde*. Cliquer sur le premier bouton pour définir ce que l'on veut sauvegarder et à quel endroit. Une fenêtre *Sauvegarder* apparaît qui va nous présenter plusieurs étapes :

1. Laisser le *Dossier à sauvegarder* défini à *Dossier personnel* avec le nom du compte, ce qui est suffisant dans la plupart des cas. Ajouter les dossiers à ignorer contenant des fichiers souvent volumineux mais plus faciles à retrouver, comme *Vidéos* ou *Musique*, dans *Dossiers à ignorer*. Choisir alors *Suivant*.
2. Dans *Emplacement de stockage* choisir l'emplacement de la sauvegarde. Pour stocker cette sauvegarde sur un disque externe, brancher le disque en question à l'ordinateur, puis le sélectionner dans la liste *Emplacement de stockage*. Choisir un nom pour le dossier de sauvegarde dans *Dossier*. Choisir alors *Suivant*.
3. Le choix *Protégez la sauvegarde par un mot de passe* est sélectionné par défaut : on renseigne alors une phrase de passe (voir page 103) dans *Mot de passe de chiffrement* pour chiffrer [2] notre nouvelle sauvegarde. Attention, le chiffrement ne porte que sur le contenu même des fichiers à sauvegarder : Déjà Dup ne chiffre pas le nom des fichiers et des répertoires sauvegardés. D'autre part, la phrase de passe ne peut plus être modifiée une fois définie. Un clic sur *Suivant* démarre alors la sauvegarde.

Une fois la sauvegarde terminée, la fenêtre *Sauvegarder* se ferme pour laisser place à la *Vue d'ensemble* de *Sauvegardes*. On y voit un message de notification sur la date de la dernière sauvegarde effectuée et la prochaine sauvegarde planifiée.

On peut activer l'automatisation de la sauvegarde *via* le bouton *Sauvegarder automatiquement*, qui passe en bleu si activé.

Par défaut, l'automatisation est hebdomadaire et la durée de rétention des sauvegardes est permanente.

On peut modifier tous ces paramètres *via* les *Préférences*, accessibles depuis le menu ☰ :

- L'emplacement de la sauvegarde est modifiable depuis l'onglet *General*.
- Le temps de rétention des sauvegardes peut être limité à trois mois, six mois, un an ou indéfiniment depuis l'onglet *General*.
- L'automatisation de la sauvegarde est activable depuis l'onglet *General* et on peut choisir la *Fréquence des sauvegardes automatiques* entre *Tous les jours* et *Toutes les semaines*.
- Les *Dossiers à sauvegarder* sont listés dans l'onglet *Folders* : le bouton ✚ permet d'ajouter un dossier supplémentaire à sauvegarder ; le bouton ━ permet de retirer le dossier correspondant de la sauvegarde.
- Les *Dossiers à ignorer* sont également listés dans l'onglet *Folders* et sont ajoutés et supprimés de la même manière.

2. Si le support externe est chiffré, on peut éventuellement décider de ne pas chiffrer les fichiers sauvegardés. Cela fait une phrase de passe de moins à inventer et à retenir. On perd néanmoins la possibilité de compartimenter les accès, au cas où le support externe servirait à d'autres choses que les sauvegardes.

Lorsque la planification des sauvegardes est activée et que le temps indiqué depuis la précédente sauvegarde est écoulé, Déjà Dup affiche un message de notification pour nous signifier que la sauvegarde planifiée est retardée et qu'elle débutera dès que le support externe sera de nouveau branché sur l'ordinateur. Et dès que ce sera le cas, une fenêtre s'ouvrira automatiquement pour demander de saisir la *phrase de passe* nécessaire pour mettre à jour la sauvegarde.

20.3.2 Restaurer une sauvegarde

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Cinq minutes pour configurer, de quelques minutes à plusieurs heures pour la restauration, selon la taille de notre sauvegarde.

Ouvrir *Sauvegardes* à partir de la vue d'ensemble des Activités : appuyer sur la touche (⌘ sur un Mac), puis taper `sauv` et cliquer sur *Sauvegardes*.

Connecter le disque contenant les sauvegardes, et l'ouvrir à partir de *Fichiers* s'il est chiffré.

L'opération de restauration démarre en cliquant sur le bouton *Restaurer*.

Si c'est la première fois qu'on utilise *Sauvegardes* (par exemple pour restaurer son dossier personnel après la perte d'un disque dur), il nous demande d'indiquer le dossier où ont été effectuées les sauvegardes. Sinon, il utilise les paramètres de sauvegarde déjà configurés.

Après un court délai, *Sauvegardes* affiche la liste des fichiers et répertoires de la dernière sauvegarde, ainsi que sa date. Une autre date de sauvegarde peut être choisie depuis la liste déroulante *Date*. Le bouton *Restaurer* est utilisable dès la sélection de tout ou partie des répertoires et fichiers que l'on souhaite récupérer.

Il faut ensuite indiquer le dossier où seront écrits les fichiers issus de la sauvegarde. On peut soit *Restaurer les fichiers vers leurs emplacements d'origine* (ce qui remplace éventuellement des fichiers par leur ancienne version se trouvant dans la sauvegarde), soit *Restaurer vers un dossier spécifique* à préciser.

Après avoir cliqué sur *Restaurer*, l'écriture des fichiers en provenance de la sauvegarde commence pour de bon, après avoir demandé la phrase de passe si la sauvegarde était chiffrée. Si tout se passe bien, la fenêtre affiche *Vos fichiers ont été restaurés avec succès.*

20.3.3 S'assurer que les sauvegardes sont toujours lisibles

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : De quelques minutes à plusieurs heures, selon la taille de nos sauvegardes.

Le fonctionnement incrémental de Déjà Dup assure superficiellement que les sauvegardes précédentes soient lisibles. Néanmoins cela ne constitue pas une garantie.

Malheureusement, la meilleure méthode actuellement disponible avec Déjà Dup pour s'assurer que l'on peut restaurer ses sauvegardes est… de faire une restauration vers un dossier temporaire que l'on effacera après. C'est loin d'être pratique, et il faut avoir accès à un disque dur chiffré suffisamment grand.

On peut toutefois s'assurer que les fichiers contenant les sauvegardes restent lisibles en utilisant les mêmes méthodes que celles décrites précédemment. page 152

Chapitre 21

Partager un secret

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Une heure environ.

Parfois, on souhaite être plusieurs à partager un secret, sans pour autant que chaque personne ne dispose de la totalité du secret.

Cela tombe bien, plusieurs techniques cryptographiques ont été inventées pour cela. Elles permettent toutes, avec des calculs mathématiques un peu différents, de découper un secret en plusieurs morceaux, que l'on pourra reconstituer en en réunissant quelques-uns [1].

21.1 Partager une phrase de passe

L'usage le plus pratique est de partager comme secret la phrase de passe d'un support chiffré. page 145

Cette étape doit idéalement être faite à partir d'un système *live* afin de ne pas laisser des traces du secret que l'on va partager. page 113

21.1.1 Installer le paquet nécessaire

Pour réaliser le partage du secret, on utilisera le programme `ssss-split`. On trouve ce programme parmi ceux fournis par le système *live* Tails. Cependant, pour en disposer sur une Debian chiffrée, il est nécessaire d'installer le paquet Debian *ssss*. page 135

Les outils contenus dans le paquet *ssss* sont à utiliser en ligne de commande. Toutes les opérations devront donc être effectuées dans un Terminal, sans les pouvoirs d'administration. page 97

21.1.2 Générer une phrase de passe aléatoire

Dans notre cas, personne ne doit pouvoir, ni se souvenir, ni deviner la phrase de passe qui sera utilisée pour le chiffrement. On va donc générer une phrase de passe complètement aléatoire en tapant la commande :

```
head -c 32 /dev/random | base64
```

L'ordinateur va répondre quelque chose comme :

```
7rZwOOu+8v1stea98OuyU1efwNzHaKX9CuZ/TKObRWY=
```

1. Pour plus de détails, voir l'article de Wikipédia sur les secrets répartis [https://fr.wikipedia.org/wiki/Secret_r%C3%A9parti].

Si l'on désire faire varier la longueur de la phrase de passe, il suffira de remplacer `32` par le nombre de caractères désirés. Sélectionner cette ligne à l'aide de la souris et la copier dans le presse-papiers, en faisant un clic-droit puis en cliquant sur *Copier*.

21.1.3 Découper le secret

Avant de découper le secret, il faut décider en combien de morceaux il sera découpé, et combien de morceaux seront nécessaires pour le reconstituer.

Ensuite, toujours à l'aide de notre terminal, il faut utiliser `ssss-split` de la façon suivante :

```
ssss-split -t NOMBRE-DE-MORCEAUX-NECESSAIRES -n
↪     NOMBRE-DE-MORCEAUX-TOTAL
```

Le `NOMBRE-DE-MORCEAUX-NECESSAIRES` est le nombre de morceaux qu'il sera nécessaire de réunir pour retrouver la phrase de passe de départ. Le `NOMBRE-DE-MORCEAUX-TOTAL` correspond au nombre de morceaux en lesquels la phrase de passe sera découpée. Le message `WARNING: couldn't get memory lock` peut être ignoré sans problème si on utilise bien un système *live*.

Lorsqu'il demande le secret, on peut coller le contenu du presse-papiers, en faisant clic-droit puis en cliquant sur *Coller*. Appuyer ensuite sur la touche *Entrée* (↵ ou return) pour valider la commande.

Chaque personne partageant le secret devra conserver l'une des lignes affichées ensuite. Et cela dans leur **intégralité**, en prenant également bien en note le premier chiffre suivi du tiret.

Voici un exemple avec la clé aléatoire générée précédemment, partagée entre six personnes et qui nécessitera que trois d'entre elles se réunissent pour la retrouver :

```
$ ssss-split -t 3 -n 6
Generating shares using a (3,6) scheme with dynamic security level.
Enter the secret, at most 128 ASCII characters: Using a 352 bit
↪     security level.
1-b8d576a1a8091760b18f125e12bb6f2b1f2dd9d93f7072ec69b129b27bb8e97536
↪     ea85c7f6dcee7b4399ea49
2-af83f0af05fc207e3b466caef30ec4d39c060800371feab93594350b7699a8db9
↪     594bfc71ed9cd2bf314b738
3-4718cb58873dab22d24e526931b061a6ac331613d8fe79b2172213fa767caa57d
↪     29a6243ec0e6cf77b6cbb64
4-143a1efcde7f4f5658415a150fcac6da04f697ebfeb9427b59dca57b50ec755510
↪     b0e57ccc594e6b1a1eeb04
5-fca1250b5cbec40ab14964d2cd7463af34c389f81158d1707b6a838a500977d957
↪     be38f83e8eefb79266e74a
6-ebf7a305f14bf3143b801a222cc1c857b7e85821193749252 74f9f335d283677f4
↪     c002f8d68bcce722ebba1f
```

21.1.4 Créer le support chiffré

page 145

On pourra ensuite créer le support chiffré. Au moment d'indiquer la phrase de passe, on pourra copier le contenu du presse-papiers, comme précédemment, ou alors la retranscrire en l'ayant sous les yeux.

21.2 Reconstituer la phrase de passe

Afin de reconstituer la phrase de passe (le secret), il est nécessaire de disposer d'au moins autant de morceaux que le nombre minimal décidé lors du découpage (trois dans notre exemple).

page 113

Cette étape doit aussi idéalement être faite à partir d'un système *live* afin de ne pas laisser de traces du secret partagé.

21.2.1 Installer les paquets nécessaires

Comme précédemment, si le programme n'est pas disponible sur le système on a besoin d'installer le paquet *ssss* et d'ouvrir un terminal.

page 135

21.2.2 Recombiner le secret

Afin de recombiner le secret, on utilisera le programme `ssss-combine`. Il est nécessaire de lui indiquer le nombre de morceaux qu'on a à notre disposition :

```
ssss-combine -t NOMBRE-DE-MORCEAUX-A-DISPOSITION
```

Le programme demande ensuite de saisir les morceaux à notre disposition. Il faut taper *Entrée* (↵ ou return) après avoir écrit chacun d'entre eux. Si tout se passe bien, le programme affichera ensuite la phrase de passe complète.

Pour reprendre l'exemple précédent, cela donne :

```
$ ssss-combine -t 3
Enter 3 shares separated by newlines:
Share [1/3]: 4-143a1efcde7f4f5658415a150fcac6da04f697ebfeb9427b59dc
↪    a57b50ec755510b0e57ccc594e6b1a1eeb04
Share [2/3]: 2-af83f0af05fc207e3b466caef30ec4d39c060800371feab9359
↪    4350b7699a8db9594bfc71ed9cd2bf314b738
Share [3/3]: 6-ebf7a305f14bf3143b801a222cc1c857b7e858211937
↪    4925274f9f335d283677f4c002f8d68bcce722ebba1f
Resulting secret: 7rZwOOu+8v1stea98OuyU1efwNzHaKX9CuZ/TKObRWY=
```

⚠ **Attention** : si un des morceaux a mal été tapé, l'erreur qui s'affiche n'est pas forcément très explicite :

```
$ ssss-combine -t 3
Enter 3 shares separated by newlines:
Share [1/3]: 4-143a1efcde7f4f5658415a150fcac6da04f697ebfeb9427b59dc
↪    a57b50ec755510b0e57ccc594e6b1a1eeb04
Share [2/3]: 2-af83f0af05fc207e3b466caef30ec4d39c060800371feab9359
↪    4350b7699a8db9594bfc71ed9cd2bf31ab738
Share [3/3]: 6-ebf7a305f14bf3143b801a222cc1c857b7e858211937
↪    4925274f9f335d283677f4c002f8d68bcce722ebba1f
Resulting secret: .....L.fm.....6 _....v..w.a....[....zS.....
WARNING: binary data detected, use -x mode instead.
```

21.2.3 Ouvrir le support chiffré

Une fois la phrase de passe obtenue, on peut utiliser un copier/coller afin de déverrouiller le support chiffré, ou alors la retranscrire en l'ayant sous les yeux.

Chapitre 22

Utiliser les sommes de contrôle

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Cinq à dix minutes.

Dans la première partie, nous avons évoqué les *sommes de contrôle* : des « nombres » qui permettent de vérifier l'intégrité d'un fichier (ou de toute autre donnée). Le principe est qu'il est quasiment impossible d'avoir une somme de contrôle identique pour deux fichiers différents. Si, dans une lettre, Ana dit à Bea que sur son site cette dernière peut télécharger un programme qui a pour somme de contrôle SHA256 `171a0233a4112858db23621dd5ffa31d269cbdb4e75bc206ada58ddab444651f` et que le fichier que Bea télécharge a la même somme de contrôle, alors il est quasiment certain que personne n'a falsifié le programme en chemin. Elle peut donc exécuter ce programme sans trop de craintes.

page 53

Il existe plusieurs algorithmes — ou *fonctions de hachage* — pour faire des sommes de contrôle. Parmi eux :

- MD5 n'est plus sûr de nos jours et est à proscrire ;
- SHA-1 était très utilisé jusqu'en 2017, année où a eu lieu une attaque effective sur cet algorithme. Il est de moins en moins utilisé depuis. Il faut l'abandonner ;
- Ceux de la famille SHA-2 (SHA-224, SHA-256, SHA-384 et SHA-512) sont toujours sûrs en 2022. Nous allons utiliser ici SHA-256, mais la méthode fonctionne aussi avec les autres algorithmes de cette famille.

22.1 Obtenir la somme de contrôle d'un fichier

Que l'on souhaite vérifier l'intégrité d'un fichier, ou permettre à nos destinataires de le faire, il faut calculer la somme de contrôle de ce fichier.

page 53

Il est possible d'utiliser un outil graphique tout aussi bien qu'un terminal pour effectuer de tels calculs. Nous n'allons cependant pas détailler l'utilisation d'un terminal ici.

22.1.1 Installer les logiciels nécessaires

S'il n'est pas encore installé, installer le paquet `nautilus-gtkhash` (voir page 135), puis redémarrer l'ordinateur. Ce paquet est installé par défaut dans Tails.

22.1.2 Calculer la somme de contrôle

Ouvrir *Fichiers* à partir de la vue d'ensemble des Activités : appuyer sur la touche ⊞ (⌘ sur un Mac), puis taper `fich` et cliquer sur *Fichiers*.

Sélectionner le fichier pour lequel on veut obtenir des sommes de contrôle, puis effectuer un clic-droit dessus. Dans le menu contextuel qui apparaît, choisir *Propriétés*, puis aller dans l'onglet *Empreintes*.

De nombreuses *Fonctions de hachage* sont proposées, avec trois sélections par défaut : MD5, SHA1, SHA256. Si une autre somme de contrôle que celles-ci est nécessaire, cocher la case correspondante. Cliquer sur *Hachage*. Les sommes de contrôle apparaissent alors dans la colonne *Empreinte*.

22.2 Vérifier l'intégrité d'un fichier

Il faut obtenir la somme de contrôle du fichier original par un moyen sûr, autre que celui par lequel on reçoit le fichier. Par exemple, si l'on télécharge le fichier, on peut recevoir sa somme de contrôle dans une lettre ou par téléphone — le mieux étant bien sûr de vive voix.

De la même manière, pour permettre à d'autres personnes de vérifier l'intégrité d'un fichier qu'on leur envoie, on leur fait parvenir la somme de contrôle selon les mêmes méthodes.

Enfin, grâce à la méthode expliquée plus haut, calculer la somme de contrôle de notre copie du fichier. Prendre garde à utiliser la même fonction de hachage que celle qui a été utilisée par notre correspondante. Si l'on utilise SHA1 et qu'elle utilise SHA256, on n'aura evidemment pas la même somme de contrôle. Si notre correspondante nous propose plusieurs sommes de contrôle, préférer l'algorithme le plus dur à casser (voir page précédente), tel que nous l'avons mentionné au début de ce chapitre.

Vérifier que les deux sommes de contrôle sont identiques — c'est un peu long et fastidieux. C'est souvent plus simple à deux, ou en les collant l'une en-dessous de l'autre dans un fichier texte.

Chapitre 23

Installer et utiliser un système virtualisé

L'objectif de ces recettes est d'utiliser un système d'exploitation virtuel, c'est-à-dire faire fonctionner, sur un seul ordinateur, plusieurs systèmes d'exploitation, presque comme s'ils fonctionnaient sur des machines physiques distinctes. Le système virtuel (appelé *invité*) fonctionne à l'intérieur de notre système GNU/Linux (appelé *hôte*) : on appelle cela de la *virtualisation*. Cette technologie ainsi qu'une politique de sécurité l'utilisant sont décrites plus avant dans le cas d'usage expliquant comment travailler sur un document sensible sous Windows. page 82



Pour aller plus loin…

Il peut y avoir d'autres raisons d'utiliser un système virtualisé. Par exemple, il est possible de démarrer une clé Tails (voir page 113) dans un système virtuel afin de l'utiliser sans avoir à redémarrer l'ordinateur. Il est même possible d'installer Tails directement dans le *Gestionnaire de machines virtuelles*[1], de la même manière que d'autres systèmes d'exploitation. Il sera tout de même important de bien réfléchir et analyser les traces que l'on peut laisser dans le système hôte, dans le système invité ou dans les métadonnées des documents créés et partagés.

23.1 Installer le Gestionnaire de machines virtuelles



Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Un quart d'heure environ.

23.1.1 Principe

L'objectif de cette recette est d'installer le *Gestionnaire de machines virtuelles*[2], logiciel qui nous permettra de faire fonctionner un système Windows virtuel (ou tout autre système) à l'intérieur de notre système Debian GNU/Linux.

1. On pourra trouver une documentation pour cela sur le site officiel de Tails [https://tails.boum.org/install/vm/index.fr.html].

2. D'anciennes éditions de ce *Guide* conseillaient d'utiliser le logiciel VirtualBox. Seulement, celui-ci n'est plus disponible dans Debian. Si l'on utilisait cet outil auparavant, il faudra soit réinstaller notre machine virtuelle, soit la migrer de VirtualBox au Gestionnaire de machines virtuelles. Cette procédure n'est pas documentée dans ce *Guide*, mais on pourra toujours se lancer dans l'aventure en suivant des instructions disponibles sur le web : Malte Gerken, 2017, *Migrate a VM from VirtualBox to libvirt* [https://maltegerken.de/blog/2017/01/migrate-a-vm-from-virtualbox-to-libvirt/] (en anglais).

23.1.2 Installer et lancer le Gestionnaire de machines virtuelles

page 134

L'étape suivante est donc d'installer le logiciel *Gestionnaire de machines virtuelles*.

Puis, pour lancer le *Gestionnaire de machines virtuelles*, ouvrir la vue d'ensemble des Activités en appuyant sur la touche [⊞] ([⌘] sur un Mac), puis taper `virt` et cliquer sur *Gestionnaire de machines virtuelles*. Notre mot de passe d'administration nous est alors demandé, c'est normal.

23.2 Activer la virtualisation matérielle

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Un quart d'heure environ.

23.2.1 Principe

La très grande majorité des processeurs actuels intègrent un support matériel spécifique pour la virtualisation, appelé *virtualisation matérielle*, afin que les systèmes virtualisés fonctionnent aussi bien que s'ils s'exécutaient sur une véritable machine physique. Cependant, cette fonctionnalité est parfois désactivée par défaut sur certains ordinateurs, ce qui rend alors les machines virtuelles extrêmement lentes.

23.2.2 Tester si la virtualisation matérielle est activée

Afin de voir si la virtualisation matérielle est activée sur notre ordinateur, on peut utiliser un petit logiciel fourni avec le Gestionnaire de machines virtuelles.

page 97

Pour cela, il faut utiliser un terminal et taper la commande suivante :

```
virt-host-validate
```

La commande affiche alors plusieurs lignes de diagnostic. Il faut chercher celle qui s'intitule *QEMU : Vérification for hardware virtualization* (c'est la première, normalement) :

- S'il est affiché *PASS* (en vert) sur cette ligne, c'est que la virtualisation matérielle est bien activée. On peut donc passer directement à la partie suivante de ce chapitre.
- Sinon, s'il est affiché *FAIL* (en rouge) sur cette ligne, cela signifie que la virtualisation matérielle est désactivée. On va donc poursuivre la lecture de cette partie afin de l'activer.

page ci-contre

23.2.3 Activer la virtualisation matérielle dans le microprogramme

Afin d'activer cette fonctionnalité, il faut modifier la configuration du microprogramme de l'ordinateur :

page 108

- Tout d'abord, redémarrer l'ordinateur puis entrer dans l'interface de configuration du microprogramme.

page 109

- Si l'on n'est pas familière avec l'interface de configuration du microprogramme, on pourra se référer à la description de celle-ci dans un chapitre précédent.
- Une fois dans le microprogramme, il faut chercher quelque chose qui ressemble à `Virtualization Technology`, `VT-x` ou `AMD-V` (qui sont les noms des technologies de virtualisation matérielle dans les processeurs Intel et AMD, respectivement). En général, on va trouver ces options dans les sous-menus `Advanced` ou `System Configuration`. Cette option est probablement marquée comme `Disabled` (« désactivée »).

- À l'aide des flèches du clavier, sélectionner l'option concernée, puis la mettre à `Enabled` (« activée »), soit en appuyant sur la touche *Entrée* (↵ ou return) puis en sélectionnant la bonne valeur (si l'interface du microprogramme indique quelque chose comme `Enter: Select` dans sa zone d'aide), soit en utilisant les touches + et − (si l'interface indique `+/-: Value`).
- Une fois la bonne valeur sélectionnée, enregistrer le changement et quitter l'interface de configuration du microprogramme. page 111

23.2.4 Vérifier que la virtualisation matérielle est bien activée

L'ordinateur redémarre alors : on pourra à nouveau faire le test avec la commande `virt-host-validate` afin de nous assurer que la virtualisation matérielle est désormais bien activée.

23.3 Installer un Windows virtualisé

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Vingt minutes environ, plus le temps d'installer Windows (de trente minutes à plus d'une heure).

Avant toute chose, télécharger une image ISO de la version de Windows souhaitée. On peut par exemple trouver les images ISO officielles des versions récentes de Windows sur le site de Microsoft [3].

23.3.1 Créer une nouvelle machine virtuelle

Pour lancer le Gestionnaire de machines virtuelles, ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `virt` et cliquer sur *Gestionnaire de machines virtuelles*.

Le programme démarre, il faut alors donner le mot de passe demandé et s'authentifier. Cliquer sur le menu *Fichier* puis *Nouvelle machine virtuelle* et suivre les cinq étapes de l'assistant. À la fin de chaque étape le bouton *Suivant* permet de passer à l'étape suivante.

- Étape 1 : sélectionner *Média d'installation local (image ISO ou CD-ROM).*
- Étape 2 : pour *Choisir un média d'installation (ISO ou CDROM)* cliquer sur *Parcourir…*, une fenêtre s'ouvre. Cliquer en bas sur *Parcourir en local* puis sélectionner l'image ISO qui a été préalablement téléchargée. Cliquer sur *Ouvrir*. Dans le champ *Choisissez le système d'exploitation que vous installez* : si le système et sa version sont mal reconnus, décocher *Détecter automatiquement depuis la source/média d'installation* pour le choisir manuellement, par exemple *Microsoft Windows 10*.
- Étape 3 : indiquer la taille de *Mémoire* et le nombre de *CPU* dédiés à la machine virtuelle. Voici les minimums recommandés pour les dernières versions de Windows :

Version	Mémoire (RAM)	CPU
Windows 7	1024 MiB	1
Windows 8	2048 MiB	1
Windows 10	2048 MiB	1
Windows 11	4096 MiB	2

3. https://www.microsoft.com/fr-fr/software-download

- Étape 4 : Choisir la taille de l'image disque allouée à la machine virtuelle. Sachant qu'on veut accueillir tout un Windows, elle doit être conséquente : 20 Go est un minimum.
- Étape 5 : Indiquer un *Nom* pour la machine virtuelle puis sélectionner *Personnaliser la configuration avant l'installation*.

Enfin cliquer sur *Terminer*.

Si un message *Le réseau virtuel n'est pas actif* s'affiche, cliquer sur *Non* : de toute façon, nous ne l'utiliserons pas pour cette machine virtuelle.

Dans la colonne de gauche de la fenêtre qui s'ouvre, sélectionner le matériel *NIC* (pour *Network Interface Card*), qui représente la carte réseau de la machine virtuelle, puis cliquer sur *Enlever* en bas. Dans la fenêtre de confirmation, choisir *Oui*. La machine virtuelle est désormais isolée du réseau.

Ajouter ensuite un canal nécessaire au partage de dossier entre le système hôte et le système invité. Pour ce faire, cliquer sur le bouton en bas à gauche *Ajouter un matériel*. Dans la fenêtre qui s'affiche, cliquer sur *Canal* dans la liste de gauche. Dans la liste déroulante *Nom*, sélectionner *org.spice-space.webdav.0*, puis cliquer sur le bouton *Terminer*.

Cliquer sur *Commencer l'installation* pour lancer l'installation de Windows.

23.3.2 Installer *Windows* dans la machine virtuelle

Le système virtuel démarre grâce au fichier ISO qu'on lui a indiqué et commence l'installation. On ne rentrera pas dans les détails du processus, qui dépend de notre version de Windows, mais il faut préciser :

- Pour voir l'installeur en entier, choisir le menu *Afficher* → *Mettre à l'échelle l'affichage* → *Toujours*.
- Ne pas mettre d'informations personnelles lorsque le *Nom* et l'*Organisation* sont demandés. Mettre « user », par exemple.
- Pareil si l'on souhaite entrer un numéro de série de Windows, un lien pourrait être fait si celui-ci a été attribué officiellement.
- Lors de la configuration du réseau, un message d'erreur peut être affiché. C'est bon signe : nous avons désactivé le réseau de la machine virtuelle.

Une fois l'installation terminée, éteindre le Windows virtuel en cliquant sur le menu *Machine virtuelle* → *Éteindre* → *Éteindre*. Si la machine ne s'éteint pas, il est aussi possible de faire *Forcer l'extinction* dans le même menu.

Depuis la fenêtre de la machine virtuelle, cliquer sur le menu *Afficher* → *Détails*. Dans la liste de gauche, choisir *SATA CDROM 1* ou *IDE CD-ROM 1* (selon votre ordinateur), puis effacer le contenu du champ *Repertoire source* et cliquer sur *Appliquer*.

23.3.3 Les outils invités pour le Gestionnaire de machines virtuelles

Des pilotes spécifiques permettent d'améliorer l'interaction entre le Gestionnaire de machines virtuelles et le système Windows invité grâce à une technologie appelée SPICE : il s'agit des outils invités et du service de partage de dossiers. Ces pilotes permettent par exemple de faire un copier-coller ou de transférer des fichiers entre le système hôte et le système virtuel invité. Pour cela, deux petits programmes d'installation vont être utilisés.

Depuis le système hôte, télécharger l'installeur Windows des outils invités pour SPICE[4].

page 345 Pour vérifier l'authenticité du fichier téléchargé, récupérer sa signature[5] et importer

la clé PGP [6] utilisée pour vérifier cette dernière. L'empreinte de la clé [7] observée par les personnes écrivant ces lignes, en admettant que l'on a un exemplaire original du guide entre les mains, est : page 343

```
94A9 F756 61F7 7A61 6864 9B23 A9D8 C214 29AC 6C82
```

Aller ensuite sur la page web de l'installeur du service WebDAV pour SPICE [8]. Cliquer sur le lien de téléchargement de la dernière version correspondant à l'architecture de notre machine virtuelle. Le nom contient *x86* pour un Windows 32 bits ou *-64* pour un Windows 64 bits. S'assurer qu'il existe également un fichier signature [9] pour le fichier de cette version. Vérifier l'authenticité du fichier. Si le fichier correspondant au fichier téléchargé est un *.sha256*, vérifiez l'authenticité en utilisant la somme de contrôle. Téléchargez la clé PGP qui se trouve sur ce lien [10] avec le navigateur web : dans le menu déroulant en haut à droite ☰, cliquer sur *Enregistrer sous...* et l'enregistrer en donnant un nom suivi de l'extension *.asc*. Importer cette clé pour vérifier l'authenticité du fichier. L'empreinte de la clé [11] observée par les personnes écrivant ces lignes, en admettant que l'on a un exemplaire original du guide entre les mains, est : page 345 page 161 page 343

```
206D 3B35 2F56 6F3B 0E65 72E9 97D9 123D E37A 484F
```

Suivre ensuite la méthode pour installer `spice-guest-tools` dans un système virtualisé. page 169

Faire de même avec `spice-webdavd`. L'installation de `spice-webdavd` peut paraitre surprenante, il n'y a pas de message qui dit que l'installation est terminée. Ne pas s'en inquiéter. page 169

Maintenant, il est possible de copier-coller du texte entre la machine hôte et la machine virtuelle. Il aussi possible de copier-coller des fichiers mais seulement de la machine hôte vers la machine virtuelle Windows. Si ce copier-coller ne fonctionne pas, essayer de glisser le document d'une fenetre à l'autre (le fichier glissé arrive sur le bureau de la machine virtuelle Windows). Une autre fonctionalité est de modifier l'affichage de la machine virtuelle en fonction de la taille de la fenêtre qui accueille Windows. Pour cela, cliquer sur le menu *Afficher* → *Mettre à l'échelle l'affichage* et sélectionner *Ajustement automatique de la machine virtuelle à la fenêtre.*

23.3.4 Sauvegarde du Windows virtuel fraîchement installé

L'installation du Windows virtuel est maintenant terminée, mais ce n'est pas fini ! Avant de travailler sur des documents sensibles à l'intérieur de la machine virtuelle, il est important d'en faire un instantané, c'est-à-dire de sauvegarder l'état de ce *Windows* qui est considéré comme « propre » puisqu'il est tout fraîchement installé.

---

4. https://www.spice-space.org/download/windows/spice-guest-tools/spice-guest-tools-latest.exe
5. https://www.spice-space.org/download/windows/spice-guest-tools/spice-guest-tools-latest.exe.sign
6. https://keys.openpgp.org/vks/v1/by-fingerprint/94A9F75661F77A6168649B23A9D8C21429AC6C82
7. L'empreinte de la clé PGP importée peut être vérifiée depuis le logiciel *Kleopatra* [page 345].
8. https://www.spice-space.org/download/windows/spice-webdavd/
9. C'est-à-dire un fichier de même nom avec une extension *.sig*.
10. https://keyserver.ubuntu.com/pks/lookup?op=get&search=0x206d3b352f566f3b0e6572e997d9123de37a484f
11. L'empreinte de la clé PGP importée peut être vérifiée depuis le logiciel *Kleopatra* [page 345].

23.4 Prendre un instantané d'une machine virtuelle

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Cinq minutes.

page 82

Pour suivre la méthode permettant de travailler sur un document sensible sous Windows, on peut avoir besoin de sauvegarder l'état d'une machine virtuelle qu'on considère comme « propre ». Pour cela, on va utiliser la gestion des instantanés des machines virtuelles, appelés aussi *Snapshot* en anglais.

Pour lancer le Gestionnaire de machines virtuelles, ouvrir la vue d'ensemble des Activités en appuyant sur la touche [⊞] ([⌘] sur un Mac), puis taper `virt` et cliquer sur *Gestionnaire de machines virtuelles* et entrer le mot de passe. Sélectionner la machine virtuelle souhaitée et cliquer sur *Ouvrir*. Si elle est en cours de fonctionnement, l'éteindre en cliquant sur le menu *Machine virtuelle* → *Éteindre* → *Éteindre*.

Cliquer sur *Afficher* → *Instantanés*. Dans la liste de gauche, cliquer sur le bouton ✚ en bas. Dans la fenêtre qui apparaît, indiquer le *Nom* de l'instantané en évitant l'usage d'espaces et de caractères spéciaux, par exemple « Windows_propre ». Ajouter éventuellement une *Description* puis cliquer sur *Terminer*.

23.5 Restaurer l'état d'une machine virtuelle à partir d'un instantané

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : selon la taille du disque.

cette page

L'objectif de cette recette est de restaurer l'état d'une machine virtuelle à partir d'un instantané créé précédemment. Ainsi, il sera possible de l'utiliser pour un nouveau projet, comme le recommande la méthode préconisée pour travailler sur un document sensible sous Windows.

page 82

23.5.1 Afficher les instantanés

Commençons donc par lancer le Gestionnaire de machines virtuelles, pour cela ouvrir la vue d'ensemble des Activités en appuyant sur la touche [⊞] ([⌘] sur un Mac), puis taper `virt` et cliquer sur *Gestionnaire de machines virtuelles* puis entrer le mot de passe. Sélectionner la machine virtuelle souhaitée et cliquer sur *Ouvrir*. Dans la nouvelle fenêtre, cliquer sur le menu *Afficher* et sélectionner *Instantanés*.

23.5.2 Choisir et restaurer un instantané

Sélectionner l'instantané souhaité à partir duquel restaurer l'état de la machine (par exemple « Windows_propre »). Cliquer sur le bouton ▶, en bas à gauche. Une nouvelle fenêtre apparaît, demandant si nous sommes sûrs de vouloir exécuter l'instantané sélectionné. Exécuter cet instantané aura pour conséquence que toutes les modifications effectuées dans la machine virtuelle depuis la création de cet instantané seront perdues. Si nous sommes sûres de notre choix, cliquer sur *Oui*, sinon, cliquer sur *Non*.

Le Gestionnaire de machines virtuelles va restaurer l'état de la machine virtuelle tel qu'il était au moment où l'instantané à été pris.

23.6 Installer un nouveau logiciel sur un système virtualisé

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Vingt minutes environ.

Pour installer des logiciels dans le système Windows virtualisé on peut utiliser une image de disque ISO du logiciel, c'est la méthode qui est expliqué ici. Il est aussi possible d'utiliser un CD ou un DVD. page 171

Il est conseillé de partir d'un « Windows propre », et donc de restaurer l'état d'une machine virtuelle considérée comme « propre » à partir d'un instantané. Cela permettra, à la fin de l'installation, de créer un nouvel instantané contenant le logiciel qui viendra d'être installé. page préc.

23.6.1 Télécharger et vérifier un logiciel

Si l'on ne l'a pas encore, commencer par trouver le logiciel, par exemple sur Internet. Il est préférable, dans la mesure du possible, de vérifier le fichier téléchargé. Le programme téléchargé est un installeur, un programme qui permet d'installer le logiciel. page 345

23.6.2 Créer une image ISO des programmes d'installation

Pour transférer un installeur de la machine hôte au Windows invité, il faut qu'il soit au format ISO. Si l'installeur est déjà au format ISO, passer diectement au paragraphe suivant. Sinon, on va créer une image de disque au format ISO contenant l'installeur avec le logiciel Brasero [12]. cette page

Pour lancer Brasero, ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `bra` et cliquer sur *Brasero*.

Choisir *Projet de données* dans la colonne de gauche. Cliquer sur l'icône ✚ et ajouter le fichier du programme-installeur précédemment téléchargé.

Dans la liste déroulante en bas de la fenêtre, choisir *Fichier image* puis cliquer sur *Graver…*. Choisir un nom de fichier et cliquer sur *Créer une image*. Une fois l'image créée, fermer Brasero.

23.6.3 Importer l'image ISO dans le système virtuel

Retourner dans le Gestionnaire de machines virtuelles pour partager l'image de disque ISO.

Commencer par lancer le Gestionnaire de machines virtuelles, pour cela ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `virt` et cliquer sur *Gestionnaire de machines virtuelles*. Enfin, entrer le mot de passe demandé.

Sélectionner la machine virtuelle Windows sur laquelle on souhaite installer le logiciel et cliquer sur *Ouvrir*. Dans la nouvelle fenêtre, afficher la vue détaillée de la machine virtuelle en cliquant sur le menu *Afficher* → *Détails*. Dans la liste des matériels à gauche, sélectionner *IDE CD-ROM 1* ou *SATA CDROM 1* selon les fonctionalités de votre ordinateur. Choisir ensuite *Emplacement de l'image ISO* ou *Répertoire souce* puis cliquer sur *Naviguer*. Dans la fenêtre qui s'affiche, choisir *Parcourir en local* et sélectionner l'image ISO et cliquer sur *Ouvrir*. Ensuite cliquer sur *Appliquer* en bas à droite.

12. Il est possible qu'il soit nécessaire d'installer *Brasero* [page 134].

23.6.4 Installer le logiciel sur la machine virtuelle

Faire *Afficher* → *Console* pour retourner à Windows. Si la fenêtre affiche *L'invité est à l'arrêt*, démarrer la machine virtuelle avec *Machine virtuelle* → *Démarrer*. Windows devrait détecter l'image ISO comme si elle était un CD/DVD. Si ce n'est pas le cas, on peut aller la chercher dans l'explorateur de fichier (aller dans *Ce PC* → *Lecteur de CD (D :)*). Si ça ne marche pas du premier coup, recommencer l'opération.

Pour faire l'installation proprement dite, double-cliquer sur le CD-ROM virtuel et double-cliquer sur le fichier permettant de lancer l'installation, son *Type* est une *Application*. Selon le type de logiciel installé, Windows peut demander s'il faut autoriser un programme inconnu (c'est-à-dire non vérifié par Microsoft). Si l'on a confiance en notre téléchargement de base, l'accepter. Accepter aussi toutes les autres demandes du programme d'installation en cliquant sur *Suivant*.

L'installation terminée, l'image ISO n'est plus utile. Retourner alors dans la vue détaillée de la machine virtuelle avec *Afficher* → *Détails*, sélectionner *IDE CD-ROM 1* ou *SATA CDROM 1* et effacer le contenu du champ *Emplacement de l'image ISO* ou *Répertoire source*, puis *Appliquer*.

page 168 Il est alors possible de prendre un instantané d'une machine virtuelle afin de conserver une version « propre » du système virtuel avec ce nouveau logiciel.

23.7 Partager une clé USB avec un système virtualisé

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Dix minutes environ.

Attention : il n'est pas toujours souhaitable que le système virtuel ait un accès direct à la clé USB ou un disque dur externe. En effet, en connectant une clé USB au système Windows, il y inscrira des données de manière automatique. Pour accéder aux données de la clés sans que le sytème virtuel n'y ait directement accès, voir le chapitre Partager un dossier avec un système virtualisé. page suiv.

Pour identifier la clé et trouver sous quel nom elle est reconnue, utiliser l'Utilitaire de disque. Commencer par ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `disque` et cliquer sur *Disques*. Dans la fenêtre de Disques, la partie de gauche liste les disques connus du système. Brancher la clé USB à l'ordinateur, elle apparait alors dans la liste. La selectionner et noter son nom de modèle quelque part, il apparait dans la fenêtre de droite du logiciel et contient en général le terme *USB* ou Flash.

23.7.1 Connecter la clé au système virtuel

Lancer le Gestionnaire de machines virtuelles en ouvrant la vue d'ensemble des Activités et en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `virt` et cliquer sur *Gestionnaire de machines virtuelles*. Enfin, entrer le mot de passe demandé.

Sélectionner la machine virtuelle sur laquelle la clé USB sera connectée et cliquer sur *Ouvrir*. Dans la nouvelle fenêtre, cliquer sur le menu *Machine virtuelle* → *Démarrer*. Pour avoir une vue du système Windows, cliquer sur le menu *Afficher* → *Console*

Quand le système a finit de démarrer, cliquer sur le menu *Machine virtuelle* → *Rediriger vers un périphérique USB*. Dans la fenêtre qui s'ouvre, sélectionner la clé USB reconnaissable par le nom de son modèle qui a été noté précédemment. Le système virtuel la reconnait immédiatement, il est alors possible de fermer la fenêtre.

23.7.2 Éjecter la clé et la déconnecter du système virtuel

Commencer par éjecter la clé au sein du sytème Windows. Il est ensuite important de supprimer la redirection vers la clé USB afin que le chemin qui relie la clé USB et Windows ne soit actif que lorsque c'est souhaité. Pour cela cliquer sur le menu *Machine virtuelle* → *Rediriger vers un périphérique USB*. Dans la fenêtre qui s'ouvre, décocher la case correspondant à la clé USB. Il est alors possible de fermer la fenêtre.

À présent la clé n'est plus accessible depuis Windows mais elle est toujours visible depuis le système hôte. Si elle n'est plus utile, il est alors possible de la démonter puis de la débrancher de l'ordinateur.

23.8 Partager un CD ou un DVD avec un système virtualisé

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Dix minutes environ.

23.8.1 Activer le partage de CD/DVD

Commencer par lancer le Gestionnaire de machines virtuelles, pour cela ouvrir la vue d'ensemble des Activités en appuyant sur la touche [⊞] ([⌘] sur un Mac), puis taper `virt` et cliquer sur *Gestionnaire de machines virtuelles*. Enfin, entrer le mot de passe demandé.

Sélectionner la machine virtuelle Windows avec laquelle on souhaite partager un CD ou un DVD et cliquer sur *Ouvrir*. Dans la nouvelle fenêtre, afficher la vue détaillée de la machine virtuelle en cliquant sur le menu *Afficher* → *Détails*. Dans la liste des matériels à gauche, sélectionner *IDE CD-ROM 1* ou *SATA CDROM 1* selon les fonctionalités de votre ordinateur.

Insérer le CD ou le DVD dans le lecteur et attendre quelques instants. Choisir *CD-ROM ou DVD* à droite puis cliquer sur *Appliquer*. Il se peut que le CD ou le DVD ait un nom. Pour le trouver ouvrir la vue d'ensemble des Activités en appuyant sur la touche [⊞] ([⌘] sur un Mac), puis taper `fic` et cliquer sur *Fichier*. Dans la colonne de gauche regarder le nom du DVD.

Afficher l'écran de la machine virtiuelle avec *Afficher* → *Console* et la démarrer avec *Machine virtuelle* → *Démarrer*. Windows devrait alors détecter le CD inséré. Si ce n'est pas le cas, essayer de le chercher dans l'explorateur de fichier. Si ça ne marche pas du premier coup, recommencer l'opération.

23.8.2 Éjecter le CD/DVD

Quand on a fini d'utiliser le CD dans Windows, l'éjecter depuis Windows, puis retourner dans la vue détaillée de la machine virtuelle avec *Afficher* → *Détails*, sélectionner *IDE CD-ROM 1* ou *SATA CDROM 1* et cliquer sur ⌫.

23.9 Partager un dossier avec un système virtualisé

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quinze minutes environ.

Vu que le Windows *invité* n'a pas le droit de sortir de sa boîte pour aller chercher lui-même des fichiers, il peut être nécessaire de lui en faire parvenir depuis « l'extérieur ». Voyons donc comment procéder.

Attention : en apprenant à utiliser ce système de partage, il pourrait être tentant de vouloir le configurer pour donner accès à la totalité des disques branchés sur le système hôte : c'est bien **la pire idée imaginable**, qui anéantirait à elle seule toute la politique de sécurité.

23.9.1 Créer un dossier réservé à cet effet dans le système hôte

Ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `fic` et cliquer sur *Fichiers*. Ensuite, choisir l'emplacement où on veut mettre ce dossier d'échange. Par exemple : dans le *Dossier personnel* cliquer sur le bouton ☰ puis sur le bouton formé de l'icône 🗀 avec un petit ✚ en bas à droite (*Nouveau dossier*) et lui donner un nom évocateur. (« *Dossier lisible par Windows* » ou « *Dossier où Windows peut écrire* », par exemple). C'est dans ce dossier qu'il faudra mettre les fichiers que l'on veut transférer dans Windows.

23.9.2 Installer l'Afficheur distant

Actuellement, le Gestionnaire de machines virtuelles ne permet pas l'activation du partage de dossiers. Il est nécessaire d'utiliser le logiciel *Afficheur distant*. L'étape suivante est donc d'installer le logiciel *Afficheur distant*.

page 134

23.9.3 Activer le partage du dossier

Pour activer le partage de dossier, il faut d'abord démarrer la machine virtuelle Windows depuis le Gestionnaire de machines virtuelles.

Pour accéder au Gestionnaire de machines virtuelles, ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `virt` et cliquer sur *Gestionnaire de machines virtuelles*. Entrer le mot de passe demandé.

Dans la fenêtre du Gestionnaire de machines virtuelles, effectuer un clic-droit sur la machine virtuelle désirée (par exemple, *Windows_propre*) et cliquer sur *Démarrer*.

La machine virtuelle démarre alors, mais son écran n'est pas visible. Nous utiliserons l'Afficheur distant pour y accéder.

Ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `affi` et cliquer sur *Afficheur distant*. La première fois, il faut entrer l'adresse de la machine virtuelle dans le champ *Adresse de la connexion*. Généralement, l'adresse est : `spice://localhost:5900`. Si plus d'une machine virtuelle est en cours de fonctionnement la première démarrée aura l'adresse `spice://localhost:5900`, la deuxième `spice://localhost:5901` et ainsi de suite. À partir de la deuxième fois, il est possible de cliquer sur l'adresse désirée dans *Connexions récentes*. Cliquer sur le bouton *Connecter*.

Une fenêtre *Permettre de neutraliser les raccourcis* apparait. Elle demande si on veut neutraliser les raccourcis. Pour avoir le même fonctionnement entre l'Afficheur distant et le *Gestionnaire de machines virtuelles* choisir *Autoriser*.

⚠ **Attention** : avant de cocher la case *Partager le dossier*, il faut être bien sûre que l'on veut laisser le système Windows lire tout le contenu du dossier qu'on a demandé de partager.

Depuis la fenêtre de l'Afficheur distant contenant la machine virtuelle Windows, cliquer sur le menu *Fichier* → *Préférences*. Dans la fenêtre qui s'affiche, sélectionner le dossier que l'on souhaite partager. Pour cela, dans le menu déroulant situé à droite, sélectionner *Autre*. Dans la fenêtre de navigation qui s'ouvre sélectionner le dossier *Dossier lisible par Windows* que l'on a créé, puis cliquer sur *Ouvrir*. Cocher les cases *Partager le dossier* et *Lecture seule*.

⚠ Toujours cocher la case *Lecture seule* sauf si l'on souhaite faire sortir des fichiers du Windows virtualisé, auquel cas on donnera un nom explicite comme *Dossier où Windows peut écrire* au dossier partagé.

⚠ **Attention** : à l'heure où ces lignes sont écrites, un bug dans l'Afficheur distant fait que l'option *Lecture seule* n'est pas prise en compte. Par conséquent, même si l'on coche cette case, le Windows virtualisé pourra écrire dans le dossier partagé. Si l'on veut partager des fichiers avec Windows, il est plus prudent d'y mettre des copies plutôt que les originaux de ces fichiers, afin de ne pas prendre le risque que Windows les modifie.

23.9.4 Copier les fichiers

Dans la machine virtuelle Windows, ouvrir l'explorateur de fichiers. Après un petit moment, *Spice Client (Z :)* devrait être accessible sous *Ce PC*.

Spice Client (Z :) correspond au dossier que nous avons choisi de partager sur notre système hôte, il est possible de lire tous les fichiers et dossiers qu'il contient et de copier ce qui nous intéresse vers un autre dossier dans Windows.

23.9.5 Arrêter le partage

Pour une raison ou pour une autre, on peut vouloir arrêter de partager le dossier avec Windows.

Après avoir démarré le système virtualisé, ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `affi` et cliquer sur Afficheur distant. Dans *Connexions récentes*, cliquer sur l'adresse désirée, `spice://localhost:5900` pour accéder à la première machine virtuelle démarrée. Cliquer sur le bouton *Connecter*.

Depuis la fenêtre de l'Afficheur distant contenant la machine virtuelle Windows, cliquer sur le menu *Fichier* → *Préférences*. Dans la fenêtre qui s'affiche, décocher la case *Partager le dossier*.

Le dossier sélectionné n'est maintenant plus accessible depuis Windows.

Chapitre 24

Garder un système à jour

Comme expliqué précédemment, les logiciels malveillants se faufilent dans nos ordi- page 32
nateurs, entre autres, par l'intermédiaire de « failles de sécurité ».

Des corrections pour ces erreurs de programmation (ou de conception) sont régulièrement mises à disposition, au fur et à mesure qu'elles sont identifiées. Une fois que ces corrections sont disponibles, il est particulièrement important de remplacer les anciennes versions des logiciels. En effet, les problèmes corrigés, qui pouvaient n'avoir auparavant été identifiés que par quelques spécialistes, sont ensuite connus et référencés publiquement… donc plus faciles à exploiter.

24.1 Garder Tails à jour

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Trente minutes à une heure, plus environ trente minutes de téléchargement.

Un système *live* étant une collection indivisible de logiciels, exécutés à partir d'un DVD ou d'une clé USB, la seule solution praticable pour utiliser les dernières versions de ces logiciels est de s'assurer qu'on utilise bien la dernière version du système *live*. page 113

Après avoir connecté le système *live* Tails à Internet, une fenêtre *Une mise à niveau est proposée* ou *Une nouvelle version est proposée* apparaît pour nous prévenir lorsqu'une nouvelle version qui corrige des failles de sécurité est disponible.

Dans le cas où l'on utilise un DVD, il faut détruire celui contenant l'ancienne version et en graver un nouveau. Sauf si celui-ci est réinscriptible, auquel cas il suffira de l'effacer pour y graver la dernière version de Tails.

Pour une clé USB et dans la mesure où l'on dispose d'une connexion Internet, on peut effectuer la mise à jour directement. Cliquer sur *Mettre à niveau maintenant* et de suivre l'assistant tout au long du processus. Si une erreur se produit, ou s'il est nécessaire d'utiliser une autre méthode de mise à jour, l'assistant nous orientera vers la page de la documentation appropriée.

Celle-ci se trouve à partir de la *Documentation de Tails* apparaissant sur le bureau. Dans l'index qui s'ouvre, chercher la section *Téléchargement, installation et mise à jour* et cliquer sur la page *Upgrading automatically*.

24.2 Garder à jour un système chiffré

page 119

Une fois installé, un système chiffré doit être gardé à jour pour qu'on puisse continuer de lui faire confiance. Les sections qui suivent concernent le système Debian, mais les concepts s'appliquent dans les grandes lignes à quasiment tous les autres systèmes.

Le projet Debian publie, à peu près tous les deux ans, une version *stable*. Cela représente un énorme effort pour coordonner la compatibilité des différentes versions des logiciels, effectuer de nombreux tests et s'assurer qu'il n'y reste aucun défaut majeur.

24.3 Les mises à jour quotidiennes d'un système chiffré

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Une minute pour lancer la mise à jour, plus un temps variable pour les téléchargements et l'installation, pendant lequel on peut continuer à utiliser son ordinateur.

Tout l'intérêt d'une version *stable* de Debian est que par la suite, les logiciels qui la composent ne sont plus modifiés en profondeur : les mises à jour incluent les améliorations de traduction, les corrections de problèmes liés à la sécurité ou empêchant d'utiliser normalement un programme, *etc.*

Généralement, ces nouvelles versions sont installées automatiquement par le système, à partir du moment où il dispose d'un accès Internet, et ne devraient pas perturber les petites habitudes qu'on a prises.

24.3.1 Procéder aux mises à jour

Lorsqu'on a installé l'*environnement graphique de bureau*, le système vérifiera automatiquement, lorsqu'il sera connecté à Internet, la disponibilité de nouvelles versions dans les dépôts configurés.

page 136

Lorsque c'est le cas, une notification indiquant que *Des mises à jour logicielles sont disponibles* apparaîtra.

Cliquer sur *Afficher* dans la notification, ce qui ouvre *Logiciels*.

Une liste des mises à jour s'affiche. Si *Logiciels* ne les a pas déjà toutes téléchargées, un bouton *Télécharger* apparaît, sur lequel il faut cliquer pour lui demander de le faire.

Une fois les mises à jour téléchargées, le bouton *Redémarrer et mettre à jour* apparaît. Cliquer sur ce bouton, puis confirmer en cliquant à nouveau sur *Redémarrer et installer*. L'ordinateur redémarre et demande la phrase de passe de chiffrement du disque dur, avant d'installer les mises à jour. L'ordinateur redémarre à nouveau sur un système à jour et demande la phrase de passe.

24.3.2 Supprimer les paquets obsolètes

Une fois l'ordinateur redémarré, il faut encore demander au système de supprimer les composants logiciels qui ne sont plus nécessaires : cette opération n'étant pas effectuée automatiquement par le système, il nous faut la faire régulièrement, sous peine de voir notre disque — et en particulier la partition de démarrage `/boot` — se remplir petit à petit, jusqu'au point où il ne sera plus possible de faire de nouvelles mises à jour.

Il n'est pas encore possible de faire cette opération à travers l'interface graphique, il faut donc ouvrir un Terminal.

page 97

Commencer par devenir admin en tapant la commande :

```
sudo su
```

L'ordinateur devrait nous demander notre mot de passe de session. Si l'on obtient `bash: sudo : commande introuvable`, alors taper plutôt :

```
su -
```

Notre terminal a maintenant le pouvoir d'administration sur notre système.

La commande suivante, à taper dans ce terminal, permet alors de supprimer les paquets obsolètes :

```
apt autoremove
```

24.4 Passage à une nouvelle version stable

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Une demi-journée à une journée, dont un long temps de téléchargement pendant lequel on peut continuer à utiliser son ordinateur, et un long temps d'installation pendant lequel il vaut mieux ne plus l'utiliser.

Lorsqu'une nouvelle version *stable* de Debian sort, le projet veille à garder à jour la précédente version *stable*, appelée *oldstable* pendant une durée d'**un an**[1] minimum. Cette durée est prolongée par un équipe de maintenance à long terme (*Long Term Support*)[2]. Ainsi, la version de Debian utilisée dans l'édition 2017 de ce guide, Debian 9 Stretch, n'était prise en charge par l'équipe de la sécurité de Debian que jusque juillet 2020 et l'équipe *Long Term Support* en avait repris la maintenance jusque juin 2022.

Il est donc nécessaire de profiter de cette période pour prendre le temps de mettre à jour son système vers la nouvelle version stable. C'est un processus plus délicat que les mises à jour quotidiennes. Pas nécessairement dans sa réalisation même, mais dans le fait qu'il est ensuite nécessaire de s'adapter aux changements qu'auront connu les logiciels que nous utilisons habituellement.

Dans tous les cas, avant de continuer il est vivement conseillé de sauvegarder ses données. page 151

Deux possibilités s'offrent à nous :

- Mettre à jour notre système vers la nouvelle version stable. L'avantage est que cela permet de garder les logiciels installés et les configurations qu'on a effectuées au fil du temps… ce qui peut aussi être un inconvénient si on a trop bidouillé. Si l'on choisit cette possibilité, continuer d'utiliser cet outil.
- Faire une nouvelle installation de la nouvelle version de Debian. L'avantage est d'en profiter pour repartir sur des bases propres. L'inconvénient est de perdre nos configurations spécifiques, et qu'il faut à nouveau télécharger et vérifier le programme d'installation. Si l'on choisit cette possibilité, une fois la sauvegarde effectuée, la suite se trouve dans l'outil faire une nouvelle installation de Debian. page 119

La précédente mise à jour du *Guide d'autodéfense numérique* utilisait la version 9 de Debian, appelée Stretch, sortie en juin 2017. À la sortie de cette mise à jour du guide, Debian en est à la version 11, appelée Bullseye, sortie en août 2021. Il est risqué de passer directement de la version 9 à la 11 sans passer par la version 10, appelée Buster, sortie en juillet 2019.

Pour savoir quelle version de Debian on utilise, ouvrir la vue d'ensemble des activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `param` et cliquer sur *Paramètres*. Dans la colonne de gauche aller tout en bas et cliquer sur *À Propos*. La version de Debian utilisée apparaît sous *Nom du système d'exploitation*.

1. Debian, 2017, *DebianOldStable* [https://wiki.debian.org/fr/DebianOldStable].
2. Debian, 2021, *Debian Long Term Support* [https://wiki.debian.org/fr/LTS]

Si l'on est encore à la version 9 Stretch, on va donc proposer une mise à jour en deux temps, de la version 9 Stretch à la version 10 Buster, puis de la version 10 Buster à la version 11 Bullseye. Il est possible de suivre seulement la seconde étape si on est déjà à la version 10 Buster.

24.4.1 Passage de Stretch à Buster

La procédure détaillée ici concerne la mise à jour de la version de Debian appelée Stretch ou 9, sortie en juin 2017, à la version Buster ou 10, sortie en juillet 2019.

Nous documenterons ici une procédure de mise à jour simplifiée qui a été testée sur des installations de Debian Stretch avec un environnement graphique de bureau GNOME et des logiciels provenant uniquement des dépôts officiels de Debian.

Elle nécessite de disposer, pour la durée de la mise à jour, d'une connexion à Internet.

⚠ **Attention** : cette procédure simplifiée a moins de chances de fonctionner lorsqu'on a bidouillé son système en ajoutant des sources de mises à jour non officielles.

Si c'est le cas, se référer aux notes de publication officielles du projet Debian[3], notamment la partie Mises à niveau depuis Debian 9 (Stretch)[4] et la partie Problèmes à connaître pour Buster[5].

Mettre à jour sa Debian Stretch

Avant tout, il est nécessaire de disposer d'une Debian Stretch à jour. Sans cela, la mise à niveau risque fort de ne pas fonctionner. Au cas où ces mises à jour n'auraient pas été faites au quotidien, c'est le moment de rattraper le retard. S'il vous est proposé de redémarrer, suite à de nombreuses mises à jour, le faire avant de procéder à la suite des opérations.

page 176

S'assurer d'avoir assez d'espace libre sur le disque dur

Afin d'éviter toute mauvaise surprise, il faut avoir au moins 4 Go d'espace libre sur le disque dur qui contient le système.

Ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `fich` et cliquer sur *Fichiers*. Dans la barre de gauche, cliquer sur *Autres emplacements*. À droite de la ligne *Ordinateur*, l'espace disponible s'affiche, par exemple *11,7 Go/17,1 Go de disponibles* signifie qu'on a 11,7 Go disponibles.

Libérer de l'espace sur le disque si nécessaire S'il n'y a pas assez d'espace sur le disque dur, une solution est d'effacer d'anciennes mises à jour devenues obsolètes. Pour cela, ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `paquet` et cliquer sur *Gestionnaire de paquets*. Puisque le gestionnaire de paquets permet de modifier les logiciels installés sur l'ordinateur, un mot de passe est nécessaire pour l'ouvrir.

Dans le menu *Configuration* choisir *Préférences*, puis sélectionner l'onglet *Fichiers* et cliquer sur le bouton *Supprimer les paquets en cache*, puis sur *OK* et fermer le *Gestionnaire de paquets Synaptic*.

Vérifier à nouveau l'espace disque disponible, comme expliqué ci-dessus. Si cela ne suffit pas, il faudra supprimer certains de nos propres fichiers ou supprimer des logiciels.

---

3. https://www.debian.org/releases/buster/amd64/release-notes/index.fr.html
4. https://www.debian.org/releases/buster/amd64/release-notes/ch-upgrading.fr.html
5. https://www.debian.org/releases/buster/amd64/release-notes/ch-information.fr.html

Désactiver les dépôts non-officiels

La mise à jour n'est testée qu'avec les paquets officiellement fournis par Debian Stretch. On va donc désactiver tous les autres dépôts Debian, y compris les dépôts *backports*.

Pour cela, ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `update` et cliquer sur *Software & Updates* (logiciels et mises à jour).

Dans l'onglet *Other software* (autres logiciels), décocher toutes les cases qui seraient cochées. Lorsqu'on effectue un changement, on doit entrer le mot de passe d'administration.

Cliquer sur *Fermer*. Si l'on a effectué des changements, une fenêtre affiche *Les informations sur les logiciels disponibles sont obsolètes*. Cliquer sur *Actualiser*.

Désactiver l'économiseur d'écran

Lors de la mise à jour, l'économiseur d'écran peut se bloquer, et laisser l'écran verrouillé. Il est donc prudent de le désactiver pour le temps de la mise à jour.

Pour cela, ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `param` et cliquer sur *Paramètres*. Dans la colonne de gauche cliquer sur *Confidentialité*.

Cliquer sur *Verrouillage de l'écran*. Dans la fenêtre qui s'affiche, désactiver *Verrouillage automatique de l'écran*. Fermer cette fenêtre en cliquant sur ✖, puis à nouveau sur ✖ en haut à droite, pour fermer la fenêtre *Paramètres*.

Ouvrir un terminal

Il n'est pas encore possible de faire cette opération à travers l'interface graphique, il faut donc ouvrir un Terminal. page 97

Commencer par devenir admin en tapant la commande :

```
sudo su
```

L'ordinateur devrait nous demander notre mot de passe de session. Si l'on obtient `bash: sudo : commande introuvable`, alors taper plutôt :

```
su -
```

Notre terminal a maintenant le pouvoir d'administration sur notre système.

Mettre à jour les dépôts

Commençons par modifier les dépôts configurés afin d'utiliser ceux dédiés à la nouvelle version. On va ouvrir le fichier contenant la liste des dépôts utilisés par Debian dans le terminal.

```
gedit /etc/apt/sources.list
```

L'éditeur de texte s'ouvre. Choisir ☰ → *Rechercher et remplacer*. Dans la fenêtre qui s'ouvre, *Rechercher* « `stretch` » pour le *Remplacer par* « `buster` ». Cliquer ensuite sur le bouton *Tout remplacer*, puis fermer la fenêtre de recherche avec ✖.

Si une installation ou une mise à jour a été faite auparavant en utilisant un CD ou un DVD, c'est une bonne idée de chercher les lignes qui commencent par « `deb cdrom:` » pour les supprimer.

On peut ensuite cliquer sur *Enregistrer* puis fermer l'éditeur.

Nous avons modifié la liste des dépôts ; il faut donc maintenant télécharger la liste des paquets qui y sont disponibles, avant de pouvoir les installer ; pour cela, toujours dans le *Terminal* qu'on gardera ouvert, taper la commande :

```
#_ apt update
```

Si une erreur s'affiche à propos du « cache système d'AppStream » on peut l'ignorer sans inquiétude.

Lancer la mise à jour proprement dite

La mise à jour se fait en plusieurs étapes que l'on pilotera à l'aide de notre Terminal.

Notre première commande dit au gestionnaire de paquets, d'une part, que nous préférons qu'il nous pose le moins de questions possible concernant les détails de la mise à jour ; d'autre part, qu'on ne veut pas voir l'historique des changements :

```
#_ export DEBIAN_PRIORITY=critical APT_LISTCHANGES_FRONTEND=none
```

Notre deuxième commande effectue la première partie de la mise à jour du système :

```
#_ apt upgrade
```

Assez rapidement, le terminal affiche `Souhaitez-vous continuer [O/n] ?` Après avoir confirmé en appuyant sur *Entrée* (↵ ou return), on peut voir apparaître une première série de fenêtres bleues nous demandant comment gérer certains changements. Lorsqu'on ne cherche pas à sortir des choix de Debian, appuyer sur *Entrée* à chaque fois est suffisant.

Une fenêtre qui indique qu'un fichier de configuration a été modifié et qui nous demande si on veut le remplacer par sa nouvelle version peut aussi s'afficher. Le *Garder* ou le *Remplacer* est un choix qui dépend de l'importance des modifications que l'on a pu y apporter ainsi que des nouveautés proposées. Il n'y a donc pas de réponse générique ici. Il faudra soit comparer les versions, soit jouer à pile ou face.

Au bout d'un moment, un certain nombre de paquets ont déjà été mis à jour, et le terminal devrait revenir à l'invite de commande.

La commande suivante terminera la mise à jour du système :

```
#_ apt full-upgrade
```

Assez rapidement, le terminal affiche à nouveau `Souhaitez-vous continuer [O/n] ?` Après avoir confirmé en appuyant sur *Entrée* (↵ ou return), on peut voir apparaître une seconde série de fenêtres bleues nous demandant comment gérer certains changements. Lorsqu'on ne cherche pas à sortir des choix de Debian, appuyer sur *Entrée* à chaque fois est suffisant.

À cette étape de la mise à jour, il peut arriver que le bureau GNOME affiche divers messages d'erreurs. Ce n'est pas particulièrement inquiétant, dans la mesure où l'on est en train de réinstaller de nombreux composants du système. Ces problèmes devraient se résoudre d'eux-mêmes une fois le processus terminé.

Quelques évolutions du système plus tard, le terminal nous invite une nouvelle fois à lui indiquer des commandes.

On peut alors saisir une dernière commande, pour libérer de l'espace disque :

```
#_ apt autoremove
```

Puis :

```
#_ apt clean
```

Premier redémarrage

Le moment est maintenant venu de redémarrer le système, en utilisant le menu ⏻ en haut à gauche et en choisissant *Redémarrer*.

24.4.2 Passage de Buster à Bullseye

La procédure détaillée ici concerne la mise à jour de la version de Debian appelée Buster ou 10, sortie en juillet 2019, à la version Bullseye ou 11, sortie en août 2021.

Nous documenterons ici une procédure de mise à jour simplifiée qui a été testée sur des installations de Debian Buster avec un environnement graphique de bureau GNOME et des logiciels provenant uniquement des dépôts officiels de Debian.

Elle nécessite de disposer, pour la durée de la mise à jour, d'une connexion à Internet.

⚠ **Attention** : cette procédure simplifiée a moins de chances de fonctionner lorsqu'on a bidouillé son système en ajoutant des sources de mises à jour non officielles.

Si c'est le cas, se référer aux notes de publication officielles du projet Debian[6], notamment la partie Mises à niveau depuis Debian 10 (Buster)[7] et la partie Problèmes à connaître pour Bullseye[8].

Mettre à jour sa Debian Buster

Avant tout, il est nécessaire de disposer d'une Debian Buster à jour. Sans cela, la mise à niveau risque fort de ne pas fonctionner. Au cas où ces mises à jour n'auraient pas été faites au quotidien, c'est le moment de rattraper le retard. S'il vous est proposé de redémarrer, suite à de nombreuses mises à jour, le faire avant de procéder à la suite des opérations.

page 176

S'assurer d'avoir assez d'espace libre sur le disque dur

Afin d'éviter toute mauvaise surprise, il faut avoir au moins 4 Go d'espace libre sur le disque dur qui contient le système.

Ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `fich` et cliquer sur *Fichiers*. Dans la barre de gauche, cliquer sur *Autres emplacements*. À droite de la ligne *Ordinateur*, l'espace disponible s'affiche, par exemple *11,7 Go/17,1 Go de disponibles* signifie qu'on a 11,7 Go disponibles.

Libérer de l'espace sur le disque si nécessaire S'il n'y a pas assez d'espace sur le disque dur, une solution est d'effacer d'anciennes mises à jour devenues obsolètes. Pour cela, ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `paquet` et cliquer sur *Gestionnaire de paquets*. Puisque le gestionnaire de paquets permet de modifier les logiciels installés sur l'ordinateur, un mot de passe est nécessaire pour l'ouvrir.

Dans le menu *Configuration* choisir *Préférences*, puis sélectionner l'onglet *Fichiers* et cliquer sur le bouton *Supprimer les paquets en cache*, puis sur *OK* et fermer le *Gestionnaire de paquets Synaptic*.

S'il n'y a pas assez d'espace sur le disque dur, il faudra supprimer certains de nos propres fichiers ou supprimer des logiciels.

---

6. https://www.debian.org/releases/bullseye/amd64/release-notes/index.fr.html
7. https://www.debian.org/releases/bullseye/amd64/release-notes/ch-upgrading.fr.html
8. https://www.debian.org/releases/bullseye/amd64/release-notes/ch-information.fr.html

Désactiver l'économiseur d'écran

Lors de la mise à jour, l'économiseur d'écran peut se bloquer, et laisser l'écran verrouillé. Il est donc prudent de le désactiver pour le temps de la mise à jour.

Pour cela, ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `param` et cliquer sur *Paramètres*. Dans la colonne de gauche cliquer sur *Confidentialité*.

Cliquer sur *Verrouillage de l'écran*. Dans la fenêtre qui s'affiche, désactiver *Verrouillage automatique de l'écran*. Fermer cette fenêtre en cliquant sur ✖, puis à nouveau sur ✖ en haut à droite, pour fermer la fenêtre *Paramètres*.

Ouvrir un terminal

Il n'est pas encore possible de faire cette opération à travers l'interface graphique, il faut donc ouvrir un Terminal. page 97

Commencer par devenir admin en tapant la commande :

```
sudo su
```

L'ordinateur devrait nous demander notre mot de passe de session. Si l'on obtient `bash: sudo : commande introuvable`, alors taper plutôt :

```
su -
```

Notre terminal a maintenant le pouvoir d'administration sur notre système.

Mettre à jour les dépôts

Commençons par modifier les dépôts configurés afin d'utiliser ceux dédiés à la nouvelle version.

⚠ **Attention** : c'est dans cette étape que se situe la différence avec la mise à jour précédente.

Dans le terminal taper :

```
sed -i 's,buster/updates,bullseye-security,g' /etc/apt/sources.list
sed -i 's,buster,bullseye,g' /etc/apt/sources.list
```

On peut ensuite cliquer sur *Enregistrer* puis fermer l'éditeur.

Nous avons modifié la liste des dépôts ; il faut donc maintenant télécharger la liste des paquets qui y sont disponibles, avant de pouvoir les installer ; pour cela, toujours dans le *Terminal* qu'on gardera ouvert, taper la commande :

```
apt update
```

Lancer la mise à jour proprement dite

La mise à jour se fait en plusieurs étapes que l'on pilotera à l'aide de notre Terminal.

Notre première commande dit au gestionnaire de paquets, d'une part, que nous préférons qu'il nous pose le moins de questions possible concernant les détails de la mise à jour ; d'autre part, qu'on ne veut pas voir l'historique des changements :

```
export DEBIAN_PRIORITY=critical APT_LISTCHANGES_FRONTEND=none
```

Notre deuxième commande effectue la première partie de la mise à jour du système :

```
apt upgrade
```

Assez rapidement, le terminal affiche `Souhaitez-vous continuer [O/n] ?` Après avoir confirmé en appuyant sur *Entrée* (↵ ou return), on peut voir apparaître une première série de fenêtres bleues nous demandant comment gérer certains changements. Lorsqu'on ne cherche pas à sortir des choix de Debian, appuyer sur *Entrée* à chaque fois est suffisant.

Une fenêtre qui indique qu'un fichier de configuration a été modifié et qui nous demande si on veut le remplacer par sa nouvelle version peut aussi s'afficher. Le *Garder* ou le *Remplacer* est un choix qui dépend de l'importance des modifications que l'on a pu y apporter ainsi que des nouveautés proposées. Il n'y a donc pas de réponse générique ici. Il faudra soit comparer les versions, soit jouer à pile ou face.

Au bout d'un moment, un certain nombre de paquets ont déjà été mis à jour, et le terminal devrait revenir à l'invite de commande.

La commande suivante terminera la mise à jour du système :

```
#_ apt full-upgrade
```

Assez rapidement, le terminal affiche à nouveau `Souhaitez-vous continuer [O/n] ?` Après avoir confirmé en appuyant sur *Entrée* (↵ ou return), on peut voir apparaître une seconde série de fenêtres bleues nous demandant comment gérer certains changements. Lorsqu'on ne cherche pas à sortir des choix de Debian, appuyer sur *Entrée* à chaque fois est suffisant.

À cette étape de la mise à jour, il peut arriver que le bureau GNOME affiche divers messages d'erreurs. Ce n'est pas particulièrement inquiétant, dans la mesure où l'on est en train de réinstaller de nombreux composants du système. Ces problèmes devraient se résoudre d'eux-mêmes une fois le processus terminé.

Quelques évolutions du système plus tard, le terminal nous invite une nouvelle fois à lui indiquer des commandes.

On peut alors saisir une dernière commande, pour libérer de l'espace disque :

```
#_ apt autoremove
```

Puis :

```
#_ apt clean
```

Premier redémarrage

Le moment est maintenant venu de redémarrer le système, en utilisant le menu ⏻ en haut à gauche et en choisissant *Redémarrer*.

Réactiver les dépôts Debian supplémentaires

On peut maintenant souffler. Le plus gros est fait. Il reste toutefois encore quelques petits ajustements…

Si l'on a désactivé des dépôts non officiels avant la mise à jour, c'est le moment de vérifier qu'on en a toujours besoin avec la nouvelle version de Debian. Si oui, les réactiver. On peut également réactiver l'économiseur d'écran si on l'a désactivé auparavant. page 136

Réactiver le verrouillage de l'écran

Pour cela, ouvrir la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `param` et cliquer sur *Paramètres*. Dans la colonne de gauche cliquer sur *Confidentialité*.

Cliquer sur *Verrouillage de l'écran*. Dans la fenêtre qui s'affiche, activer *Verrouillage automatique de l'écran*. Fermer cette fenêtre en cliquant sur ✖.

S'assurer que le nouveau système fonctionne correctement

Il peut être utile de s'assurer que les actions et les commandes les plus courantes sont fonctionnelles. Le cas échéant, il pourrait être nécessaire de diagnostiquer et de résoudre les problèmes. Il vaut certainement mieux le faire dès la prise de contact avec le nouveau système, afin de pouvoir repartir pour deux ans avec un système fonctionnel. Les problèmes les plus courants sont souvent décrits, avec les astuces pour les résoudre, dans diverses documentations sur Debian et GNU/Linux.

page 129

Rappelons également qu'il existe des notes de publication officielles du projet Debian [9].

9. https://www.debian.org/releases/bullseye/amd64/release-notes/index.fr.html

Chapitre 25

Nettoyer les métadonnées d'un document

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quelques minutes.

L'objectif de l'outil que l'on va examiner est d'effacer les métadonnées présentes dans un document avant sa publication. Ces métadonnées ne sont pas les mêmes dans tous les formats de documents : certaines sont plus difficiles à nettoyer que d'autres, voire impossibles. Cependant, la plupart des formats utilisés pour échanger des documents terminés, que ce soient des textes, des images, du son ou de la vidéo, sont « nettoyables ».

page 30

L'outil à utiliser pour cela est *MAT2* (pour *Metadata Anonymisation Toolkit 2*) qui permet de nettoyer aisément de nombreux formats de fichiers.

Attention : nettoyer les métadonnées n'anonymise pas le contenu des fichiers, et n'enlève pas les éventuels marquages [1] qui seraient inclus dans le contenu lui-même.

25.1 Installer les logiciels nécessaires

Sur un système où il n'est pas encore présent, il faut installer le paquet (voir page 135) `mat2`. Sous Tails, MAT2 est déjà installé.

25.2 Nettoyer un ou des fichiers

Dans le gestionnaire de fichiers, faire un clic droit sur le document dont on veut enlever les métadonnées puis sélectionner *Remove metadata*. Un nouveau document sans métadonnées est alors créé. Il porte le nom du fichier original suivi de *.cleaned* puis de l'extension du fichier.

Astuce ! Pour traiter plusieurs fichiers, il est possible de sélectionner un ensemble de fichiers et de faire un clic droit puis *Remove metadata*. L'opération peut prendre un peu de temps en fonction du nombre de fichiers et de leur taille.

Certains formats ne sont pas supportés par cet outil. Dans ce cas un message d'avertissement *Failed to clean some items* apparaît. Un bouton *Show* permet d'avoir la liste des fichiers qui n'ont pas été traités. Si le format n'est pas supporté il est possible d'exporter le fichier qui ne peut pas être traité dans un format plus commun. Par exemple pour nettoyer un fichier au format XCF du programme de manipulation d'images GIMP, il est possible de l'exporter au format JPEG ou PNG.

1. Voir à ce sujet Wikipédia, 2014, *Tatouage numérique* [https://fr.wikipedia.org/wiki/Tatouage_num%C3%A9rique] et Wikipédia, 2014, *Stéganographie* [https://fr.wikipedia.org/wiki/St%C3%A9ganographie].

25.2.1 Cas particulier des fichiers PDF

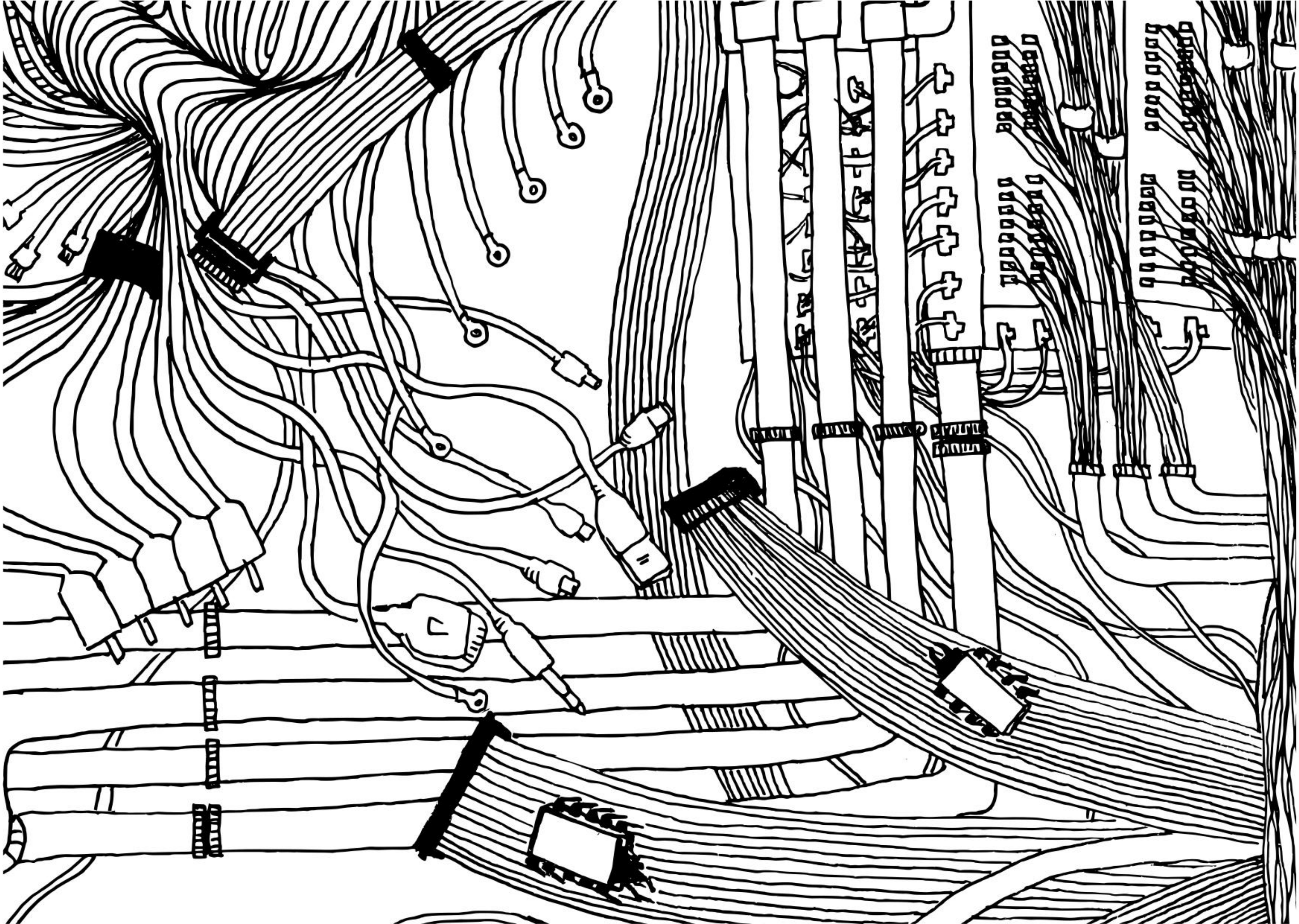
Pour enlever correctement les métadonnées d'un fichier PDF, MAT2 le « transforme » en image. Ainsi un fichier PDF sans metadonnées perdra tous ses liens hypertextes et aura une taille supérieure au fichier initial.

25.2.2 Cas particulier des vidéos

MAT2 supprime les métadonnées d'un fichier vidéo, mais il n'est pas capable de supprimer d'autres traces qui pourraient parfois permettre d'identifier la source de la vidéo : des rayures ou des traces de doigts sur l'objectif par exemple, ou encore comme on l'a vu plus haut des marques invisibles et indétectables (appelées *tatouages numériques*, ou *digital watermarks* en anglais) qui pourraient être directement ajoutées aux images de la vidéo par le matériel ou le logiciel de captation utilisé.

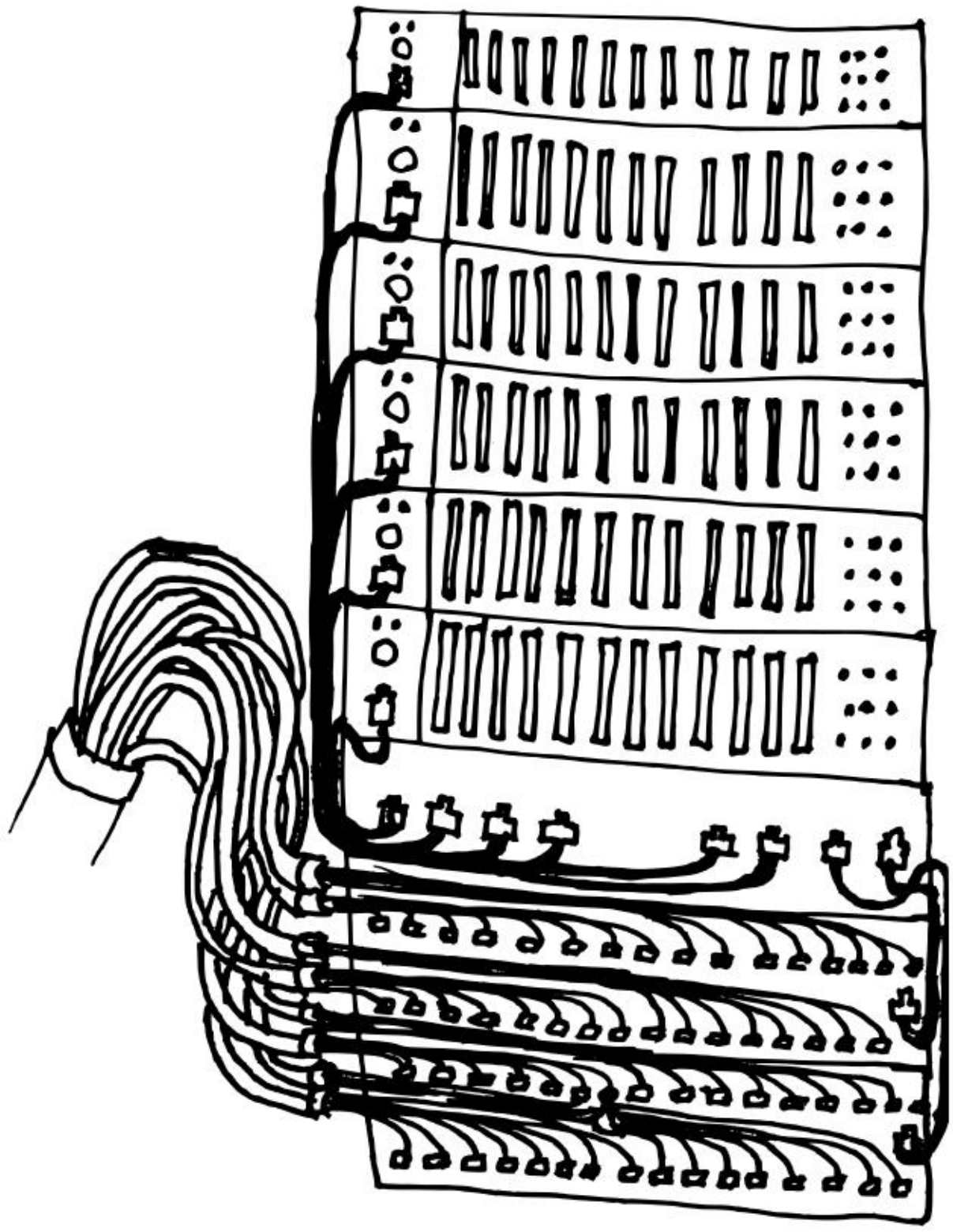
Ainsi, pour faire en sorte qu'une vidéo ne contienne vraiment plus aucune information permettant de retrouver son autrice, la suppression des métadonnées par MAT2 ne suffit pas : il faut aussi réaliser cette vidéo avec du matériel qui n'est lié à aucune identité (c'est-à-dire qui n'a jamais servi pour publier des images avec une autre identité contextuelle), et utiliser uniquement Tails pour l'éditer.

Néanmoins, dans la plupart des cas et face à la plupart des adversaires (et de leurs moyens) qui voudraient identifier l'autrice d'une vidéo, supprimer les métadonnées de cette vidéo avec MAT2 constitue déjà une assez bonne mesure de protection.



Tome 2

En ligne



Quatrième partie

Comprendre

Introduction

Dans le premier tome, nous avons expliqué que l'utilisation d'ordinateurs laisse des traces de nos activités et de nos données. La plongée dans les mystères de ces machines, pourtant familières, s'était déjà avérée un brin complexe. Qu'en sera-t-il maintenant qu'on se propose de se connecter à Internet ? Qu'est-ce que ça implique de connecter notre ordinateur à d'autres ordinateurs, sur lesquels on a peu ou pas de prise du tout ? Un ordinateur connecté est avant tout un ordinateur ; aussi, la lecture du premier tome est essentielle pour appréhender ce *tome 2* à propos de sécurité *en ligne*.

*
* *

Commençons par le début. Internet est un réseau. Ou plutôt, un ensemble de réseaux connectés entre eux qui, à partir d'une obscure application à visée militaire, s'est étendu au fil de dizaines d'années au monde entier. Réseau qui a vu se multiplier les applications, les usagers et les usagères, les technologies et les techniques de contrôle.

Beaucoup ont pu disserter à l'infini sur le « nouvel âge » qui s'ouvrait, les supposées possibilités d'horizontalité et de transparence dans la diffusion de l'information et des ressources, ou dans l'organisation collective, auxquelles a pu ouvrir cette nouvelle technologie — y compris dans l'appui qu'il pouvait offrir pour les luttes politiques. Cependant, comme il semble évident que les pouvoirs n'aiment pas ce qui peut leur échapper, même partiellement, il s'est développé, en même temps que l'expansion des usages, une expansion des techniques de contrôle, de surveillance et de répression dont les conséquences se font de plus en plus sentir.

Au cours de l'année 2011, pour la première fois, des gouvernements ont organisé la déconnexion de la quasi-totalité de leur population vis-à-vis du réseau mondial. Les dirigeants d'Égypte et d'Iran, puisque c'est d'eux qu'il s'agit, ont estimé que pour mieux contenir les révoltes qui prenaient place sur leurs sols, ils avaient tout intérêt à limiter au maximum les possibilités de communication par le réseau — ce qui ne les a pas empêchés, dans le même mouvement, de chercher à organiser la surveillance et le pistage sur Internet. Le gouvernement iranien fut ainsi capable de mettre en place un système d'analyse de trafic demandant des ressources importantes pour surveiller les personnes révoltées, connues ou non, établir une cartographie de leurs relations pour les confondre et condamner les révoltées qui utilisaient le réseau pour s'organiser.

Autre exemple, depuis la mise en place d'une version chinoise de Google[1] en 2006, l'entreprise accepte avec plus ou moins de docilité la politique du gouvernement chinois de filtrage des résultats de recherche.

Des méthodes similaires ont aussi cours dans des pays dits démocratiques. Ainsi, à la fin de l'été 2011, après plusieurs journées d'émeutes à Londres, deux jeunes

1. Wikipédia, 2017, *Google China* [https://fr.wikipedia.org/wiki/Google_China].

anglais ont été condamnés [2] à 4 ans de prison pour avoir appelé sur Facebook à des rassemblements dans leurs quartiers — et ce, alors même que leurs « appels » n'ont pas été suivis.

De même, les révélations d'Edward Snowden [3] sur l'état de la surveillance électronique mise en place par la NSA [4] à l'échelle mondiale ont rendu crédibles les hypothèses parmi les plus pessimistes.

À partir de là, il apparaît indispensable de prendre conscience que l'utilisation d'Internet, tout comme celle de l'informatique en général, est tout sauf anodine. Elle nous expose à la surveillance, et à la répression qui peut lui succéder : c'est l'objet principal de ce second tome que de permettre à tout le monde de comprendre quels sont les risques et les limites associés à l'utilisation d'Internet. Mais il s'agit aussi de se donner les moyens de faire des choix éclairés quant à nos usages. Des choix qui peuvent permettre de compliquer la tâche des surveillantes, de contourner des dispositifs de censure, voire de mettre en place des outils, des infrastructures, de manière autonome. Une première amorce pour reprendre le contrôle de technologies qui semblent parfois vouées à nous échapper — ambition qui dépasse cependant largement les objectif de ce guide.

*
* *

Octobre 2010, Paris

Ce matin, Ana arrive en avance au travail. Elle est employée à La Reboute, une entreprise de vente de vêtements par correspondance, située au dernier étage d'un immeuble rue Jaurès : « Pfiou, 18 étages, vivement que cet ascenseur soit réparé ! » Elle s'installe à son bureau, se penche et appuie sur le bouton d'allumage de l'ordinateur.

Sur l'écran, une petite fenêtre vient d'apparaître. « Connexion réseau établie ». Avant de se mettre au boulot, elle veut regarder ses emails. Ana clique sur l'icône du navigateur web, provoquant l'ouverture d'une fenêtre qui reste vierge quelques millisecondes, avant de faire apparaître la page d'accueil de Google. Tout en appréciant mentalement la page d'accueil « spéciale Halloween » de Google, Ana déplace le pointeur de sa souris et clique sur le lien Connexion. *Une fois la page chargée, elle y rentre son nom d'utilisatrice et son mot de passe, puis clique sur Gmail. Quelque part dans une obscure salle bondée d'ordinateurs, un disque dur grésille. Quelques secondes après avoir ouvert son navigateur web, Ana commence à parcourir sa boîte mail. Alors qu'elle consulte un email reçu du site* leboncoin.fr, *son regard est attiré par le lien qui vient de s'afficher dans la colonne de droite : « Tiens, quelqu'un vend le même modèle d'appareil photo que celui que je cherche, juste au coin de la rue... je devrais peut-être y faire un saut. »*

— *« Ah ben t'es là ? »*

La voix dans le dos d'Ana la fait légèrement sursauter. C'est Bea, une collègue.

— *« Ben oui, je me suis levée un peu plus tôt que d'habitude, alors j'ai pris le RER de 7h27 au lieu de 7h43. Je regarde vite fait mes emails*

2. France Soir, 2011, *Émeutes à Londres : Deux jeunes condamnés à quatre ans de prison* [http://archive.francesoir.fr/actualite/international/emeutes-londres-deux-jeunes-condamnes-quatre-ans-prison-128302.html].

3. Wikipédia, 2014, *Edward Snowden* [https://fr.wikipedia.org/wiki/Edward_Snowden].

4. *National Security Agency*, agence dépendant du département de la Défense des États-Unis, chargée de la collecte et de l'analyse des données étrangères et de la protection des données états-uniennes.

avant de m'y mettre. J'attends la confirmation d'une réservation de billet pour les Baléares cet hiver.
— *Vacances au soleil, j'vois le genre… Et t'en as pour longtemps ? »*

Bea a l'air pressée.

— *« Euh… non non, j'avais presque fini. Pourquoi ?*
— *Ben, si ça te dérange pas, je t'emprunterais bien ton poste deux minutes… Le mien est planté depuis hier, j'attends que la nouvelle responsable informatique arrive pour régler ça ».*

Aussitôt assise, Bea clique nerveusement sur la barre d'adresse du navigateur web, et rentre directement l'adresse du blog sur lequel sont régulièrement publiées des informations sur les personnages politiques de son arrondissement. Elle n'aime pas passer par Google pour ses recherches, alors elle l'a apprise par cœur. Sait-on jamais, ça pourrait éviter les mouchards. Ouvrant un deuxième onglet, elle entre également l'adresse de no-log, sa boîte mail, et s'y connecte. Nickel, il est là ! Le document concernant les comptes bancaires en Suisse de la mairesse de son arrondissement, Mme Alavoine ! Bea télécharge aussitôt le document et l'ouvre dans l'éditeur de texte. Elle le parcourt rapidement, et supprime quelques informations qu'il vaut mieux ne pas laisser. Après avoir entré son identifiant et son mot de passe pour se connecter au blog, Bea copie-colle le contenu du document depuis sa boîte mail, et clique sur Envoyer. *« Espérons que cela inspire d'autres personnes ! »*

Satisfaite d'avoir pu enfin envoyer son document, Bea se relève aussitôt et rend sa place à Ana.

— *« On va se prendre un café ? »*

Novembre 2010. Siège social de La Reboute

En arrivant au bureau, Sarah Ahmed, PDG de La Reboute, commence par éplucher le courrier reçu en buvant son café. Une convocation au commissariat. Pour une fois, il y a autre chose que des factures ! Sans doute une erreur ou une enquête de voisinage ?

Sarah ne pense pas avoir quoi que ce soit à se reprocher, alors inutile de s'inquiéter. Elle se rend donc au commissariat le jour de sa convocation.

— *« Mme Ahmed ? Bonjour, nous voudrions vous poser quelques questions concernant une plainte pour diffamation… »*

Plus tard le même jour. Bureau d'Ana

— *« Allô, ressources humaines de La Reboute, Ana j'écoute.*
— *Bonjour, Mme Ahmed à l'appareil. Écoutez, je viens de passer deux heures au poste de police. J'ai été interrogée quant à des documents bancaires publiés sur Internet et concernant une certaine Mme Alavoine, mairesse du 10^{e}, dont j'ignorais l'existence jusqu'alors. En plus de ça, lors de mon audition, elles m'ont présenté un papier les autorisant à faire une perquisition aux bureaux rue Jaurès.*
— *Quelle histoire ! Mais quel rapport avec nos bureaux ?*
— *Eh bien c'est également pour ça que je vous appelle. Elles affirment qu'elles ont toutes les preuves comme quoi ces documents ont été publiés depuis vos bureaux. Je leur ai dit que ce n'était pas moi, que je ne voyais*

pas de quoi elles parlaient. Elles ont fait des recherches, contacté je ne sais qui. Mais elles disent qu'une enquête a été ouverte, et qu'elle ira jusqu'au bout. Qu'elles retrouveront les responsables. Autant vous dire que je ne suis pas franchement rassurée. J'espère bien que vous n'y êtes pour rien et qu'il s'agit d'une regrettable erreur.

— *Honnêtement, j'en suis la première étonnée, je ne vois absolument pas ce que j'aurais à voir là-dedans, ni ce dont il s'agit.*

— *J'espère bien... Enfin bref, c'est à la police de faire son travail désormais. Je vous rappellerai si j'ai des nouvelles de leur part.*

— *D'accord, je ferai de même si elles appellent ici.*

— *Au revoir. »*

Ana repose le combiné, hébétée. Se gratte la tête. Mais qu'est-ce donc que cette histoire de documents bancaires ? Qui aurait pu faire ça ?

Commissariat central de Paris, quelques semaines plus tard

— *« Commissaire Marta ?*

— *Elle-même.*

— *Officière Neus à l'appareil. Je vous appelle à propos de l'affaire Alavoine. On a eu un email des collègues de la technique et scientifique qui travaillent sur les ordinateurs saisis. Et on a du neuf.*

— *Allez-y, Neus. Je vous écoute.*

— *Apparemment, les collègues ont fini par retrouver le document sur le poste de travail d'une certaine Ana. Il a été téléchargé depuis le navigateur web, et modifié. Il y aurait eu une connexion à une boîte mail chez Gmail, ainsi qu'une autre adresse mail, chez no-log cette fois-ci, peu de temps avant la publication des documents incriminés.*

— *Ah, très bien. On sait qui convoquer pour un interrogatoire alors ! Mais comment avoir des preuves ?*

— *On va demander à Gmail ainsi qu'à no-log les informations sur ces adresses email. À partir de là, on aura sans doute des éléments, ou au moins de quoi poser les bonnes questions !*

— *Bien, Neus. Très bien. De mon côté, je contacte la proc'. Et tenez-moi au courant dès qu'il y a du neuf.*

— *Bien, commissaire. Bonne journée. »*

Voilà pour la mise en contexte. Cette petite histoire fictive pourra en rappeler d'autres, bien plus réelles. L'idée était simplement de montrer combien il est facile et rapide de *s'exposer* lors de la moindre connexion à Internet, et cela sans qu'aucune forme de surveillance ciblée ne soit nécessaire.

Un des objectifs de ce second tome est d'apporter des éclaircissements sur les traces numériques qui permettraient de remonter jusqu'à Ana et Bea. Puis de baliser quelques pistes pour se protéger des attaques — ciblées ou non.

Chapitre 26

Bases sur les réseaux

Internet, ce n'est pas un espace virtuel, un nuage d'information abstrait où l'on trouve tout et n'importe quoi. En tout cas ce n'est pas seulement cela.

Ce qu'on appelle Internet est avant tout un ensemble de réseaux[1]. Des millions de réseaux, agrégés sur plusieurs décennies et, de façon plus ou moins chaotique, gérés aussi bien par des entreprises, des universités, des gouvernements, des associations que des particuliers ; des millions d'ordinateurs et de matériaux de tous types, reliés entre eux par des technologies très diverses, allant du câble de cuivre à la fibre optique en passant par le sans-fil.

Mais pour nous, derrière notre petit écran, Internet c'est avant tout ce qu'il nous permet de faire : visiter des sites web, envoyer des emails, tchatter avec des gens ou télécharger des fichiers. De nouvelles applications apparaissent en permanence et seule l'imagination humaine semble en limiter les possibles.

Comprendre comment fonctionne Internet et comment se protéger, c'est décortiquer cette complexité afin de comprendre comment ces ordinateurs communiquent entre eux ; mais aussi comment fonctionnent les diverses applications que l'on utilise.

26.1 Des ordinateurs branchés entre eux

Assez tôt dans l'histoire de l'informatique, il est apparu nécessaire, notamment dans le travail universitaire et dans le domaine militaire, de faire en sorte que des ordinateurs puissent partager des ressources ou des informations — et ce, à des distances de plus en plus grandes. Ainsi sont nés les réseaux informatiques. On a d'abord relié des ordinateurs les uns aux autres dans un lieu restreint — généralement une université, une entreprise ou un site militaire —, puis on a relié ces lieux entre eux. Aux États-Unis, à la fin des années 1960, est créé ARPANET (*Advanced Research Projects Agency Network*), un réseau qui reliait les universités dans tout le pays. Pour sa mise en place et son amélioration ont été inventées une bonne partie des techniques utilisées aujourd'hui avec Internet. La naissance d'Internet est liée à celle des logiciels libres, et il fonctionne selon des principes similaires d'ouverture et de transparence[2], ce qui n'empêche pas qu'au départ il a été développé pour répondre à des besoins militaires.

Les différents réseaux informatiques ont été interconnectés, constituant ainsi Internet, qui se développe de façon importante depuis les années 1990.

---

1. Pour une explication en cinq minutes : Rémi explique, 2015, *Internet ! Comment ça marche ?* [https://www.youtube.com/watch?v=dCknqcjcItU]. Pour une explication détaillée en quatre heures : Benjamin Bayart, 2012, *Qu'est-ce qu'Internet ? – Cycle de conférences à Sciences Po* [https://www.fdn.fr/actions/confs/qu-est-ce-qu-internet/].

2. Selon Benjamin Bayart, « on ne peut pas dissocier Internet et logiciel libre » car ils sont apparus aux mêmes dates, avaient les mêmes acteurs, une croissance et un fonctionnement similaires. Benjamin Bayart, 2007, *Internet libre, ou Minitel 2.0 ?*, conférence aux 8es rencontres mondiales du logiciel libre, Amiens [https://www.fdn.fr/actions/confs/internet-libre-ou-minitel-2-0/].

De plus en plus d'objets — dont la fonction première n'est pas d'être un ordinateur — sont connectés à Internet : des caméras de surveillance[3], des radars routiers[4], des bornes PMU[5], des télés[6], des frigos[7], des équipements médicaux[8], des jouets pour enfants[9], des voitures[10], *etc.* Certaines personnes parlent même d'*Internet of Shit*[11] (« l'Internet des objets de merde ») afin de montrer l'absurdité de nombre d'objets qui font leur entrée sur Internet.

26.1.1 Un réseau d'ordinateurs

« Un réseau est un ensemble de nœuds [...] reliés entre eux par des liens »[12]. Dans un réseau informatique, les nœuds sont des ordinateurs. C'est donc un ensemble d'ordinateurs reliés entre eux par des câbles, des ondes, *etc.*

page 15

Les ordinateurs qui font partie des réseaux ne ressemblent pas tous aux ordinateurs personnels, fixes ou portables, que l'on utilise en général. Certains sont en effet spécialisés pour assurer des fonctions particulières au sein du réseau. Ainsi, la « box » qui permet à la plupart d'entre nous d'accéder à Internet est un petit ordinateur ; de même, les serveurs sur lesquels sont enregistrés les sites web sont aussi des ordinateurs. D'autres types d'ordinateurs spécialisés pourraient encore être ajoutés à cette liste : on en découvrira certains dans les pages qui viennent.

page ci-contre

26.1.2 Carte réseau

Malgré leurs différences, tous les ordinateurs connectés à un réseau ont nécessairement un point commun : en plus du matériel minimum qui compose un ordinateur, ils doivent disposer d'au moins un périphérique qui sert à se connecter au réseau. On l'appelle *carte réseau*. Elle permet d'établir le lien avec d'autres ordinateurs. De nos jours, plusieurs cartes réseau sont souvent intégrées dans tout ordinateur personnel (une carte réseau filaire et une carte Wi-Fi par exemple).

page 15

page 20

page ci-contre

Chaque carte réseau possède une adresse matérielle, qui l'identifie de façon plus ou moins unique. Dans la technologie filaire domestique, appelée Ethernet, comme dans la technologie sans-fil *Wi-Fi*, cette adresse matérielle est appelée *adresse MAC*. L'adresse MAC livrée avec la carte est conçue pour que la probabilité que deux cartes réseau possèdent la même adresse matérielle soit très faible[13], ce qui n'est pas sans poser problème en matière d'anonymat, comme nous le verrons plus loin.

page 215

3. Jérôme G., 2012, *Caméras IP : faille du voyeur comblée*, Génération-NT [https://www.generation-nt.com/actualites/camera-ip-trendnet-faille-securite-voyeur-1539071].

4. Korben, 2013, *Les radars pédagogiques à la merci des pirates ?* [https://korben.info/les-radars-pedagogiques-a-la-merci-des-pirates.html].

5. Ouest-France avec AFP, 2020, *Paris. Il piratait les bornes de jeux de grattage du PMU et de la FDJ dans les bars* [https://www.ouest-france.fr/societe/faits-divers/paris-il-piratait-les-bornes-de-jeux-de-grattage-du-pmu-et-de-la-fdj-dans-les-bars-6949018].

6. Fabien Soyez, 2013, *Vie privée : télé connectée, l'espion parfait*, CNET France [https://www.cnetfrance.fr/news/vie-privee-tele-connectee-l-espion-parfait-39793195.html].

7. Camille Kaelblen, 2016, *Votre frigo connecté est-il la porte d'entrée idéale pour les hackers ?*, RTL [https://www.rtl.fr/culture/futur/votre-frigo-connecte-est-il-la-porte-d-entree-ideale-pour-les-hackers-7785045780].

8. Gilles Halais, 2012, *Un hacker a trouvé comment pirater à distance les pacemakers*, Franceinfo [https://www.francetvinfo.fr/sciences/un-hacker-a-trouve-comment-pirater-a-distance-les-pacemakers_1631785.html].

9. Sandrine Cassini, 2015, *Les jouets VTech victimes d'un piratage*, Le Monde [https://www.lemonde.fr/economie/article/2015/12/01/les-jouets-vtech-victimes-d-un-cybercriminel_4821275_3234.html].

10. Paul Ackermann, 2015, *Une voiture piratée à distance par des hackers*, HuffPost [https://www.huffingtonpost.fr/2015/07/22/voiture-pirate-distance-hackers_n_7846132.html].

11. Guillaume Ledit, 2017, *Sur Twitter, « Internet of Shit » ridiculise l'Internet des objets… merdiques*, Usbek & Rica [https://usbeketrica.com/article/sur-twitter-internet-of-shit-ridiculise-l-internet-des-objets-merdiques].

12. Wikipédia, 2014, *Réseau informatique* [https://fr.wikipedia.org/wiki/R%C3%A9seau_informatique].

13. Une adresse MAC se présente sous la forme d'une suite de 12 chiffres hexadécimaux (de `0` à `9`, puis `a` pour 10, `b` pour 11, et ainsi de suite jusqu'à `f` pour 15) comme par exemple `00:3a:1f:57:23:98`.

26.1.3 Différents types de liens

Les façons les plus courantes de connecter des ordinateurs personnels en réseau sont soit d'y brancher un câble, que l'on appelle câble Ethernet, soit d'utiliser des ondes radio, avec le *Wi-Fi*.



Un connecteur Ethernet standard RJ-45

Mais au-delà de notre prise téléphonique, nos communications sur Internet sont transportées par bien d'autres moyens. Il existe de nombreux supports pour transmettre l'information : câble de cuivre, fibre optique, ondes radio, *etc.* De la transmission par modem[14] des années 1990 à la fibre optique[15] utilisée pour les connexions intercontinentales, en passant par l'ADSL[16] des années 2000, chacun d'eux a des caractéristiques différentes, notamment en termes de débit d'information (également appelé *bande passante*) et de coût d'installation et d'entretien.

Ces différentes technologies n'ont pas les mêmes faiblesses vis-à-vis de la confidentialité des communications qu'on leur confie ou des traces qu'elles laissent : il sera ainsi plus facile d'intercepter à distance un signal radio diffusé à la ronde que de la lumière qui passe à l'intérieur d'une fibre optique.

26.2 Protocoles de communication

Pour que des machines puissent se parler, il ne suffit pas qu'elles soient reliées entre elles, il faut aussi qu'elles parlent une langue commune. On appelle cette langue un *protocole de communication*. La plupart des « langues » utilisées par les machines sur Internet sont définies de façon précise dans des documents publics[17] : c'est ce qui permet à des réseaux, à des ordinateurs et à des logiciels variés de fonctionner ensemble, pour peu qu'ils respectent ces standards. C'est ce que recouvre la notion d'*interopérabilité*.

Différents protocoles répondent à différents besoins : le téléchargement d'un fichier, l'envoi d'un email, la consultation d'un site web, *etc.*

Pour simplifier, nous détaillerons ci-dessous ces différents protocoles en les classant en trois catégories : protocoles physiques, réseau, puis applicatifs[18].

---

14. « Modem » est le mot condensé de *modulateur-démodulateur* : il permet de transmettre des données numériques sur un canal permettant de véhiculer du son, comme par exemple une ligne téléphonique.

15. Une fibre optique est un fil constitué d'un matériau transparent permettant de transmettre des données sous forme d'impulsions lumineuses. Cela permet la transmission d'importants volumes d'information, même sur de longues distances.

16. L'ADSL (pour *Asymmetric Digital Subscriber Line*) ou VDSL (pour *Very-high-bit-rate Digital Subscriber Line*) est une technologie permettant de transmettre des données numériques sur une ligne téléphonique de manière indépendante du service téléphonique.

17. Ces documents publics sont des *Request For Comments*. Le site Commentcamarche explique très bien le concept de RFC. Jean-François Pillou, 2011, *Les RFC*, CommentCaMarche [https://web.archive.org/web/20210219111153/https://www.commentcamarche.net/contents/533-les-rfc].

18. En réalité c'est un peu plus compliqué. Pour plus de détails voir : Wikipédia, 2017, *Suite des protocoles Internet* [https://fr.wikipedia.org/wiki/Suite_des_protocoles_Internet].

Et afin de bien comprendre, quoi de mieux qu'une analogie ?

Comparons donc le voyage de nos informations à travers Internet à l'acheminement d'une carte postale, dont les étapes, du centre de tri postal à la boîte aux lettres, correspondraient aux différents ordinateurs traversés.

26.2.1 Les protocoles physiques

Afin de livrer notre courrier à bon port, plusieurs moyens de transport peuvent être utilisés successivement : avion, bateau, camion, ou encore bicyclette.

Chacun de ces moyens obéit à un certain nombre de règlements : code de la route, aiguillage aérien, droit maritime, *etc.*

page préc.

De même, sur Internet, les diverses technologies matérielles présentées précédemment impliquent l'usage de différentes conventions. On parle dans ce cas de *protocoles physiques*.

26.2.2 Les protocoles réseau

Savoir naviguer n'est pas suffisant pour acheminer notre carte postale. Il faut également savoir lire un code postal et posséder quelques notions de géographie pour atteindre la destinataire, ou du moins le centre de tri le plus proche.

C'est là qu'interviennent les *protocoles réseau* : leur but est de permettre l'acheminement d'informations d'une machine à une autre, parfois très éloignées, indépendamment des connexions physiques entre ces machines.

page 202

Le protocole réseau le plus connu est le protocole IP.

26.2.3 Les protocoles applicatifs

page 209

On se sert souvent d'Internet pour accéder au web, c'est-à-dire un ensemble de pages accessibles sur des serveurs, que l'on consulte à partir d'un navigateur web : *https://guide.boum.org* est un exemple de site web. Les applications web utilisent un protocole nommé *HTTP*, dont la version chiffrée et authentifiée est *HTTPS*. Le langage courant confond fréquemment le web avec Internet, avec des expressions comme « aller sur Internet » par exemple. Or, le web n'est qu'un des nombreux usages d'Internet.

Il existe en fait de très nombreuses applications qui utilisent Internet, que la plupart des internautes n'ont pas conscience d'utiliser. Outre le web, on peut ainsi citer le courrier électronique, la messagerie instantanée, le transfert de fichiers, les crypto-monnaies, *etc.*

Ainsi, vous pourrez rencontrer ces différents protocoles qui, s'ils utilisent Internet, ne sont *pas* du web :

- *SMTP*, *POP*, *IMAP* sont des protocoles utilisés dans la messagerie électronique [19], dont il existe également des versions chiffrées et authentifiées (*SMTPS*, *POPS*, *IMAPS*) ;
- *Skype*, *Signal*, *IRC* et *XMPP* sont des protocoles utilisés dans la messagerie instantanée ;
- *BitTorrent* est un protocole de partage de fichiers en pair à pair.

En fait, une personne qui a des connaissances suffisantes en programmation peut créer elle-même un nouveau protocole et donc une nouvelle application d'Internet.

page 202

cette page

Chaque application d'Internet utilise ainsi un langage particulier, appelé *protocole applicatif*, et met ensuite le résultat dans des « paquets » qui sont transmis par les protocoles réseau d'Internet. On peut comparer le protocole applicatif à la langue dans

19. Il existe une différence notable dans les protocoles employés, qui a des conséquences en termes de confidentialité et d'anonymat, selon qu'on utilise une boîte mail par le biais de son navigateur web (webmail) ou par le biais d'un client de messagerie. Tout cela sera développé plus loin [page 290].

laquelle on écrit le texte d'une carte postale : il faut que l'expéditrice et la destinataire comprennent cette langue. Cependant, la Poste n'a pas besoin d'y comprendre quoi que ce soit, tant que la lettre contient une adresse valide.

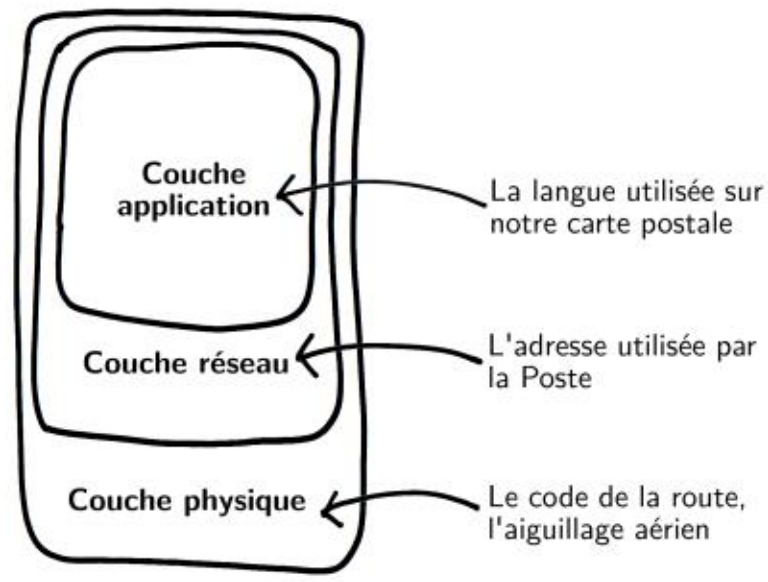
En général, les cartes postales ne sont pas mises dans des enveloppes : n'importe qui sur la route peut les lire. De même, la source et la destination écrites dans l'en-tête des paquets sont lisibles par quiconque. Il y a aussi beaucoup de protocoles applicatifs qui ne sont pas chiffrés : le contenu des paquets est dans ce cas lui aussi lisible par quiconque. page 47

Les protocoles applicatifs ne sont pas tous transparents. Si beaucoup d'entre eux sont définis par des conventions ouvertes et accessibles (et donc vérifiables par les personnes qui le souhaitent), certaines applications utilisent des protocoles propriétaires pas ou peu documentés. Il est alors difficile d'analyser les éventuelles informations sensibles que contiendraient les données échangées. Par exemple, *Skype* fonctionne comme une véritable boîte noire, qui fait ce qu'on veut (communiquer), mais possiblement beaucoup d'autres choses : il a été notamment découvert que le contenu des messages est analysé et éventuellement censuré [20] et que toutes les adresses web qui sont envoyées *via* la messagerie sont transmises à Microsoft [21]. page 39

26.2.4 Encapsulation

En réalité, différents protocoles sont employés simultanément lors d'une communication, chacun d'entre eux ayant un rôle dans l'acheminement des informations.

Il est courant de représenter ces différents protocoles en couches qui se superposent.



Des protocoles encapsulés

De fait, lorsqu'on communique par courrier, notre communication se base sur l'écriture (dans une certaine langue), puis sur l'acheminement par la Poste, qui s'appuie elle-même sur différents moyens de transport.

De manière similaire, une application d'Internet utilisera un *protocole applicatif* précis, sera aiguillée grâce à l'usage de *protocoles réseau*, et parcourra les différentes infrastructures en respectant les *protocoles physiques* en vigueur.

On parle d'*encapsulation* (l'action de « mettre dans une capsule ») : les protocoles applicatifs sont encapsulés dans les protocoles réseau, qui sont à leur tour encapsulés dans les protocoles physiques.

---

20. Ryan Gallagher, traduit par Cécile Dehesdin, 2013, *« Lance des œufs », « cinéma coquin »… La liste des mots surveillés par Skype en Chine*, Slate.fr [https://www.slate.fr/monde/69269/tom-skype-surveillance-chine-espionnage-liste-noire].

21. Jürgen Schmidt, 2013, *Skype's ominous link checking : Facts and speculation*, The H [http://www.h-online.com/security/features/Skype-s-ominous-link-checking-Facts-and-speculation-1865629.html] (en anglais).

26.2.5 Plus de détails sur le protocole IP

Il est intéressant de remarquer que, contrairement aux protocoles physiques et applicatifs, les protocoles réseau sont relativement universels. Les protocoles physiques évoluent au gré des avancées technologiques, filaires ou sans-fil. Les protocoles applicatifs évoluent avec le développement de nouvelles applications : web, email, chat, *etc.* Entre ces deux niveaux, pour savoir par où passer et comment acheminer nos paquets à travers les millions de réseaux d'Internet, tout passe depuis les années 1980 par le protocole *IP* : *Internet Protocol*.

Paquets

Dans le protocole IP, les informations à transmettre sont découpées et emballées dans des *paquets*, sur lesquels sont écrites notamment l'adresse d'expédition et celle de destination. Cette « étiquette » sur laquelle sont écrites les informations utiles à l'acheminement des paquets, à l'aller comme au retour, est appelée l'*en-tête* du paquet. Les paquets d'informations sont ensuite transmis indépendamment les uns des autres, parfois en utilisant différents chemins, puis réassemblés une fois arrivés à destination.

En complément du protocole IP, il existe deux protocoles : *TCP* (*Transmission Control Protocol*) et *UDP* (*User Datagram Protocol*). TCP a été conçu pour transmettre des paquets sans perdre de données, en prenant le temps de tout vérifier. UDP assure la vitesse des échanges sans vérifier que les paquets arrivent à destination ; il est en particulier utilisé pour la vidéo- ou l'audio-conférence.

Adresse IP

Pour que cela fonctionne, tout ordinateur connecté au réseau doit avoir une adresse, qui est utilisée pour lui envoyer des paquets : l'*adresse IP*. Cette adresse doit être unique au sein d'un réseau. En effet, si plusieurs ordinateurs du réseau avaient la même adresse, le réseau ne pourrait pas savoir à quel ordinateur envoyer les paquets.

On peut comparer l'adresse IP à un numéro de téléphone : chaque poste téléphonique doit avoir un numéro de téléphone pour qu'on puisse l'appeler. Si plusieurs postes téléphoniques avaient le même numéro de téléphone, il y aurait un problème.

Les adresses utilisées depuis les débuts d'Internet se présentent sous la forme de quatre nombres de 0 à 255, séparés par un point : on parle d'adresses IPv4 (*Internet Protocol version 4*). Une adresse IPv4 ressemble à : `203.0.113.12`.

Le protocole IPv4 a été défini au début des années 1980 et il permet d'attribuer au maximum 4 milliards d'adresses. À cette époque, on n'imaginait pas qu'Internet serait un jour accessible au grand public, et on pensait que 4 milliards, ce serait suffisant.

Dans les années 1990, pour faire face à la pénurie d'adresses qui s'annonçait, l'IETF [22] a commencé à travailler sur IPv6 (*Internet Protocol version 6*). Depuis 2011 la pénurie est une réalité et il est difficile pour de nouveaux opérateurs d'obtenir des adresses IPv4. Le protocole IPv6 est donc progressivement déployé chez les opérateurs (même s'il y a des récalcitrants). La mise en place d'IPv6 implique des enjeux politiques considérables [23], mais aussi de nouvelles problématiques de sécurité [24]. En 2022, les deux protocoles (v4 et v6) fonctionnent en parallèle. Une adresse IPv6 ressemble à : `2001:0db8:85a3:0000:0000:8a2e:0370:7334`.

---

22. Wikipédia, 2016, *Internet Engineering Task Force* [https://fr.wikipedia.org/wiki/Internet_Engineering_Task_Force].

23. Dans cette conférence [https://ldn-fai.net/intranet-ipv4-ou-internet-ipv6/], LDN explique les enjeux du basculement vers IPv6.

24. Cette nouvelle norme pose de nouveaux problèmes vis-à-vis de notre anonymat en ligne. Florent Fourcot, 2011, *IPv6 et conséquences sur l'anonymat*, LinuxFr.org [https://linuxfr.org/users/ffourcot/journaux/ipv6-et-cons%C3%A9quences-sur-lanonymat]. À suivre, donc…

L'adresse IP est une information extrêmement utile pour quiconque cherche à surveiller ce qui se passe sur un réseau, car elle identifie un ordinateur du réseau de façon unique à un instant donné, sans pour autant être une preuve réelle[25] contre une personne (car un ordinateur peut être utilisé par plusieurs personnes). Elle peut néanmoins indiquer l'origine géographique d'une connexion, donner des indices, amorcer ou confirmer des suspicions.

26.2.6 Port

On peut utiliser de nombreuses applications simultanément à partir d'un même ordinateur : lire ses emails dans le gestionnaire d'emails Thunderbird, regarder le site web de la SNCF, tout en tchattant avec ses potes par messagerie instantanée en écoutant de la musique en ligne. Chaque application doit recevoir seulement les paquets qui lui sont destinés et qui contiennent des messages dans une langue qu'elle comprend. Or, il arrive qu'un ordinateur connecté au réseau n'ait qu'une seule adresse IP. On ajoute donc à cette adresse un numéro qui permet à l'ordinateur de faire parvenir le paquet à la bonne application. On écrit ce numéro sur le paquet, en plus de l'adresse : c'est le numéro de *port*.

Pour comprendre, comparons notre ordinateur à un immeuble : l'immeuble n'a qu'une seule adresse, mais abrite de nombreux appartements, et différentes personnes. Le numéro d'appartement inscrit sur une enveloppe permet de faire parvenir le courrier à la bonne destinataire. Il en est de même pour les numéros de port : ils permettent de faire parvenir les données à la bonne application.

Certains numéros de port sont assignés, par convention, à des applications particulières. Ainsi, quand notre navigateur web veut se connecter à un serveur web, il sait qu'il doit toquer au port 80 (ou 443 dans le cas d'une connexion chiffrée). De la même façon, pour livrer un email, notre ordinateur se connectera en général au port 25 du serveur (ou 465 s'il s'agit d'une connexion chiffrée). page 209

Sur l'ordinateur qu'on utilise, chaque application connectée à Internet ouvre au moins un port, que ce soit un navigateur web, un logiciel de messagerie instantanée, un lecteur de musique, *etc.* Ainsi, le nombre de ports ouverts dans le cadre d'une connexion à Internet peut être très élevé, et fermer son navigateur web est souvent loin d'être suffisant pour couper toute connexion au réseau…



Précision

Plus il y a de ports ouverts, plus il y a de points par lesquels des personnes malintentionnées ou des virus peuvent tenter de s'infiltrer dans un ordinateur connecté au réseau. C'est le rôle habituellement dévolu aux *pare-feux* (*firewalls* en anglais) que de ne laisser ouverts que certains ports définis dans leur configuration et de rejeter les requêtes allant vers les autres.

26.3 Les réseaux locaux

On peut faire des réseaux sans Internet. D'ailleurs, les réseaux informatiques sont apparus bien avant Internet. Dans les années 1960, des protocoles réseau comme HP-IB[26], ne permettant de connecter qu'un nombre restreint d'ordinateurs, faisaient déjà fonctionner des réseaux *locaux*.

25. Legalis, 2013, *L'adresse IP, preuve insuffisante de l'auteur d'une suppression de données sur Wikipedia* [https://www.legalis.net/actualite/ladresse-ip-preuve-insuffisante-de-lauteur-dune-suppression-de-donnees-sur-wikipedia/].
26. Wikipédia, 2014, *HP-IB* [https://fr.wikipedia.org/wiki/HP-IB].

26.3.1 Le réseau local, structure de base de l'Internet

Quand on branche plusieurs ordinateurs entre eux dans une même maison, école, université, bureau, bâtiment, *etc.*, on parle de *réseau local* (ou LAN, pour *Local Area Network*). Les ordinateurs peuvent alors communiquer entre eux, par exemple pour échanger des fichiers, partager une imprimante ou jouer en réseau.

On peut comparer les réseaux locaux aux réseaux téléphoniques internes de certaines organisations (entreprises, universités, *etc.*).

Ces réseaux locaux sont souvent composés de différents appareils qui communiquent entre eux :



Schéma d'un réseau local

26.3.2 Switch et point d'accès Wi-Fi

Pour relier les machines constituant un réseau local, on les connecte en général chacune à une « multiprise » réseau, que ce soit avec un câble ou par des ondes Wi-Fi. On utilise souvent un « switch », que l'on peut effectivement comparer à une multiprise. Cependant, au lieu de transmettre chaque paquet qui lui arrive à *tous* les ordinateurs branchés, un switch lit l'adresse indiquée sur le paquet pour ne l'envoyer qu'à la bonne prise de destination.

L'équivalent du switch des réseaux filaires s'appelle un « point d'accès » dans le monde sans-fil. Chaque point d'accès possède un nom, qui est diffusé aux environs (c'est la liste des réseaux Wi-Fi qu'affiche notre logiciel réseau).

Pour reprendre notre comparaison, le switch est un peu comme la factrice de quartier, qui va dispatcher le courrier, dans tout le quartier, à chaque destinataire. Pour cela, le switch traite les informations des cartes réseau, identifiées par leur adresse matérielle, branchées sur chacune de ses prises.

page 198

Tout comme l'accès physique à une machine donne beaucoup de possibilités pour récupérer les informations qui s'y trouvent, avoir accès physiquement à un réseau permet, sauf défenses particulières, de se faire passer pour l'une des autres machines de ce réseau. Cela rend possible de collecter beaucoup d'informations sur les communications qui y circulent, en mettant en place une attaque de type *monstre du milieu*. L'accès physique au réseau peut se faire en branchant un câble à un switch, mais aussi *via* un point d'accès Wi-Fi.

page 254

26.3.3 Adressage

Pour que les machines qu'on connecte au réseau puissent communiquer avec le protocole IP, elles doivent avoir chacune une adresse IP. Des logiciels et protocoles ont été développés pour automatiser l'attribution d'adresses IP aux ordinateurs lors du

page 202

branchement à un réseau, comme par exemple les protocoles DHCP [27] en IPv4 ou NDP [28] et SLAAC en IPv6 [29].

Pour fonctionner, le système doit garder en mémoire l'association de telle carte réseau, identifiée par son adresse matérielle, à telle adresse IP. La correspondance entre l'adresse IP et l'adresse matérielle n'est utile que dans ce réseau local. Les adresses matérielles n'ont donc aucune raison technique de circuler sur Internet, mais cela arrive tout de même parfois [30].

page 198

26.3.4 NAT et adresses réservées pour les réseaux locaux

Les organismes de standardisation d'Internet se sont rendu compte dans les années 1990 que le nombre d'adresses IPv4 disponibles n'allait pas être suffisant pour faire face à la croissance rapide du réseau. Pour répondre à ce problème, certaines plages d'adresses ont été réservées pour les réseaux privés et ne sont pas utilisées sur Internet : ce sont les *adresses privées* [31].

page 202

Ainsi, la plupart des « box » Internet assignent aux ordinateurs qui s'y connectent des adresses commençant par `192.168` [32] en IPv4 et par `fe80:` en IPv6. Plusieurs réseaux locaux peuvent utiliser les mêmes adresses IP privées, au contraire des adresses IP sur Internet, qui doivent être uniques au niveau mondial.

Les paquets portant ces adresses ne peuvent pas sortir du réseau privé tels quels. Ces adresses privées ne sont donc utilisées que sur le réseau local. Ainsi, par exemple, une machine peut avoir l'adresse IPv4 `192.168.0.12` sur le réseau local mais, du point de vue des autres machines avec qui elle communiquera par Internet, elle semblera utiliser l'adresse IPv4 de la « box » (par exemple, `203.0.113.48`) : ce sera son *adresse publique*. C'est la « box » qui se charge de modifier les paquets en conséquence, grâce à la *traduction d'adresse réseau* (ou *NAT*, pour *Network Address Translation*).

26.4 Internet : des réseaux interconnectés

Internet signifie *INTERconnected NETworks*, c'est-à-dire « réseaux interconnectés ».

Chacun de ces réseaux est appelé *système autonome* (*Autonomous System* ou *AS* en anglais).

26.4.1 Fournisseurs d'accès à Internet

Le *fournisseur d'accès à Internet* (ou *FAI*) est une organisation offrant une connexion à Internet, que ce soit *via* une fibre optique, des ondes électromagnétiques [33], une ligne téléphonique ou un câble coaxial. En France, les principaux fournisseurs d'accès à Internet commerciaux sont, pour un usage domestique, Bouygues, Orange, Free et SFR. Il existe aussi des FAI associatifs, tels que les membres de la Fédération FDN [34].

Souvent, un FAI opère son propre réseau, auquel sont connectées les « box » des abonnées.

---

27. Utilisé dans les réseaux IPv4, DHCP signifie « protocole de configuration dynamique d'hôte » (*Dynamic Host Configuration Protocol* en anglais).
28. Wikipédia, 2017, *Neighbor Discovery Protocol* [https://fr.wikipedia.org/wiki/Neighbor_Discovery_Protocol].
29. Wikipédia, 2022, *IPv6*, section « Attribution des adresses IPv6 » [https://fr.wikipedia.org/wiki/IPv6#Attribution_des_adresses_IPv6].
30. L'un des cas où l'adresse matérielle circule sur Internet est l'utilisation de portails captifs, dont on parlera plus tard [page 216].
31. En même temps, l'IETF travaillait sur la version 6 du protocole IP [page 202] qui résout le problème de pénurie.
32. Les plages d'adresses privées sont définies par convention dans un document appelé « RFC 1918 ». Elles incluent, en plus des adresses commençant par `192.168`, celles qui commencent par `10` et de `172.16` à `172.31`.
33. Wi-Fi, 4G ou autre…
34. La liste des membres de la Fédération FDN [https://www.ffdn.org/fr/membres].

Pour connecter un réseau local à d'autres réseaux, il faut un *routeur*. C'est un ordinateur dont le rôle est de faire transiter des paquets entre deux réseaux ou plus.

Une « box » que l'on utilise pour raccorder une maison à Internet joue ce rôle de routeur. Elle dispose d'une carte réseau connectée au réseau local, mais aussi d'un modem ADSL ou d'un port fibre connecté au réseau du fournisseur d'accès à Internet : on parle de modem-routeur. Elle fait partie non seulement du réseau local, mais aussi d'Internet : en IPv4, c'est l'adresse IP de la « box » qui est visible depuis Internet sur tous les paquets qu'elle achemine pour les ordinateurs du réseau local. Inversement, en IPv6, toutes les machines connectées au réseau ont des adresses publiques routées et donc font partie d'Internet.

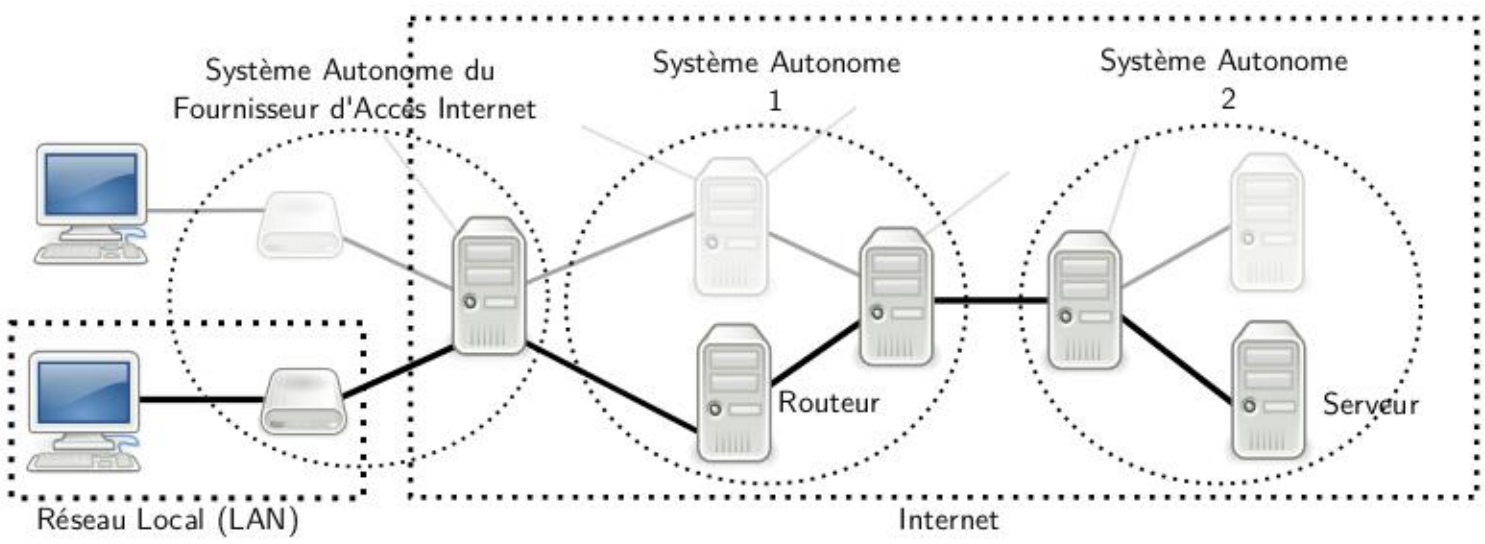
La « box » est un petit ordinateur qui intègre, dans le même boîtier que le modem-routeur, les logiciels permettant la gestion du réseau local (comme le logiciel de page 204 DHCP), ainsi qu'un switch Ethernet et/ou Wi-Fi pour brancher plusieurs ordinateurs mais aussi parfois un décodeur de télévision, un disque dur, *etc.*

26.4.2 Des systèmes autonomes

Un système autonome est un réseau cohérent — généralement sous le contrôle d'une entité ou organisation unique — capable de fonctionner indépendamment des autres réseaux.

En 2022, c'est l'interconnexion de plus de 72 000 AS dans le monde[35] qui forme Internet.

Un système autonome peut typiquement être le réseau d'un fournisseur d'accès à Internet (par exemple Free, SFR ou *tetaneutral.net*). Dans ce cas, chaque « box » qui sert à connecter un réseau local domestique à Internet fait ainsi partie du réseau du fournisseur d'accès, qui est lui-même interconnecté à d'autres systèmes autonomes pour former Internet. Les organisations qui hébergent des services Internet (par exemple Gitoyen[36], Google ou Riseup) et celles qui gèrent les « gros tuyaux » — comme les câbles transatlantiques par lesquels passe une grande partie des flux de données de l'Internet — possèdent aussi leurs propres systèmes autonomes.



Internet est une interconnexion de réseaux autonomes

Ainsi, Internet n'est pas un grand réseau homogène qui serait géré de façon centrale. Il est plutôt constitué d'une multitude de réseaux interconnectés gérés par des organisations et entreprises diverses et variées, chacune ayant son fonctionnement propre.

Tous ces réseaux, infrastructures et ordinateurs ne marchent pas tout seuls : ils sont gérés au quotidien par des personnes, appelées *adminstratrices systèmes et réseaux*,

35. On peut trouver de jolies statistiques sur l'évolution des AS sur le site du CIDR Report [https://www.cidr-report.org/as2.0/] (en anglais).

36. Association qui fournit des services à Globenet [https://www.globenet.org/-Services-.html], à plusieurs membres de la Fédération FDN, et à plusieurs Chatons [https://chatons.org/]. Plus d'informations sur son site [https://gitoyen.org/].

« admins » ou « adminsys »[37]. Les admins s'occupent d'installer, d'entretenir et de mettre à jour ces machines, donc elles ont *nécessairement* accés à beaucoup d'informations.

En termes de surveillance, les intérêts commerciaux et les obligations légales des systèmes autonomes sont très variées en fonction des États et des types d'organisation en jeu (institutions, entreprises, associations, *etc.*). Personne ne contrôle entièrement Internet, et son caractère mondial rend compliquée toute tentative de législation unifiée. Il n'y a donc pas d'homogénéité des pratiques.

Interconnexion de réseaux

De la même façon que l'on a branché notre réseau local au système autonome de notre FAI, celui-ci établit des connexions à d'autres réseaux. Il est alors possible de faire passer des informations d'un système autonome à un autre. C'est grâce à ces interconnexions que nous pouvons communiquer avec les différents ordinateurs formant Internet, indépendamment de l'AS auquel ils appartiennent.



Un routeur

Un routeur est un ordinateur qui relie et fait communiquer plusieurs réseaux. Chez les opérateurs, les routeurs sont allumés en permanence et ils ressemblent davantage à de grosses boîtes de pizza qu'à des ordinateurs personnels ; leur principe de fonctionnement reste cependant similaire à celui des autres ordinateurs, et on leur adjoint quelques circuits spécialisés pour basculer très vite les paquets d'un réseau à un autre.

Les systèmes autonomes se mettent d'accord entre eux pour échanger du trafic ; on parle aussi d'accords de *peering*. Le plus souvent, le *peering* est gratuit, et l'échange est équilibré. Pour joindre les systèmes autonomes avec lesquels il n'a pas d'accord de *peering*, un opérateur peut avoir recours à un fournisseur de transit. Un fournisseur de transit est un opérateur qui sait joindre tout l'Internet et vend de la connectivité aux autres opérateurs[38].



Précision

Il existe un principe qui interdit toute discrimination de trafic ; que ce soit à l'égard de la source, de la destination ou du contenu de l'information transmise sur le réseau. Il s'agit de la *neutralité du Net*. Ainsi, ce principe garantit aux internautes de ne faire face à aucune gestion du trafic Internet qui aurait pour effet de limiter leur accès aux applications et services distribués sur le réseau. Par exemple, limiter la consultation de vidéos en ligne ou le téléchargement. La neutralité du Net assure que les flux d'informations ne sont ni bloqués, ni dégradés, ni favorisés par les opérateurs de télécommunications, permettant ainsi d'utiliser librement le réseau[39]. En France, la Quadrature du Net[40] et la Fédération FDN[41] défendent et promeuvent la neutralité du Net[42].

37. On parlera plus loin d'« admins » pour désigner les administratrices systèmes et réseaux.
38. Loïc Komol, 2013, *Le peering : petite cuisine entre géants du Net*, Clubic [https://www.clubic.com/pro/it-business/article-558086-1-peering-petite-cuisine-geants-web.html].
39. #DataGueule a fait une vidéo [https://peertube.datagueule.tv/videos/watch/64077068-5d05-4815-9095-af63a33a91c4] qui explique clairement la neutralité du Net et les enjeux politiques associés.
40. La neutralité du Net vue par la Quadrature du Net [https://www.laquadrature.net/neutralite_du_net].
41. Principes fondateurs de la Fédération FDN [https://www.ffdn.org/fr/principes-fondateurs].
42. La neutralité du net est définie en droit français dans l'article L33-1 du Code des postes et des communications électroniques [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043545209/].

Des points d'interconnexion...

Avant, les opérateurs réseau tiraient des câbles directement entre leurs routeurs, ce qui faisait beaucoup de câbles, et beaucoup de frais. Ils utilsent désormais des *points d'interconnexion* (*IX* ou *IXP*, pour *Internet eXchange Points*), qui sont des endroits où de nombreux systèmes autonomes sont reliés entre eux. Les opérateurs qui veulent s'y connecter y amènent chacun une fibre et y installent des routeurs. Du fait de la quantité importante de trafic qui passe par ces lieux, ceux-ci sont d'une grande importance stratégique pour les États et autres organisations qui voudraient surveiller ce qui transite par le réseau. [43]

... reliés entre eux

Les grands centres d'interconnexion sont reliés par de gros faisceaux de fibres optiques. L'ensemble de ces liaisons forment les *épines dorsales* (*backbones* en anglais) d'Internet [44].

Ainsi, pour relier l'Europe à l'Amérique, plusieurs faisceaux de fibres optiques courent au fond de l'océan Atlantique. Ces faisceaux de fibres sont autant de points de faiblesse, et il arrive de temps en temps qu'un accident, par exemple une ancre de bateau qui coupe un câble, ralentisse fortement Internet à l'échelle d'un continent [45]. Ça peut paraître étrange, vu qu'historiquement, l'idée d'Internet était d'inspiration militaire : un réseau décentralisé, qui multiplie les liens pour être résistant à la coupure de l'un d'eux.

26.4.3 Routage

Nous avons vu que les ordinateurs s'échangeaient des informations en les mettant dans des paquets.

page 202

Imaginons deux ordinateurs connectés à Internet sur des réseaux différents et qui veulent communiquer. Par exemple, l'ordinateur d'Ana, situé en France, se connecte à celui de Bea, situé au Venezuela.

L'ordinateur d'Ana accède à Internet par sa « box », qui se trouve sur le réseau de son fournisseur d'accès à Internet (ou FAI). L'ordinateur de Bea, lui, fait partie du réseau de son université.

Le paquet destiné à l'ordinateur de Bea arrivera tout d'abord sur le réseau du FAI d'Ana. Il sera transmis au routeur C de son FAI, qui joue le rôle de centre de tri. Le routeur lit l'adresse de l'ordinateur de Bea sur le paquet, et doit décider à qui faire passer le paquet pour qu'il se rapproche de sa destination. Comment s'effectue ce choix ?

Chaque routeur maintient une liste des réseaux auxquels il est connecté. Il envoie régulièrement les mises à jour de cette liste aux autres routeurs auxquels il est branché, ses voisins, qui font de même. C'est grâce à ces listes qu'il peut aiguiller les paquets reçus et les transmettre vers leur destination.

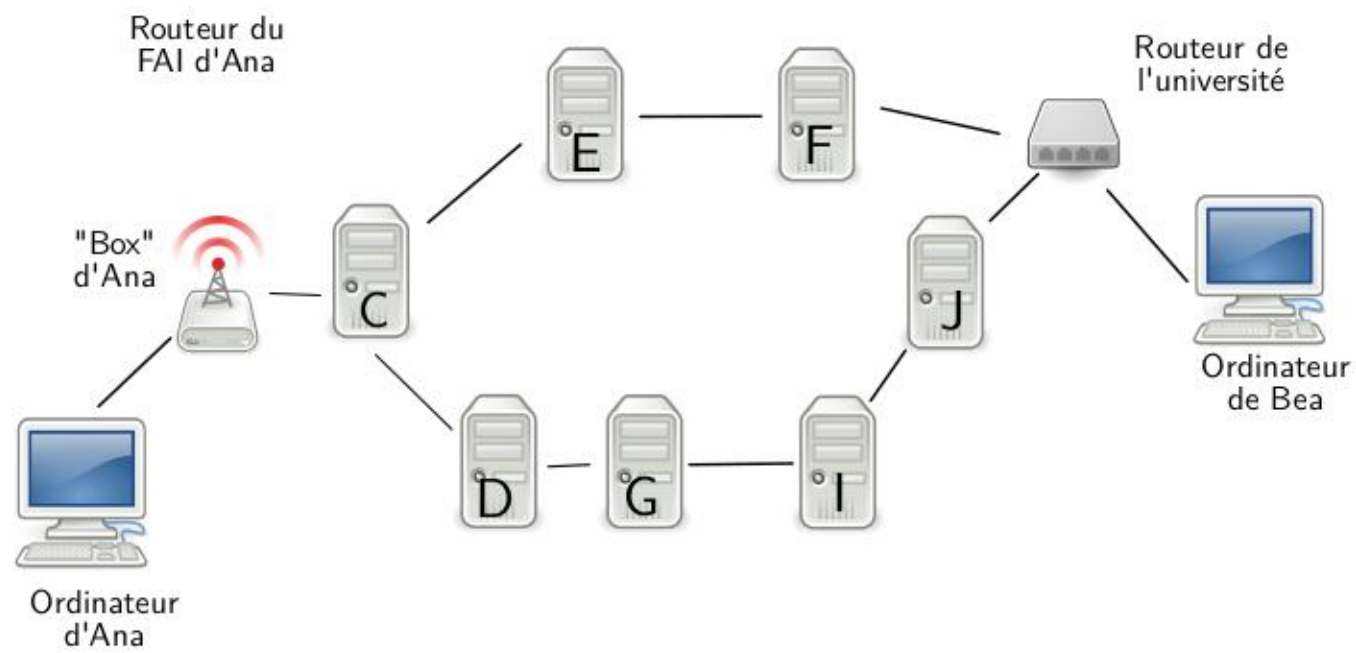
Ainsi, le routeur du FAI d'Ana sait qu'il peut joindre le réseau de l'université de Bea par quatre intermédiaires en envoyant le paquet au routeur D. Mais il peut aussi

---

43. Guillaume Champeau, 2013, *Comment l'Allemagne aussi espionne nos communications*, Numerama [https://www.numerama.com/politique/26279-comment-l-allemagne-aussi-espionne-nos-communications.html].

44. TeleGeography, 2017, *Submarine Cable Map* [https://www.submarinecablemap.com/] (en anglais).

45. Pierre Col, 2009, *Internet, les ancres de bateaux et les séismes sous-marins*, ZDNet [https://www.zdnet.fr/blogs/infra-net/internet-les-ancres-de-bateaux-et-les-seismes-sous-marins-39602117.htm], Cécile Dehesdin, 2013, *Des coupures dans des câbles sous-marins ralentissent Internet dans plusieurs pays*, Slate.fr [https://www.slate.fr/monde/70063/cable-internet-sous-marin-coupe-impact-afrique-egypte].



Routage

l'envoyer par deux intermédiaires, en le passant au routeur E. Il va choisir d'envoyer le paquet à E, qui a un chemin plus direct.

Le paquet arrive ainsi à E, le routeur d'un opérateur de transit, une organisation payée par le FAI d'Ana pour acheminer des paquets. E va faire le même genre de calcul, et envoyer le paquet à F. Le réseau de F comprend des ordinateurs non seulement en Europe, mais aussi en Amérique, reliés par un câble transatlantique. F appartient à une entreprise, similaire à celle qui gère E, qui est payée par l'université de Bea. F envoie finalement le paquet au routeur de l'université, qui l'envoie à l'ordinateur de Bea. Ouf, voilà notre paquet arrivé à destination.

Ainsi, chaque paquet d'information qui traverse Internet passe par plusieurs réseaux. À chaque fois, un routeur joue le rôle de centre de tri, et l'envoie à un routeur voisin. Au final, chaque paquet passe par beaucoup d'ordinateurs différents, qui appartiennent à des organisations nombreuses et variées.

De plus, la topologie du réseau, à savoir son architecture, la disposition des différents postes informatiques ainsi que leur hiérarchie changent au fil du temps.

Lorsque, le lendemain, Ana se connecte de nouveau à l'ordinateur de Bea, les paquets que son ordinateur envoie ne prendront pas nécessairement le même chemin que la veille. Par exemple, si le routeur E est éteint à la suite d'une coupure de courant, le routeur du FAI d'Ana fera passer les paquets par D, qui avait auparavant une route plus longue.

C'est en agissant au niveau du routage que le gouvernement égyptien a fait couper Internet lors de la révolution de 2011. Les routeurs des principaux fournisseurs d'accès à Internet du pays ont cessé de dire aux autres routeurs que c'est à eux qu'il fallait s'adresser pour acheminer les paquets vers les ordinateurs égyptiens[46]. Ainsi, les paquets destinés à l'Égypte ne pouvaient plus trouver de chemin, interrompant de fait l'accès au réseau, le tout sans avoir coupé le moindre câble.

26.5 Des clients, des serveurs

Historiquement, dans les années 1980, chaque ordinateur connecté à Internet fournissait une partie d'Internet. Non seulement il servait à « aller voir des choses sur Internet », mais il proposait également des informations, des données et des services aux autres utilisatrices connectées à Internet : il *faisait* Internet autant qu'il y *accédait*.

46. Stéphane Bortzmeyer, 2011, *Coupure de l'Internet en Égypte* [https://www.bortzmeyer.org/egypte-coupure.html].

Le tableau général est très différent de nos jours. On a vu qu'il existe des ordinateurs allumés en permanence qui se chargent de relier des bouts d'Internet entre eux : les routeurs. De même, il y a une autre catégorie d'ordinateurs allumés en permanence qui, eux, contiennent presque toutes les données et services disponibles sur Internet. On appelle ces ordinateurs des serveurs, car ils *servent* des informations et des services. Ils centralisent la plupart des contenus, que ce soient des sites web, de la musique, des emails, *etc.* Cela induit de la verticalité dans la hiérarchie du réseau. En effet, plus on dispose d'information, au sens large, plus on a potentiellement de pouvoir.

Les serveurs fournissent, contrairement aux clients qui ne font qu'accéder aux informations. Cette situation correspond à un Internet où nos machines ont principalement un rôle de clients, centralisant Internet autour des fournisseurs de contenus [47].

Prenons l'exemple d'un des services disponibles sur Internet, le site web du Guide d'autodéfense numérique [https://guide.boum.org/] : lorsqu'Ana consulte une page de ce site web, son ordinateur joue le rôle de *client*, qui se connecte au *serveur* qui héberge le Guide d'autodéfense numérique.

Cela dit, n'importe quel ordinateur peut être à la fois client et serveur, que ce soit dans un même temps ou successivement. C'est notamment le cas du modèle pair à pair, ou *P2P*, très utilisé pour le partage de fichiers. Dans cette situation, chaque ordinateur, autrement appelé *nœud*, est connecté au réseau et communique en jouant à la fois le rôle de client et celui de serveur. Ces deux usages ne sont pas déterminés par le type de machine.

26.5.1 Les serveurs de noms

Lorsqu'Ana demande à son navigateur web d'aller sur le site du Guide d'autodéfense numérique, son ordinateur doit se connecter au serveur qui héberge ce site.

page 202

Pour cela, il est nécessaire de connaître l'adresse IP du serveur. Or une adresse IP est une suite de nombres assez pénible à mémoriser, à taper ou à transmettre, comme par exemple `88.99.208.38` (pour une adresse IPv4). Pour résoudre ce problème, il existe des serveurs à qui on peut poser des questions telles que : « Quelle est l'adresse IP de *guide.boum.org* ? », comme on chercherait dans l'annuaire téléphonique quel est le numéro d'une correspondante. Ce système s'appelle le DNS (*Domain Name System*, ce qui donne « système de noms de domaine » en français). L'ordinateur d'Ana commence donc, *via* sa « box », par interroger le serveur DNS de son fournisseur d'accès à Internet pour obtenir l'adresse IP du serveur qui héberge le *nom de domaine guide.boum.org*.

L'ordinateur d'Ana reçoit en retour l'adresse IP du serveur et peut donc communiquer avec celui-ci.

26.5.2 Chemin d'une requête web

L'ordinateur d'Ana se connecte alors au serveur du guide (`88.99.208.38`), et lui envoie une requête qui signifie : « Envoie-moi la page d'accueil du site web `guide.boum.org`. » Les paquets qui véhiculent la demande partent de son ordinateur et passent alors par sa « box » pour arriver au routeur de son fournisseur d'accès. Ils traversent ensuite plusieurs réseaux et routeurs (non représentés sur le schéma), pour atteindre enfin le serveur de destination.

page 206

page 217

26.5.3 Le logiciel serveur

Afin d'envoyer à Ana la page web demandée, le serveur recherche alors celle-ci dans sa mémoire, sur son disque dur, ou bien il la fabrique.

---

47. La conférence de Benjamin Bayart *Internet libre, ou Minitel 2.0 ?* [https://www.fdn.fr/actions/confs/internet-libre-ou-minitel-2-0/], donnée aux 8es rencontres mondiales du logiciel libre à Amiens en 2007, explique très bien ce glissement et les enjeux qu'il recouvre.

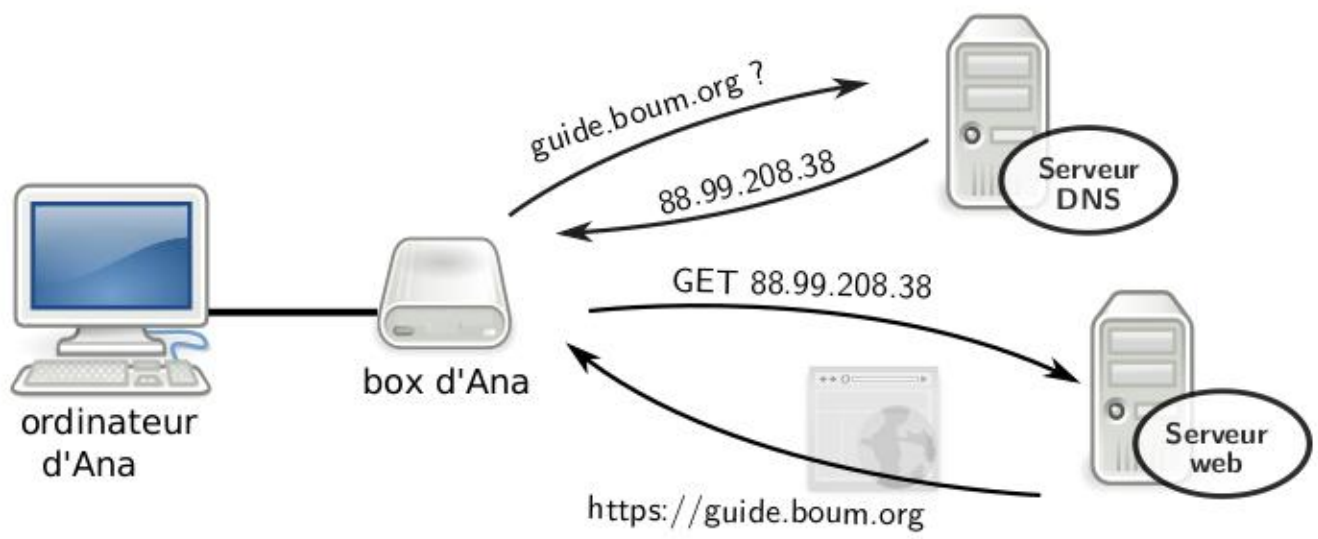


Schéma d'une requête web

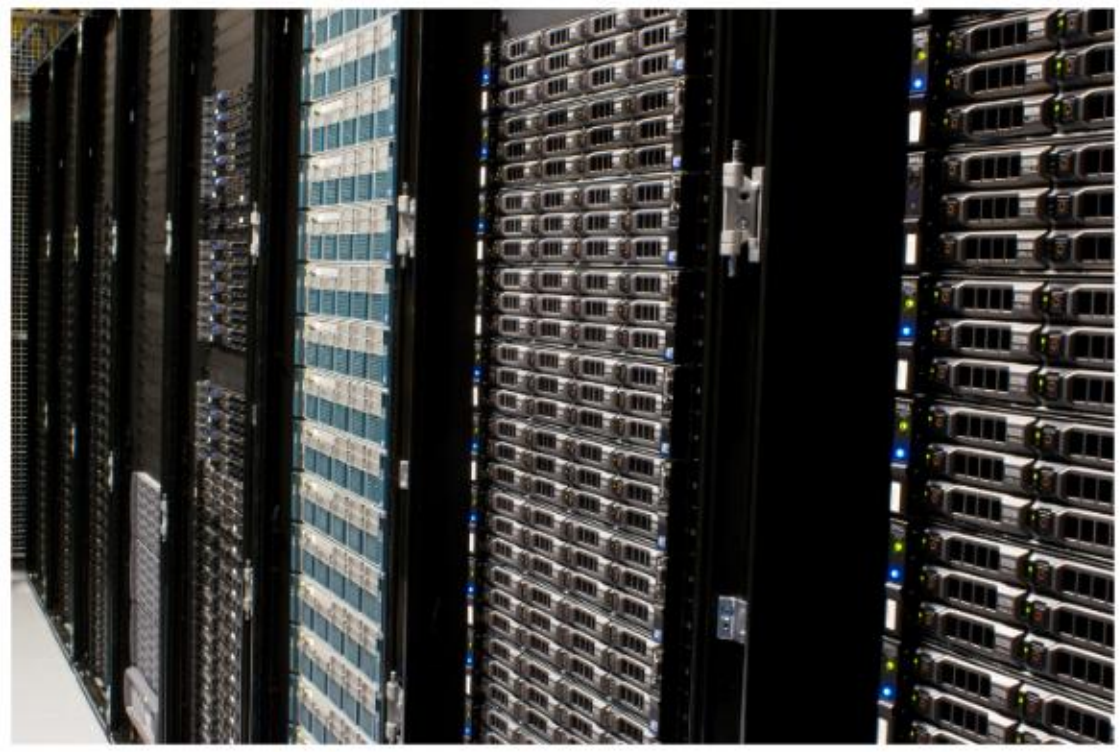
En effet, les pages consultables sur le web n'existent pas forcément sous une forme telle qu'on peut la voir sur notre ordinateur *avant* qu'on ait demandé à y accéder. Elle sont souvent générées automatiquement, à la demande. On parle alors de *sites web dynamiques*, par opposition aux *sites web statiques*, dont les pages sont écrites par avance.

Par exemple, si l'on cherche « ouistiti moteur virtuose » dans un moteur de recherche, celui-ci n'a pas encore la réponse en réserve. Le serveur exécute alors le code source du site pour calculer la page contenant la réponse avant de nous l'envoyer. page 39

Sur le serveur, il y a donc un logiciel qui fonctionne, et qui répond lorsqu'on lui fait une requête. Ce logiciel serveur est spécifique à chaque application : c'est lui qui comprend le protocole applicatif. Dans le présent exemple, ce logiciel recherche et sert à l'ordinateur d'Ana la page web : on l'appelle donc un serveur *web*. page 200

26.5.4 L'hébergement des serveurs

Les serveurs, ordinateurs sur lesquels fonctionnent les logiciels serveurs évoqués précédemment, sont en général regroupés dans des immeubles disposant d'une bonne connexion au réseau et d'une alimentation électrique très fiable : des centres de données (ou *data centers* en anglais). page ci-contre



Une allée de serveurs dans un centre de données

De nos jours, la mode est de parler de *cloud computing* (ou « informatique en nuage » en français). Ce concept « marketing » ne remet pas en cause la séparation entre clients

et serveurs, bien au contraire. Il signifie simplement que les données sont susceptibles d'être déplacées d'un serveur à un autre, pour des raisons légales, techniques ou économiques. Et cela sans que leurs propriétaires en soient nécessairement informées.



Il n'y a pas de cloud, seulement les ordinateurs d'autres personnes



Précision

La société Google possède par exemple au moins une vingtaine de data centers répartis sur trois continents[48] afin d'assurer l'opérabilité de ses services 24 heures sur 24, 7 jours sur 7, même lorsque certains équipements sont indisponibles.

Les hébergeurs de ce type font tourner des centaines de machines physiques réparties dans plusieurs centres de données autour du monde et mettent en commun leur puissance de stockage et de calcul pour en faire une super-machine abstraite. Ensuite, ils vendent des « machines virtuelles », c'est-à-dire des parts de puissance de calcul et de stockage de cette super-machine. L'« Amazon Elastic Compute Cloud » (ou EC2) est l'un des services les plus connus dans ce domaine[49].

Une machine virtuelle peut être déplacée automatiquement en fonction de l'utilisation des machines physiques, de la qualité de leur connexion au réseau, *etc.* Avec une telle infrastructure, il est impossible de savoir à l'avance sur quelle machine physique — et donc précisément à quel endroit — se trouve une machine virtuelle donnée.

Cela rend en pratique impossible d'avoir du contrôle sur nos données[50]. Seront-elles réellement effacées des machines physiques si on les « supprime » ? On a vu dans le premier tome qu'effacer des données sur un ordinateur était quelque chose de compliqué. Ce problème se corse encore plus si nous ne savons pas de quel ordinateur il s'agit. De plus, cela pose des problèmes juridiques : des données légales à un endroit peuvent se retrouver illégales parce que la machine qui les contient ou les sert sur Internet a changé de juridiction.

page 42

Il y a donc eu un glissement d'un Internet où tout le monde consultait et distribuait des données, vers un modèle où les données étaient centralisées sur des machines physiques appelées serveurs, puis aujourd'hui vers le *cloud*, où ces mêmes données peuvent être enregistrées, parfois éparpillées, sur des serveurs indéterminés. Il devient extrêmement compliqué de savoir au final où elles sont réellement stockées, et l'utilisatrice a encore moins de prise sur le devenir de ses données.

48. Google, 2017, *Data center locations* [https://www.google.com/about/datacenters/inside/locations/index.html] (en anglais).
49. Wikipédia, 2014, *Amazon Elastic Compute Cloud* [https://fr.wikipedia.org/wiki/Amazon_Elastic_Compute_Cloud].
50. Jos Poortvliet, 2011, *openSUSE and ownCloud* [https://news.opensuse.org/2011/12/20/opensuse-and-owncloud/] (en anglais).

Chapitre 27

Traces sur toute la ligne

Le fonctionnement *normal* des réseaux implique que de nombreux ordinateurs voient ce que l'on y fait. Il n'est pas question ici de surveillance active. C'est parfois complètement nécessaire à leur fonctionnement. Il arrive aussi que ces informations soient collectées parce que c'est « plus pratique », par exemple pour diagnostiquer des problèmes.

Or, le fonctionnement de n'importe quel ordinateur laisse un certain nombre de traces. C'est le thème du premier tome de ce guide. page 27

Dans le cas d'une utilisation en ligne, ce n'est pas seulement l'ordinateur que l'on a devant les yeux qui peut garder des traces de ce que l'on fait sur le réseau, mais aussi chacun des ordinateurs par lesquels transitent les informations. Or beaucoup de ces informations circulent *en clair*, et non pas de façon chiffrée. page 47

27.1 Sur l'ordinateur client

L'ordinateur utilisé pour se connecter au réseau est appelé client. Cette machine sait tout ce que l'on fait avec et, bien souvent, en conserve des traces. page 209

Comme cela a été longuement expliqué dans le premier tome de ce guide, ces traces, et l'aisance avec laquelle elles peuvent être exploitées, dépendent très largement de l'ordinateur et du système d'exploitation utilisés. page 27

27.1.1 La mémoire des navigateurs web

Pour être plus agréables à utiliser, les navigateurs web enregistrent de nombreuses informations sur les pages que l'on consulte. Voici quelques exemples :

- La plupart des navigateurs web gardent un historique des pages web consultées.
- Ils proposent aussi souvent d'enregistrer ce que l'internaute saisit dans les formulaires qui se trouvent sur certaines pages web, ainsi que les mots de passe des différents comptes en ligne.
- En général, ils enregistrent aussi les pages récemment ou couramment consultées pour en accélérer le chargement : on parle de « mise en cache » [1].

Ce sont autant de données sauvegardées pouvant permettre à la police (entre autres) de retracer notre navigation sur Internet. Souvenons-nous, dans notre histoire du début : page 194

> — *Apparemment, les collègues ont fini par retrouver le document sur le poste de travail d'une certaine Ana. Il a été téléchargé depuis le*

1. Pour voir le contenu du cache du navigateur web Firefox ou du Navigateur Tor, taper `about:cache` dans la barre d'adresse.

> *navigateur web, et modifié. Il y aurait eu une connexion à une boîte mail chez Gmail, ainsi qu'une autre adresse mail, chez no-log cette fois-ci, peu de temps avant la publication des documents incriminés.*

27.1.2 Les cookies

Le mot « cookie » vient de l'anglais « *fortune cookie* », en référence à des gâteaux qui cachent un message sur un petit papier. Un « cookie » est un petit « texte » envoyé par un site web que le navigateur de l'internaute stocke, puis renvoie au site à chaque visite. C'est ce qui permet par exemple aux applications de mail en ligne (« webmail ») ou aux sites commerciaux de se rappeler qu'on est bien authentifiée avec notre adresse et notre mot de passe pendant notre session, ou de mémoriser la langue que l'on désire utiliser.

Les cookies permettent aussi à un site web de pister les personnes qui le visitent.

Ainsi, les régies publicitaires sur Internet incluent, dans les publicités qu'elles affichent sur les sites, des cookies « traceurs » qui permettent de suivre l'internaute dans ses déplacements sur tous les sites qui affichent des publicités en provenance de la même régie publicitaire. Ainsi, elles peuvent « collecter des informations de plus en plus précises sur celle-ci et par conséquent lui proposer une publicité de mieux en mieux ciblée. » [2]

De plus, lorsqu'on consulte des pages web, celles-ci établissent des connexions vers des sites de publicités et souvent vers les mêmes sites, ce qui augmente d'autant plus la possibilité de pistage de la part de ces sites.

Enfin, certains cookies ont une date d'expiration, mais d'autres sont à durée indéfinie — les sites qui nous les auront refilés pourront identifier notre navigateur web pendant des années !

Les cookies classiques sont cependant restreints en termes de volume de données, et faciles à supprimer par une utilisatrice avertie. Aussi ont-ils été « améliorés », par exemple avec le « stockage web local » [3] inclus dans la norme HTML5, qui permet de stocker plusieurs mégaoctets de données dans le navigateur web.

D'autres techniques pour renforcer le pistage consistent à stocker un même cookie à différents emplacements dans le navigateur web et à recréer à chaque visite ceux qui auraient été supprimés (en partant du principe que si chacun peut être supprimé, ils ne le seront pas tous en même temps [4]).

Accepter l'usage de cookies a donc des conséquences en termes de pistage, et cela laisse des traces sur notre ordinateur et sur des serveurs.

27.1.3 Applications côté client

page 39
page 210

Dans l'évolution du web et de ses navigateurs, il est rapidement devenu clair que pour avoir un minimum d'interactivité, il était nécessaire qu'une partie du code source du site web soit exécutée du côté du client, par le navigateur web, et non sur le serveur web qui héberge le site.

Cela a plusieurs aspects pratiques : du côté du serveur web, c'est du travail en moins et des économies sur le matériel. Du côté du client, l'affichage et les fonctionnalités du site web sont accélérées. Cela permet aussi de minimiser le trafic réseau entre le navigateur et le site web : plus besoin de demander une page complète du site web à chaque fois que l'on clique sur un petit bouton, seul un petit fragment de la page doit être transmis.

---

2. CNIL, *La publicité ciblée en ligne* [https://www.cnil.fr/fr/publicite-ciblee-en-ligne-quels-enjeux-pour-la-protection-des-donnees-personnelles].

3. Wikipédia, 2020, *Stockage web local* [https://fr.wikipedia.org/wiki/Stockage_web_local].

4. La bibliothèque JavaScript evercookie [https://samy.pl/evercookie/] (en anglais) est un exemple de ce type de technologies.

Des technologies ont été ajoutées aux navigateurs web pour permettre ces fonctionnalités : JavaScript et Java en sont les principaux représentants.

Mais ces petits plus ont également un coût : comme précisé plus haut, cela signifie que l'autrice d'un site est en mesure d'exécuter le code de son choix sur les ordinateurs des personnes qui le visitent (ce qui pose de nombreux problèmes de sécurité, comme nous l'avons vu dans le premier tome de ce guide). Bien sûr, des protections ont été mises en place au sein des navigateurs web [5], mais elles ne couvrent pas tous les risques et ne remplacent en tout cas pas la vigilance des internautes.

page 32

D'autant que ces technologies ont parfois des fonctionnalités qui, si elles peuvent être utiles, posent question : ainsi WebRTC [6], une technologie qui vise à intégrer aux navigateurs web les communications en temps réel, permet d'accéder au micro et à la caméra de l'ordinateur sur lequel elle est utilisée.

On a vu que placer sa confiance dans un logiciel était un choix complexe. Dès lors, l'exécution de ce genre de programmes pose des questions quant au pouvoir donné aux autrices de sites ou d'applications web d'accéder aux ressources de notre ordinateur, et aux informations qu'il contient.

page 39

De plus, avant d'être exécutés par le navigateur web, ces bouts de code transitent par le réseau, souvent sans aucune authentification. Cela laisse le loisir aux personnes malintentionnées et bien placées de les modifier, tout comme le reste d'une page web. Pour y introduire, par exemple, un logiciel malveillant. Il est aussi possible de jouer avec les données que ces codes doivent traiter pour tenter de détourner leur usage. Ce genre de manipulation de pages web a par exemple été détecté par le passé lors de l'utilisation du point d'accès Wi-Fi d'un hôtel à New York qui utilisait un équipement réseau dédié à cette tâche [7].

page 31

Au final, un navigateur web moderne a tellement de fonctionnalités que d'éventuelles adversaires disposent d'un nombre considérable d'angles d'attaque.

27.1.4 Dans les journaux des logiciels

Le navigateur web n'est pas le seul logiciel à enregistrer des traces sur l'ordinateur utilisé ; la plupart des logiciels ont des journaux.

page 29

Par exemple, les logiciels de messagerie instantanée enregistrent souvent l'historique des conversations ; les logiciels de partage de fichiers en pair-à-pair (comme BitTorrent), eux aussi, ont tendance à se souvenir de ce qu'on a téléchargé récemment ; les logiciels de mail gardent les emails qu'on a téléchargés ; *etc.*

> — *Apparemment, les collègues ont fini par retrouver le document sur le poste de travail d'une certaine Ana. Il a été téléchargé depuis le navigateur web, et modifié.*

Dans notre histoire, les flics ont pu retrouver les traces du document de Bea dans l'historique du navigateur web et du logiciel de traitement de texte de l'ordinateur d'Ana.

27.2 Sur la « box » : l'adresse matérielle de la carte réseau

On a vu que la carte réseau utilisée par tout ordinateur pour se connecter possède une adresse matérielle, ou adresse MAC. Cette adresse est utilisée par les équipements

page 198

5. Il s'agit en général de ne donner accès au code des sites web qu'à des fonctions limitées en l'exécutant dans un « bac à sable » (Wikipédia, 2014, *Sandbox (sécurité informatique)* [https://fr.wikipedia.org/wiki/Sandbox_(s%C3%A9curit%C3%A9_informatique)].

6. Dans le Navigateur Tor, la fonctionnalité WebRTC est désactivée.

7. Justin Watt, 2012, *Hotel Wifi JavaScript Injection* [https://justinsomnia.org/2012/04/hotel-wifi-javascript-injection/] (en anglais).

réseaux pour rediriger un paquet de données vers la bonne carte réseau, lorsque plusieurs ordinateurs sont connectés sur la même « box » par exemple.

Normalement, cette adresse ne sort pas du réseau local. Cependant, on se connecte en général directement à la « box » d'un fournisseur d'accès à Internet — si l'on utilise le partage de connexion d'un téléphone, c'est lui qui jouera le rôle de « box ». Chaque carte réseau connectée à la « box » lui donne donc son adresse matérielle.

page 29

La plupart des « box » gardent un journal (*log*) qui contient ces adresses matérielles, au moins pendant le temps où elles sont allumées. Il est difficile de savoir les types et la quantité d'informations contenues dans ce journal, ainsi que l'existence potentielle de portes dérobées[8] ou de failles de sécurité permettant d'y accéder. En effet, ces

page 22

« box » fonctionnent avec un logiciel installé par le fournisseur d'accès à Internet, qui y garde un accès privilégié, ne serait-ce que pour effectuer les mises à jour du logiciel.

Ainsi, le fournisseur d'accès Orange admet collecter pendant 12 mois les adresses matérielles des ordinateurs qui se connectent sur ses « box », et les adresses IP associées pour la « gestion des diagnostics »[9]. Pour nous, la « box » est donc à considérer comme une véritable boîte noire, dont nous n'avons pas les clés, qui peut connaître (et faire) beaucoup de choses sur le réseau local.



Pour aller plus loin…

Si on aime bidouiller, il est possible de remplacer le modem-routeur du FAI (Fournisseur d'Accès à Internet) par un modem-routeur sous OpenWrt[10] ou plus simplement d'ajouter un routeur sous OpenWrt entre la « box » du FAI et nos ordinateurs. Il en existe des préinstallés et de plus, certains FAI associatifs fournissent des routeurs n'utilisant que des logiciels libres à leurs adhérentes[11].

De plus, lorsque le réseau local inclut l'usage du Wi-Fi, il se peut que de manière plus ou moins accidentelle les adresses matérielles des ordinateurs se connectant à la « box » en Wi-Fi soient enregistrées par d'autres ordinateurs écoutant ce qui « passe dans les airs ». C'est ainsi que les Google Cars, en même temps qu'elles parcouraient des milliers de rues pour établir la carte de Google Street View, en ont profité pour « capturer » les adresses MAC des ordinateurs environnants[12].

Il est par contre possible de changer temporairement l'adresse matérielle d'une carte réseau, afin par exemple de ne pas être pistées avec nos ordinateurs portables[13] lors de nos déplacements.

Il faut aussi mentionner les cas où, avant de pouvoir se connecter à Internet, on doit entrer un *login* et un mot de passe dans son navigateur web : c'est souvent le cas sur les réseaux Wi-Fi publics, que ce soit ceux d'une agglomération, d'une institution ou d'un fournisseur d'accès à Internet (*FreeWifi*, *SFR WiFi public* et autres *Bouygues Telecom Wi-Fi*). On appelle ces pages des *portails captifs*. Dans ce cas, en plus de l'adresse matérielle de la carte Wi-Fi, on donne à l'organisation qui gère le portail l'identité de la personne abonnée correspondant à ces identifiants.

---

8. Un exemple de porte dérobée sur les routeurs d'un constructeur [https://korben.info/backdoor-les-routeurs-d-link.html].
9. Orange, 2021, *Gestion des diagnostics* [https://web.archive.org/web/20210510112139/https://assistance.orange.fr/ordinateurs-peripheriques/installer-et-utiliser/la-securite/risques-et-prevention/les-donnees-personnelles/gestion-des-diagnostics_195036-739979#onglet2].
10. OpenWrt est un système d'exploitation libre pour routeurs. Voici quelques raisons de l'utiliser [https://openwrt.org/fr/reasons_to_use_openwrt].
11. Une liste de modems et routeurs utilisés par les membres de la Fédération FDN : Fédération FDN, 2017, *Modems et routeurs* [https://www.ffdn.org/wiki/doku.php?id=modems-routeurs].
12. Europe 1 avec AFP, 2011, *Street View : la Cnil épingle Google* [https://www.europe1.fr/economie/Street-View-la-Cnil-epingle-Google-309338].
13. Wikipédia, 2014, *Mac Spoofing* [https://fr.wikipedia.org/wiki/Filtrage_par_adresse_MAC#MAC_Spoofing].

27.3 Sur les routeurs : les en-têtes de paquets

Sur le chemin entre un ordinateur et le serveur auquel on souhaite se connecter, il y a de nombreux routeurs, qui relaient les paquets et les envoient au bon endroit. page 206

Pour savoir où envoyer un paquet, ces routeurs lisent une sorte d'enveloppe sur laquelle un certain nombre d'informations sont écrites ; on appelle cette « enveloppe » l'*en-tête* du paquet. page 202

L'en-tête d'un paquet contient de nombreuses informations qui sont nécessaires à son acheminement, et notamment l'adresse IP de la machine destinataire, mais aussi l'IP publique de la machine expéditrice (à qui la réponse devra être envoyée). Le routeur voit donc quel ordinateur veut parler à quel autre ordinateur, de la même manière que la factrice doit avoir l'adresse de la destinataire pour lui transmettre le courrier, ainsi que l'adresse de l'expéditrice pour un éventuel retour.

Les en-têtes contiennent aussi le numéro du port source et celui du port de destination, ce qui peut renseigner sur l'application utilisée. page 203

Pour faire leur travail, les routeurs *doivent* lire ces informations ; ils *peuvent* aussi en garder la trace dans des journaux.

Bien qu'ils n'aient pas de bonne raison de le faire, les routeurs sont aussi en mesure d'accéder à l'*intérieur* de l'enveloppe transportée ; par exemple le contenu de la page web consultée par l'internaute ou celui d'un email envoyé : on parle alors d'examen approfondi des paquets[14] (*Deep Packet Inspection* ou DPI en anglais).

Le fournisseur d'accès à Internet français Orange inclut par exemple dans le contrat de ses abonnées une clause concernant l'usage des « données relatives » à son trafic[15].

27.4 Sur le serveur

Le serveur qui héberge le site visité a accès, comme les routeurs, aux en-têtes des paquets IP et donc à toutes ces informations dont on vient de parler. Il regarde notamment l'adresse IP de la « box » utilisée par l'ordinateur qui se connecte pour savoir à qui envoyer la réponse. page 202

En plus des en-têtes IP, correspondant à la couche réseau de la communication, le serveur lira les en-têtes du protocole applicatif, qui correspondent à la couche applicative de la communication. page 200 page 200

Mais le serveur lit aussi le contenu des paquets eux-mêmes : c'est en effet lui qui doit ouvrir l'enveloppe et lire la lettre pour y répondre. Le logiciel serveur va alors interpréter la lettre reçue, qui est écrite avec le protocole applicatif, pour fournir la réponse adaptée.

Or, de très nombreux protocoles applicatifs véhiculent aussi des informations qui permettent d'identifier l'ordinateur qui se connecte — c'est ce que nous allons voir en détails ici.

Les serveurs ont, comme les ordinateurs clients, des journaux systèmes — on en parlera davantage dans la partie suivante. page 225

27.4.1 Les en-têtes HTTP

Lorsqu'un navigateur web demande une page web, il inclut dans la requête le nom du logiciel, son numéro de version, le système d'exploitation utilisé et la langue dans laquelle celui-ci est configuré.

---

14. Wikipédia, 2021, *Deep Packet Inspection* [https://fr.wikipedia.org/wiki/Deep_packet_inspection].
15. Martin Untersinger, 2016, *Fin de l'Internet illimité : ça se précise chez Orange, qui dément* [https://www.nouvelobs.com/rue89/rue89-internet/20121011.RUE3086/fin-de-l-internet-illimite-ca-se-precise-chez-orange-qui-dement.html].

Voici une requête envoyée par le navigateur web Firefox :

```
GET /index.php HTTP/2
Host: exemple.org
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.5) Gecko/20100101
↪    Firefox/91.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
↪    webp,*/*;q=0.8
Accept-Language: fr-FR,en;q=0.5
Accept-Encoding: gzip, deflate, br
Referer: https://duckduckgo.com/
Cookie: donation-identifier: dd634367a6b4485ba288197bd92745b4
```

On y voit tout d'abord une commande contenant le nom de la page demandée (`/index.php`), le nom de domaine correspondant (`exemple.org`), suivie d'un en-tête qui contient entre autres le nom et la version de navigateur web (`Mozilla/5.0 (X11; Linux x86_64; rv:91.5) Gecko/20100101 Firefox/91.5`) ainsi que le système d'exploitation utilisé (`Linux x86_64`), les langues acceptées (`fr-FR` pour français de France, `en` pour anglais), la page sur laquelle se trouvait le lien que l'internaute a suivi pour arriver à la page demandée (`https://duckduckgo.com/`), et le cookie de session (`donation-identifier: dd634367a6b4485ba288197bd92745b4`).

page 214



Pour aller plus loin…

Dans le navigateur web Firefox, on peut afficher en quelques clics les en-têtes de nos requêtes :

- cliquer sur ☰ en haut à droite ;
- sélectionner *Outils supplémentaires* puis *Outils de développement web*, puis sélectionner l'onglet ⇅ *Réseau*.

Un nouveau panneau s'ouvre. Lorsqu'on charge une page, une ligne s'affiche pour chaque requête. En sélectionner une — la première, par exemple, qui correspond au chargement de la page elle-même — pour afficher ses en-têtes dans le panneau de droite, dans un onglet nommé *En-têtes*.

Ces informations sont là pour être utilisées par le serveur web, qui va adapter sa réponse en fonction : c'est notamment grâce à cela qu'un site disponible en plusieurs langues s'affiche dans notre langue sans que nous ayons eu à l'indiquer.

Mais ces informations, comme toutes celles qui transitent par le serveur, sont aussi accessibles aux personnes qui s'occupent de la maintenance du serveur : ses admins… et leur hiérarchie. En général, les serveurs gardent aussi ces informations dans des journaux, plus ou moins longtemps, notamment pour faire des statistiques et pour faciliter les diagnostics en cas de panne. Ils ajoutent aux en-têtes l'adresse IP d'origine ainsi que la date et l'heure. Voici une ligne de journal enregistrée pour notre requête (l'adresse IP d'origine se trouve au début : `203.0.113.42`) :

page 225

```
203.0.113.42 - - [22/Jan/2022:00:00:00 +0100] "GET /index.php HTTP
↪    /2" 200 2131 "https://duckduckgo.com/" "Mozilla/5.0 (X11;
↪    Linux x86_64; rv:91.5) Gecko/20100101 Firefox/91.5) Gecko
↪    /20100101 Firefox/91.5"
```

27.4.2 Les en-têtes mail

Chaque courrier électronique inclut un en-tête ; malgré son nom, ce dernier n'a strictement rien à voir avec l'en-tête d'une page web. Cet en-tête contient des informations sur les données contenues dans l'email : un autre exemple de métadonnées, les « don-

page 30

nées sur les données ». Il est rarement montré dans sa totalité par notre logiciel de courrier électronique, mais il reste néanmoins bien présent. Il inclut souvent de nombreuses informations sur l'expéditrice — bien plus que son adresse mail.

Dans l'exemple suivant, on peut lire l'adresse IP publique, à savoir celle qui sera visible sur Internet, de l'ordinateur utilisé pour envoyer l'email (`203.0.113.98`), ce qui permet de connaître l'endroit où l'expéditrice se trouvait à ce moment-là, l'adresse IP de son ordinateur à l'intérieur de son réseau local (`192.168.0.10`), le logiciel de mail utilisé (`Thunderbird/91.5.0`), ou encore son système d'exploitation (`Mac OS X 11`).

page 205

```
Return-Path: <bea@fai.net>
Delivered-To: ana@exemple.org
Received: from smtp.fai.net (smtp.fai.net [198.51.100.67])
        by mail.exemple.org (Postfix) with ESMTP id 0123456789
        for <ana@exemple.org>; Sat, 22 Jan 2022 20:00:00 +0100 (CET)
Received: from [192.168.0.10] (paris.abo.fai.net [203.0.113.98])
        by smtp.fai.net (Postfix) with ESMTP id ABCDEF1234;
        Sat, 22 Jan 2022 19:59:49 +0100 (CET)
Message-ID: <CB0ABB91.17B7F@fai.net>
Date: Sat, 22 Jan 2022 19:59:45 +0100
From: Bea <bea@fai.net>
User-Agent: Mozilla/5.0 (Macintosh; Intel Mac OS X 11; rv:91.5)
        Gecko/20100101 Thunderbird/91.5.0
MIME-Version: 1.0
To: Ana <ana@exemple.org>
Subject: À mardi
Content-Type: text/plain; charset=iso-8859-1
Content-Length: 22536
Lines: 543
```

Ces en-têtes contiennent aussi parfois l'identifiant de l'abonnée chez son prestataire mail ou encore le nom de sa machine[16].

À l'instar de ces quelques exemples courants, quasiment toutes les applications envoient des informations sur le contenu, mais aussi des métadonnées dans leur protocole.

page 30

27.5 Les traces qu'on laisse soi-même

Il n'y a pas que les traces que laisse le fonctionnement des réseaux : il y a bien sûr aussi celles que nous laissons nous-mêmes, de façon plus ou moins volontaire, par exemple en saisissant des informations sur des sites web ou simplement en nous connectant à des services.

Tenter de maîtriser les traces qu'on laisse sur les réseaux, c'est donc aussi réfléchir aux utilisations qu'on fait des services proposés sur Internet, et aux données qu'on leur confie — des thèmes qu'on traitera plus avant dans les parties à venir.

16. La plupart du temps, cela se trouve dans la ligne `Received` de la première machine ou dans le `Message-ID`. Mais certains autres logiciels ou services de messagerie rajoutent d'autres lignes plus spécifiques.

Chapitre 28

Surveillance et contrôle des communications

Au-delà des traces laissées par le fonctionnement même des réseaux en général et d'Internet en particulier, il est possible d'« écouter » nos activités sur Internet à plusieurs niveaux.

De plus en plus souvent, les organismes qui font fonctionner des parties d'Internet (câbles, serveurs, *etc.*) sont même dans l'obligation légale de conserver un certain nombre de données sur ce qui se passe sur leurs machines, au titre de lois de *rétention de données*. page 224

28.1 Qui veut récupérer les données ?

Diverses personnes ou organisations peuvent porter des regards indiscrets sur les échanges *via* Internet. Parents un peu trop curieux, sites web à la recherche d'une clientèle à cibler, multinationales comme Microsoft, gendarmes de Saint-Tropez, ou *National Security Agency* états-unienne…

Comme dans le cas des mouchards sur les ordinateurs personnels, les différentes entités impliquées ne collaborent pas forcément ensemble, et ne forment pas une totalité cohérente. Si les curieuses sont trop variées pour prétendre dresser une liste exhaustive des intérêts en jeu, on peut toutefois décrire quelques motivations parmi les plus courantes. page 31

28.1.1 Des entreprises à la recherche de profils à revendre

« Vous décidez de réserver un billet d'avion pour New-York sur Internet. Deux jours plus tard, en lisant votre quotidien en ligne, une publicité vous propose une offre intéressante pour une location de voitures à New York. Ce n'est pas une simple coïncidence : il s'agit d'un mécanisme de publicité ciblée, comme il s'en développe actuellement de plus en plus sur Internet. » [1]

La publicité est l'une des principales sources de revenus des entreprises qui fournissent des services « gratuits » sur Internet : boîtes mail, moteurs de recherche, médias sociaux, *etc.* Or, du point de vue des annonceuses, la qualité et donc le prix d'un espace publicitaire en ligne est fonction de l'intérêt que les internautes vont porter aux publicités.

Dès lors, les données personnelles valent de l'or. Centres d'intérêt, genre, âge, *etc.* : autant d'informations qui permettent de présenter les publicités auxquelles l'internaute est le plus susceptible de réagir. Ainsi Google croise-t-il le résultat de l'analyse des

1. CNIL, 2009, *La publicité ciblée en ligne* [https://web.archive.org/web/20170830003226/https://www.cnil.fr/sites/default/files/typo/document/Publicite_Ciblee_rapport_VD.pdf].

activités personnelles [2] sur l'ensemble de ses services, comme le moteur de recherche, les vidéos YouTube regardées ou les photos dans Google Photos pour afficher des publicités ciblées sur ses autres applications, comme Gmail [3].

En outre, chaque site visité est un « centre d'interêt » de plus. En additionnant ces informations les unes aux autres, c'est tout un profil qui se dessine [4]. Un petit logiciel permet de voir quels cookies se téléchargent sur notre ordinateur à chaque page consultée. Si l'internaute commence par visiter allocine.fr, quatre régies publicitaires enregistrent sa visite. Se rendant ensuite sur le site du *Monde* ce sera quatre régies qui seront au courant, dont deux qui se trouvaient déjà sur le site d'AlloCiné. Elles savent donc que l'internaute a visité ces deux sites et peuvent donc recouper ces deux centres d'intérêt. En se rendant par la suite sur deux autres sites (Gmail et Dailymotion), ce sont au total vingt-et-une régies publicitaires qui ont eu connaissance de la visite de cet internaute. Dans chacune de ces visites se trouvaient les régies publicitaires XiTi et Google-Analytics. Le plus gros moteur de recherche a donc eu connaissance de la totalité des sites visités et peut maintenant mettre en place sa publicité ciblée.

page 214

Les médias sociaux sont particulièrement bien placés pour obtenir directement des internautes des données personnelles les concernant. Ainsi, sur Facebook, une entreprise peut « cibler une publicité auprès des jeunes de 13 à 15 ans habitant Birmingham en Angleterre et ayant "la boisson" comme centre d'intérêt. De plus, Facebook indique que la cible choisie comporte approximativement une centaine de personnes [5]. La société Facebook exploite ainsi les données qu'elle collecte de ses membres de manière à fournir une publicité qui peut être très ciblée » [6].

La publicité ciblée est d'ailleurs « l'une des raisons qui a poussé les acteurs Internet à diversifier leurs services et leurs activités, afin de collecter toujours plus d'informations sur le comportement des utilisateurs sur Internet. » « Par exemple, Google fournit des services de recherche. Il a racheté des sociétés de publicité comme DoubleClick. Il a [...] lancé un service Google Suggest, intégré à son navigateur Chrome, qui envoie à Google l'ensemble des pages web visitées par les internautes, même quand ces dernières n'y ont pas accédé *via* le moteur de recherche, *etc.* » [7]

Pour se donner une idée de l'importance des enjeux, notons que Google a racheté la société Doubleclick pour la somme de 3,1 milliards de dollars [8].

Cette accumulation de données et leur traitement permet également à Google de trier et d'adapter les résultats aux supposés centres d'intérêt de l'internaute. Ainsi, pour une recherche identique, deux personnes ayant un profil différent n'obtiendront pas le même résultat, ce qui a pour effet de renforcer chaque personne dans ses

2. Julien Lausson, 2017, *Pourquoi Google ne va pas arrêter la publicité ciblée et le scan de vos emails sur Gmail*, Numerama [https://www.numerama.com/tech/270293-pourquoi-google-ne-va-pas-arreter-la-publicite-ciblee-et-le-scan-de-vos-mails-sur-gmail.html]

3. « Lorsque vous ouvrez Gmail, vous voyez des annonces sélectionnées en fonction de leur utilité et de leur pertinence. Le processus de sélection et d'affichage des annonces personnalisées dans Gmail est entièrement automatisé. Ces annonces vous sont présentées sur la base de votre activité en ligne pendant que vous êtes connecté à Google. Nous n'analysons ni ne lisons vos messages Gmail pour choisir les annonces qui vous seront présentées. » Google, 2021, *Fonctionnement des annonces dans Gmail* [https://support.google.com/mail/answer/6603?hl=fr].

4. Data Gueule, 2014, *Big data : données, données, donnez-moi ! – #DATAGUEULE 15* [https://peertube.datagueule.tv/w/etMw3qxMsdZHcvhFzekvie].

5. Une interface similaire est disponible publiquement et permet de répondre à des requêtes inquiétantes : Tom Scott, 2014, *Actual Facebook Graph Searches* [https://actualfacebookgraphsearches.tumblr.com/] (en anglais).

6. CNIL, 2009, *La publicité ciblée en ligne* [https://web.archive.org/web/20170830003226/https://www.cnil.fr/sites/default/files/typo/document/Publicite_Ciblee_rapport_VD.pdf], p. 13.

7. CNIL, 2009, *La publicité ciblée en ligne* [https://web.archive.org/web/20170830003226/https://www.cnil.fr/sites/default/files/typo/document/Publicite_Ciblee_rapport_VD.pdf], p. 4.

8. Le Monde, 2007, *Google rachète DoubleClick pour 3,1 milliards de dollars* [https://www.lemonde.fr/technologies/article/2007/04/14/google-rachete-doubleclick-pour-3-1-milliards-de-dollars_896316_651865.html].

propres intérêts et ses propres convictions. C'est ce que certaines personnes nomment « l'individualisation de l'Internet » [9].

En plus d'être ciblée thématiquement, la publicité l'est aussi géographiquement : grâce aux GPS intégrés dans les terminaux mobiles tels les smartphones, mais aussi grâce à l'adresse IP et aux réseaux Wi-Fi « visibles » à portée de l'ordinateur portable ou du téléphone [10]. Ainsi, il est par exemple possible de faire apparaître des publicités pour des boutiques situées à proximité de l'abonnée.

Des intérêts économiques poussent les fournisseurs de services Internet à rassembler des profils d'internautes, les plus précis possibles, pour ensuite vendre, directement ou pas, des espaces publicitaires ciblés.

Une fois ces informations collectées, les entreprises seront en mesure de répondre aux demandes des flics. Tous les gros fournisseurs de contenus ont des bureaux dédiés pour répondre aux demandes et donc des formulaires, des procédures, *etc.*, écrites pour les flics, pour expliquer la meilleure marche à suivre pour demander des informations [11].

28.1.2 Des entreprises et des États cherchant à préserver leurs intérêts

D'autres entreprises s'intéressent à ce qui se passe sur Internet pour préserver leurs intérêts. Cela va de la lutte menée par l'industrie de l'audiovisuel contre le téléchargement illégal à la veille technologique : les entreprises observent et analysent en temps réel et de manière automatisée des centaines de sources (sites d'actualité, bases de dépôt de brevets, blogs d'experts, *etc.*) afin de connaître rapidement les dernières avancées technologiques et de rester les plus compétitives possible.

Les entreprises sont loin d'être les seules à scruter Internet. Les États, de la justice aux services secrets en passant par les différents services de police sont même certainement les plus curieux.

De plus en plus de pays mettent en place des lois visant à rendre possible l'identification des autrices de toute information qui circule sur Internet [12].

Mais cela va plus loin encore. Les agences de renseignement et autres services secrets ne se contentent plus d'espionner quelques groupes ou personnes qu'elles considèrent comme des cibles. À la limite de la légalité, la NSA, agence de renseignement étatsunienne, collecte « toutes sortes de données sur les personnes — nous pensons que cela concernerait des millions de personnes » [13]. Parmi ses objectifs : « examiner "quasiment tout ce que fait un individu sur Internet" » [14] et établir un *graphe social*, c'est-à-dire « le réseau de connexions et de relations entre les gens » [15]. « "En général, ils analysent les réseaux situés à deux degrés de séparation de la cible." Autrement

9. Xavier de la Porte, 2011, *Le risque de l'individualisation de l'Internet*, InternetActu.net, Fondation Internet nouvelle génération [https://web.archive.org/web/20210413221428/https://www.internetactu.net/2011/06/13/le-risque-de-lindividualisation-de-linternet/].
10. Audenard, 2013, *Bornes wifi et smartphones dans les magasins*, blogs/sécurité, Orange Business [https://www.orange-business.com/fr/blogs/securite/mobilite/souriez-vous-etes-pistes-merci-aux-bornes-wifi-des-magasins].
11. Plusieurs versions du guide publié par Facebook ont fuité [https://publicintelligence.net/facebook-law-enforcement-subpoena-guides/] ces dernières années. On trouve également plusieurs autres guides du même acabit (mais tout n'est pas forcément juste) sur cryptome.org [https://cryptome.org/isp-spy/online-spying.htm] (liens en anglais).
12. Begeek, 2013, *Facebook publie son premier rapport international des demandes gouvernementales* [https://www.begeek.fr/facebook-publie-premier-rapport-international-demandes-gouvernementales-102351].
13. Bruce Schneier, cité par Guillaud, 2013, *Lutter contre la surveillance : armer les contre-pouvoirs*, Internet Actu [https://web.archive.org/web/20220126013621/https://www.internetactu.net/2013/06/13/lutter-contre-la-surveillance-armer-les-contre-pouvoirs/].
14. Maxime Vaudano, 2013, *Plongée dans la « pieuvre » de la cybersurveillance de la NSA*, Le Monde.fr [https://www.lemonde.fr/technologies/visuel/2013/08/27/plongee-dans-la-pieuvre-de-la-cybersurveillance-de-la-nsa_3467057_651865.html].
15. Pisani, 2007, *Facebook/5 : la recette* [https://www.francispisani.net/facebook5-la-recette/].

dit, la NSA espionne aussi ceux qui communiquent avec ceux qui communiquent avec ceux qui sont espionnés » [16].

Les services de renseignement français disposent désormais d'un arsenal de lois qui leur permettent d'effectuer des analyses sur l'ensemble du trafic Internet ou sur des personnes ciblées en toute légalité, en France [17] comme à l'étranger [18].

28.2 Journaux et rétention de données

La plupart des organisations qui fournissent des services sur Internet (connexion, hébergement de site, *etc.*) conservent plus ou moins de traces de ce qui transite sur leurs machines, sous forme de journaux de connexion : qui a fait quoi, à quel moment. On appelle ces journaux des *logs*.

page 29

Historiquement, ces journaux répondent à un besoin technique : ils sont utilisés par les personnes qui s'occupent de la maintenance des serveurs afin de diagnostiquer et résoudre les problèmes. Cependant, ils peuvent aussi être très utiles pour recueillir des données sur les utilisatrices de ces serveurs.

28.2.1 Lois de rétention de données

Désormais, dans la plupart des pays occidentaux, les fournisseurs de services Internet sont légalement tenus de conserver leurs journaux pendant un certain temps, pour pouvoir répondre à des réquisitions.

Les lois qui règlementent la rétention de données définissent de façon plus ou moins claire les informations qui doivent être conservées dans ces journaux. La notion de fournisseur de service Internet peut ainsi être entendue de façon assez large [19] : un cybercafé est un fournisseur de service Internet qui fournit *aussi* une machine pour accéder au réseau.

Au-delà des obligations légales, de nombreux fournisseurs de services Internet conservent de plus ou moins grandes quantités d'information sur les internautes qui utilisent leurs services, notamment pour la publicité ciblée. Les GAFAM, tels Google, Amazon ou Facebook, sont particulièrement connues pour cela. Étant donné que ce « modèle de fourniture de services adossés à de la publicité est quasiment devenu la norme » [20], on peut supposer que nombre d'autres font de même plus discrètement.

Au Royaume-Uni, un fournisseur d'accès à Internet (FAI) a ainsi créé une polémique lorsqu'il est apparu qu'il gardait la trace de l'ensemble des pages web visitées par ses abonnées pour tester une technologie de profilage destinée à « offrir » de la « publicité comportementale » [21] [22].

Le serveur qui héberge le contenu utilisé (page web, boîte mail, *etc.*) et le fournisseur d'accès à Internet sont particulièrement bien placés pour disposer des informations permettant d'identifier qui est à l'origine d'une requête de connexion. En France, ce sont eux qui sont particulièrement visés par les lois de rétention de données.

---

16. Manach, 2013, *Pourquoi la NSA espionne aussi votre papa (#oupas)*, Bug Brother [https://bugbrother.blog.lemonde.fr/2013/06/30/pourquoi-la-nsa-espionne-aussi-votre-papa-oupas/].
17. Légifrance, *Code de la sécurité intérieure*, articles L851-2 et L851-3 [https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000025503132/LEGISCTA000030935576].
18. Légifrance, *Code de la sécurité intérieure*, article L854-1 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000037200982/].
19. CNIL, 2010, *Conservation des données de trafic : hot-spots wi-fi, cybercafés, employeurs, quelles obligations ?* [https://www.cnil.fr/fr/conservation-des-donnees-de-trafic-hot-spots-wi-fi-cybercafes-employeurs-quelles-obligations].
20. CNIL, 2009, *La publicité ciblée en ligne* [https://web.archive.org/web/20170830003226/https://www.cnil.fr/sites/default/files/typo/document/Publicite_Ciblee_rapport_VD.pdf], p. 4.
21. CNIL, 2009, *La publicité ciblée en ligne* [https://web.archive.org/web/20170830003226/https://www.cnil.fr/sites/default/files/typo/document/Publicite_Ciblee_rapport_VD.pdf], p. 17.
22. Arnaud Devillard, 2009, *Affaire Phorm : Bruxelles demande des comptes au Royaume-Uni* [https://www.01net.com/actualites/affaire-phorm-bruxelles-demande-des-comptes-au-royaume-uni-501173.html].

28.2.2 Les journaux conservés par les hébergeurs

On a vu que le serveur qui héberge un service (comme un site web, une boîte mail ou un salon de messagerie instantanée) avait accès à une grande quantité de données. page 217

En France, c'est l'article 6 de la Loi pour la Confiance dans l'Économie Numérique[23] (LCEN) qui oblige les hébergeurs de contenus publics à conserver « les données de nature à permettre l'identification » de « toute personne ayant contribué à la création d'un contenu mis en ligne » ; par exemple : écrire sur un média social, sur un blog ou sur un site de média participatif ou poster sur une liste de diffusion publique[24].

Pour ce qui concerne les contenus ayant le caractère d'une correspondance privée, c'est l'article L34-1 du code des postes et des communications électroniques[25] (CPCE) qui amène la même obligation pour l'écriture d'un email ou l'envoi d'un message instantané par exemple. Concrètement, il s'agit de conserver pendant un an les éventuels identifiants ou pseudonymes fournis par l'autrice, mais surtout l'adresse IP à la source de la connexion à chaque modification de contenu[26]. Une réquisition auprès du fournisseur d'accès à Internet (FAI) qui fournit cette adresse IP permet ensuite généralement de remonter jusqu'à la propriétaire de la connexion utilisée. page 202

De plus, la *loi relative à la programmation militaire*[27], promulguée fin décembre 2013, permet de demander ces mêmes informations, en temps réel, pour des motifs aussi variés que : les attaques terroristes, les cyber-attaques, les atteintes au potentiel scientifique et technique, la criminalité organisée, *etc.*

C'est donc cette obligation de rétention de données qui permet à la police, dans notre histoire introductive, d'obtenir des informations auprès des organismes hébergeant les adresses mail incriminées : page 194

> — *On va demander à Gmail ainsi qu'à no-log les informations sur ces adresses email. À partir de là on aura sans doute des éléments, ou au moins de quoi poser les bonnes questions !*

Les hébergeurs pourront être plus ou moins coopératifs sur la façon de vérifier la légalité des réquisitions que leur adressent les flics et d'y répondre : il semblerait que

23. Légifrance, 2022, Article 6 de la *loi n° 2004575 du 21 juin 2004 pour la confiance dans l'économie numérique* [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000045292730].

24. Légifrance, 2021, *Décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne* [https://www.legifrance.gouv.fr/loda/id/JORFTEXT000044228912].

25. Légifrance, 2013, *Article L34-1 - code des postes et des communications électroniques* [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000028345210/].

26. « Les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services » (LCEN, *op. cit.*, article 6 alinéa I.2 [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000045292730]), c'est-à-dire les hébergeurs, sont tenus de conserver pendant un an et pour chaque opération de création, modification ou suppression de contenu : « a) L'identifiant de la connexion à l'origine de la communication ; b) Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus » (article 5 du décret n° 2021-1362 du 20 octobre 2021, *op. cit.* [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230063]).

Mais aussi : « a) L'identifiant attribué par le système d'information au contenu, objet de l'opération ; b) La nature de l'opération ; c) Les date et heure de l'opération ; d) L'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni » (article 6 du décret n° 2021-1362 du 20 octobre 2021, *op. cit.* [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230065], au vu de l'article 1 du décret n° 2021-1363 du 20 octobre 2021 portant injonction, au regard de la menace grave et actuelle contre la sécurité nationale, de conservation pour une durée d'un an de certaines catégories de données de connexion [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044231713]).

27. Légifrance, 2014, *Loi n° 2013-1168 du 18 décembre 2013 relative à la programmation militaire pour les années 2014 à 2019 et portant diverses dispositions concernant la défense et la sécurité nationale* [https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028338825&dateTexte&categorieLien=id].

certains répondent à un simple email des flics alors que d'autres attendront d'avoir un courrier signé d'une juge [28], voire ne répondent pas aux requêtes [29].

Non seulement les personnes ayant accès au serveur peuvent collaborer avec les flics de plein gré, mais des adversaires peuvent aussi, comme dans le cas d'un ordinateur personnel, s'y introduire et espionner ce qui s'y passe en utilisant des failles, sans passer par l'étape réquisition. Elles auront alors accès à toutes les données stockées sur le serveur, y compris les journaux.

Mais le serveur ne connaît pas toujours l'identité réelle des internautes qui s'y connectent : en général, tout ce qu'il peut donner c'est une adresse IP.

C'est alors qu'intervient le fournisseur d'accès à Internet.

28.2.3 Les journaux conservés par les fournisseurs d'accès Internet

page 205

On a vu qu'on accédait à Internet par l'intermédiaire d'un fournisseur d'accès à Internet (FAI). Ce FAI est en général une société qui fournit une « box » connectée à Internet. Mais ça peut aussi être une association ou une institution publique (une université, par exemple, quand on utilise leurs salles informatiques). Les FAI sont eux aussi soumis à des lois concernant la rétention de données.

Au sein de l'Union Européenne, une directive oblige les fournisseurs d'accès à Internet à garder la trace de qui s'est connectée, quand, et depuis où [30]. En pratique, cela consiste à enregistrer quelle adresse IP a été assignée à quelle abonnée pour quelle période [31]. Les institutions qui fournissent un accès à Internet, comme les bibliothèques et les universités, font de même : en général il faut se connecter avec un nom d'utilisatrice et un mot de passe. On peut ainsi savoir qui utilisait quel poste à quel moment. La directive européenne précise que ces données doivent être conservées de 6 mois à 2 ans. En France, la durée légale est de un an [32].

Contre-intuitivement, cette obligation s'applique à tous les endroits qui proposent un accès au réseau Internet au public, à titre payant ou gratuit et ce, même si les internautes ne sont pas identifiées. Des gérants de bars ignorant cette disposition en ont fait les frais et se sont retrouvés en garde-à-vue pour avoir offert du Wi-Fi à leurs clientes sans conserver les données de connexion [33].

---

28. Globenet, 2014, *No-log, les logs et la loi* [https://www.globenet.org/No-log-les-logs-et-la-loi.html].

29. « Précisons que les serveurs hébergeant les sites du réseau Indymedia, domiciliés aux USA à Seattle, refusent systématiquement de donner connaissance aux autorités des *logs* de connexion des ordinateurs consultant ces sites ou y déposant une contribution, rendant de fait non-identifiable les auteurs des contributions » (dossier d'instruction judiciaire cité par Anonymes, 2010, *Analyse d'un dossier d'instruction antiterroriste* [https://infokiosques.net/spip.php?page=lire&id_article=789].

30. Parlement Européen et Conseil, 2006, *Directive 2006/24/CE du Parlement européen et du Conseil du 15 mars 2006 sur la conservation de données générées ou traitées dans le cadre de la fourniture de services de communications électroniques accessibles au public ou de réseaux publics de communications, et modifiant la directive 2002/58/CE* [https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0024:FR:HTML], dite « Data Retention ».

31. « Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne » (LCEN, *op. cit.*), c'est-à-dire les FAI, sont tenues de conserver durant un an : « a) L'identifiant de la connexion ; b) L'identifiant attribué par ces personnes à l'abonné ; c) L'adresse IP attribuée à la source de la connexion et le port associé » (article 5 du décret n° 2021-1362 du 20 octobre 2021, *op. cit.* [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230063]).

Mais aussi : « a) Les dates et heure de début et de fin de la connexion ; b) Les caractéristiques de la ligne de l'abonné » (article 6 du décret n° 2021-1362 du 20 octobre 2021, *op. cit.* [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230065], au vu de l'article 1 du décret n° 2021-1363 du 20 octobre 2021, *op. cit.* [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044231713]).

32. Légifrance, 2021, Décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne [https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044228912].

33. Sputnik France, 2020, *Des gérants de bars en garde à vue pour avoir offert du wifi à leurs clients à Grenoble* [https://fr.sputniknews.com/faits_divers/202009291044498557-des-gerants-de-bars-en-garde-a-vue-pour-avoir-offert-du-wifi-a-leurs-clients-a-grenoble/].

De plus, FAI et hébergeurs français sont tenus de conserver « les informations relatives à l'identité civile de l'utilisateur » pendant les cinq années qui suivent la fin de validité de son contrat[34]. Ils doivent aussi conserver « les autres informations fournies par l'utilisateur lors de la souscription d'un contrat ou de la création d'un compte »[35] et « les informations relatives au paiement [...] pour chaque opération de paiement »[36] pour une durée d'un an après la fin de validité de son contrat ou de la fermeture de son compte.

L'objectif des lois de rétention de données est donc de rendre facile, pour les autorités, d'associer un nom à tout geste effectué sur Internet.

Des flics qui enquêteraient par exemple sur un article publié sur un blog peuvent demander aux responsables du serveur hébergeant le blog l'adresse IP de la personne qui a posté l'article, ainsi que la date et l'heure correspondantes. Une fois ces informations obtenues, ils vont demander au fournisseur d'accès à Internet responsable de cette adresse IP à qui elle était assignée au moment des faits.

> — *Quelle histoire ! Mais quel rapport avec nos bureaux ?*
> — *Et bien c'est également pour ça que je vous appelle. Elles affirment qu'elles ont toutes les preuves comme quoi ces documents ont été publiés depuis vos bureaux. Je leur ai dit que ce n'était pas moi, que je ne voyais pas de quoi elles parlaient.*

C'est exactement de ça qu'il s'agit quand, dans notre histoire du début, la police prétend, traces à l'appui, que les relevés bancaires ont été postés depuis les bureaux rue Jaurès. Elle a au préalable obtenu auprès des hébergeurs du site de publication l'adresse IP qui correspond à la connexion responsable de la publication des documents incriminés. Cette première étape permet de savoir d'où, de quelle « box », provient la connexion. La réquisition auprès du fournisseur d'accès à Internet permet de savoir quel est le nom de l'abonnée — adresse en prime — *via* son contrat, associé à l'adresse IP.

page 194

28.2.4 Le VPN, une histoire de confiance

Le VPN (*Virtual Private Network*, en français Réseau Privé Virtuel ou RPV) est un système créé initialement pour partager un réseau privé entre plusieurs sites[37]. Il permet de créer un lien direct entre notre ordinateur et le serveur du fournisseur de VPN choisi. Un VPN permet de changer les adresses IP d'une connexion Internet : pour les routeurs et les serveurs auxquels on se connecte, la connexion ne vient plus de la « box » du FAI, mais du serveur de VPN. Cela peut permettre de contourner certains types de censure.

---

34. « 1° Les nom et prénom, la date et le lieu de naissance ou la raison sociale, ainsi que les nom et prénom, date et lieu de naissance de la personne agissant en son nom lorsque le compte est ouvert au nom d'une personne morale ; 2° La ou les adresses postales associées ; 3° La ou les adresses de courrier électronique de l'utilisateur et du ou des comptes associés le cas échéant ; 4° Le ou les numéros de téléphone. » (Article 2 du décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données, *op. cit.* [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230081]).

35. « 1° L'identifiant utilisé ; 2° Le ou les pseudonymes utilisés ; 3° Les données destinées à permettre à l'utilisateur de vérifier son mot de passe ou de le modifier, le cas échéant par l'intermédiaire d'un double système d'identification de l'utilisateur, dans leur dernière version mise à jour. » (Article 3 du décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données, *op. cit.* [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230083]).

36. « 1° Le type de paiement utilisé ; 2° La référence du paiement ; 3° Le montant ; 4° La date, l'heure et le lieu en cas de transaction physique. » (Article 4 du décret n° 2021-1362 du 20 octobre 2021 relatif à la conservation des données, *op. cit.* [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000044230085]).

37. Certaines entreprises utilisent des stockages de documents partagés sur leur réseau local. Le VPN permet de se connecter de façon chiffrée et authentifiée sur le réseau local de l'entreprise pour accéder au stockage partagé.

Certains services de VPN relaient le trafic de nombreuses personnes avec seulement quelques addresses IP. Cela permet de se fondre dans la masse des personnes qui utilisent ce service de VPN et de compliquer l'identification des internautes.

Les données peuvent être chiffrées aux yeux du FAI, mais elles restent visibles par le fournisseur de VPN. Les admins du service VPN ont toujours accès à la fois à la source et à la destination des communications. L'utilisation d'un VPN ne fait que déplacer le problème de la confiance que l'on accorde aux FAI vers la confiance que l'on accorde au VPN.

Bien qu'elle puisse être considérée dans certains modèles de menaces, l'utilisation du VPN n'est pas dévelopée dans ce guide. Si l'on souhaite se fondre dans une masse d'internautes et être dificilement identifiable, sans dépendre de la confiance dans un intermédiaire unique, il est plus sûr d'utiliser Tor, comme proposé plus loin.

28.2.5 Réquisition

En France, lorsque les flics souhaitent accéder aux journaux prévus par les lois de rétention de données, ils sont supposés passer par une *réquisition judiciaire* : une demande officielle qui oblige les personnes qui administrent un serveur à leur fournir les informations demandées... ou à désobéir. Ces réquisitions sont supposées préciser les informations demandées et être fondées juridiquement. Mais elles ne le sont pas toujours, et les fournisseurs de services Internet donnent parfois des informations que la loi ne les oblige pas à fournir.

Voici l'extrait d'une réquisition reçue par un hébergeur de mail français, l'adresse mail du compte visé a été anonymisée en remplaçant l'identifiant par *adresse*. L'orthographe n'a pas été modifiée.



REQUISITION JUDICIAIRE

Lieutenant de Police En fonction à la B.R.D.P

Prions et, au besoin, requérons :

Monsieur le président de l'association GLOBENET 21ter, rue Voltaire 75011 Paris

à l'effet de bien vouloir :

Concernant l'adresse de messagerie adresse@no-log.org

- Nous communiquer **l'identité complète** (nom, prénom date de naissance, filiation) et les **coordonnées** (postales, téléphoniques, électroniques et bancaires) de son **titulaire**
- Nous indiquer les TRENTE dernières données de connexion (adresse IP, date heures et fuseau horaire) utilisées pour **consulter, relever où envoyer des messages** avec ladite adresse (Pop, Imap ou Webmail)
- Nous indiquer si une **redirection est active** sur cette messagerie, et nous communiquer le ou les e-mails de destination, le cas échéant
- Nous communiquer le **numéro de téléphone** à l'abonnement internet du compte no-log.org « adresse » et les **trente dernières données de connexion** qui lui sont relatives
- Nous communiquer les TRENTES **dernières données de connexion** (adresse IP, date heure et fuseau horaire) aux **pages d'aministration** du compte no-log « adresse »

De plus, il est avéré que les flics demandent parfois de telles informations dans un simple courrier électronique, et il est probable que de nombreux fournisseurs de services Internet répondent directement à de telles requêtes officieuses, ce qui implique

que *n'importe qui* peut obtenir de telles informations en se faisant passer pour la police.

Les réquisitions sont monnaie courante. Les gros fournisseurs de services Internet ont désormais des services légaux dédiés pour y répondre, et une grille tarifaire chiffre chaque type de demande[38]. Depuis octobre 2013, en France, une grille tarifaire indexée par l'État vient même homogénéiser ces différentes prestations[39] : identifier une abonnée à partir de son adresse IP coûtait ainsi 4 € (tarifs en vigueur en octobre 2013). Au-delà de 20 demandes, ce tarif est réduit à 18 centimes.

Ainsi pour la première moitié de l'année 2020, Google a reçu chaque mois, en moyenne, 1 349 demandes de renseignements sur ses utilisatrices de la part de la France, concernant au total 10 864 comptes — des chiffres en augmentation constante depuis 2009. Après analyse de la recevabilité des demandes sur le plan juridique, la société a répondu à 60 % d'entre elles[40] : l'autre moitié des demandes n'entrait donc pas dans le cadre de ce que l'entreprise s'estimait légalement contrainte de fournir.

En plus des journaux de connexion, depuis la loi de 2016[41] contre le crime organisé, les autorités peuvent prendre connaissance du contenu des correspondances stockées[42] sur simple réquisition.

28.3 Écoutes de masse

Au-delà des journaux et des réquisitions prévus par les lois de rétention de données, les communications sur Internet sont surveillées de façon systématique par divers services étatiques.

Un ancien employé de l'opérateur de télécommunications états-unien AT&T a témoigné[43] du fait que la NSA (l'agence de renseignement électronique états-unienne) surveillait l'ensemble des communications Internet et téléphoniques qui passaient par une importante installation de l'opérateur de télécommunication AT&T à San Francisco. Ceci, à l'aide d'un superordinateur spécialement conçu pour la surveillance de masse, en temps réel, de communications[44]. Il a aussi déclaré que de telles installations existaient probablement au sein d'autres infrastructures similaires dans d'autres villes des États-Unis, ce que confirment les révélations d'un ex-employé de la NSA et de la CIA[45]. Des installations similaires seraient mises en place par les services secrets britanniques sur plus de 200 fibres optiques sous-marines[46].

38. Christopher Soghoian, 2010, *Your ISP and the Government : Best Friends Forever* [https://www.defcon.org/html/defcon-18/dc-18-speakers.html#Soghoian] (en anglais).

39. Légifrance, 2013, *arrêté du 21 août 2013 pris en application des articles R. 213-1 et R. 213-2 du code de procédure pénale fixant la tarification applicable aux réquisitions des opérateurs de communications électroniques* [https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000028051025].

40. Google, 2021, *France - Google Transparence des informations* [https://www.google.com/transparencyreport/userdatarequests/FR/].

41. Loi n° 2016-731 (*op. cit.*)

42. Légifrance, 2019, *Article n° 706-95-1 du code de procédure pénale* [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000038311668]; Cet article permet ainsi de contourner les contraintes d'une perquisition et de ne pas alerter la personne concernée de cette atteinte à sa vie privée.

43. Mark Klein, 2004, *AT&T's Implementation of NSA Spying on American Citizens* [https://www-tc.pbs.org/wgbh/pages/frontline/homefront/etc/kleindoc.pdf] (en anglais).

44. Reflets.info, 2011, *#OpSyria : BlueCoat maître artisan de la censure syrienne* [https://web.archive.org/web/20160823002531/https://reflets.info/opsyria-bluecoat-maitre-artisan-de-la-censure-syrienne/].

45. Craig Timberg et Barton Gellman, 2013, *NSA paying U.S. companies for access to communications networks* [https://www.washingtonpost.com/world/national-security/nsa-paying-us-companies-for-access-to-communications-networks/2013/08/29/5641a4b6-10c2-11e3-bdf6-e4fc677d94a1_story.html] (en anglais).

46. L'expansion.com, 2013, *"Operation Tempora" : comment les Britanniques dépassent les Américains pour espionner Internet* [https://lexpansion.lexpress.fr/high-tech/operation-tempora-comment-les-britanniques-depassent-les-americains-pour-espionner-internet_390971.html].

Les services de sécurité français sont désormais autorisés à mettre en place dans le réseau des fournisseurs d'accès à Internet de tels outils d'analyse de tout le trafic pour « détecter des connexions susceptibles de révéler une menace terroriste » [47].

Depuis la loi de finances 2020 [48], l'administration fiscale et les douanes françaises sont autorisées à exploiter certaines données personnelles de manière automatisée. Elles peuvent en effet collecter les informations librement accessibles des médias sociaux servant à « la mise en relation de plusieurs parties en vue de la vente d'un bien, de la fourniture d'un service ou de l'échange ou du partage d'un contenu, d'un bien ou d'un service », soit des plateformes comme Le Bon Coin ou BlaBlaCar.

La NSA a aussi obtenu un accès direct aux serveurs de plusieurs « géants » du net (Microsoft, Yahoo, Google, Facebook, PalTalk, Youtube, Skype, AOL et Apple) [49], ce qui lui permet d'accéder aux données qu'ils hébergent ou qui transitent par leurs serveurs [50]. La DGSE, l'équivalent français de la NSA dispose d'un tel accès direct aux réseaux d'Orange [51].

De même, les communications satellites sont écoutées par le réseau Echelon, un « système mondial d'interception des communications privées et publiques » [52] élaboré par des pays anglo-saxons [53]. Les informations à ce sujet restent floues, mais la France semble aussi disposer d'un réseau d'écoute des télécommunications sur son territoire [54].

La NSA surveille et recoupe également les échanges d'emails pour établir une carte des relations entre toutes les habitantes des États-Unis [55]. Si ce genre de pratiques n'est pas forcément attesté ailleurs dans le monde, elles y sont tout aussi possibles.

page 217

De plus, pour toute organisation ayant les moyens d'être un nœud conséquent du réseau, que ce soit officiellement ou non, l'utilisation du *Deep Packet Inspection* (ou *DPI* : Inspection en profondeur des paquets, en français) se généralise. La surveillance que permet le DPI est particulièrement intrusive : elle ne se limite plus aux seules informations inscrites dans les en-têtes des paquets IP, mais touche au contenu même des communications. Si celles-ci ne sont pas chiffrées, il est alors possible de retrouver par exemple le contenu complet d'emails, ou l'intégralité de nos consultations et recherches sur le web.

page 217

page suiv.

L'utilisation de cette technique, en Lybie ou en Syrie par exemple, a permis dans un premier temps de mettre sous surveillance numérique toute la population du pays, pour dans un second temps notamment effectuer des attaques ciblées. La société Amesys, basée en France, a en effet, avec l'aide et l'appui du gouvernement [56] de

47. Légifrance, *Code de la sécurité intérieure*, article L851-3 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043887520/].
48. Légifrance, 2019, *LOI n° 2019-1479 du 28 décembre 2019 de finances pour 2020* [https://www.legifrance.gouv.fr/jorf/article_jo/JORFARTI000039684091].
49. NSA, 2013, *Dates When PRISM Collection Began For Each Provider* [https://commons.wikimedia.org/wiki/File:Prism_slide_5.jpg].
50. Le Monde, 2013, *Le FBI aurait accès aux serveurs de Google, Facebook, Microsoft, Yahoo ! et d'autres géants d'Internet* [https://www.lemonde.fr/ameriques/article/2013/06/07/le-fbi-a-acces-aux-serveurs-des-geants-d-internet_3425810_3222.html].
51. Jacques Follorou, 2015, *Espionnage : comment Orange et les services secrets coopèrent*, Le Monde [https://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses_4386264_3210.html].
52. Wikipédia, 2021, *Echelon* [https://fr.wikipedia.org/wiki/Echelon].
53. Gerhard Schmid, 2001, *Rapport sur l'existence d'un système d'interception mondial des communications privées et économiques (système d'interception ECHELON)* [https://www.europarl.europa.eu/doceo/document/A-5-2001-0264_FR.html].
54. Wikipédia, 2021, *Frenchelon* [https://fr.wikipedia.org/wiki/Frenchelon].
55. Gorman, Siobhan, 2008, *NSA's Domestic Spying Grows As Agency Sweeps Up Data : Terror Fight Blurs Line Over Domain ; Tracking Email* [https://online.wsj.com/article/SB120511973377523845.html] (en anglais).
56. kitetoa, 2011, *Amesys : le gouvernement (schizophrène) français a validé l'exportation vers la Libye de matériel d'écoute massive des individus*, Reflets.info [https://web.archive.org/web/20181121190456/https://reflets.info/articles/amesys-le-gouvernement-francais-a-valide-l-exportation-vers-la-libye-de-materiel-de-surveillance].

l'époque, installé de tels systèmes en Lybie[57], au Maroc, au Qatar[58] ou encore en France[59].

28.4 Attaques ciblées

Lorsqu'une internaute ou qu'une ressource disponible *via* Internet — comme un site web ou une boîte mail — éveille la curiosité des adversaires, ces dernières peuvent mettre en place des attaques ciblées. Ces attaques ciblées peuvent avoir lieu à différents niveaux : les annuaires qui permettent de trouver la ressource, les serveurs qui l'hébergent, les clients qui y accèdent, *etc.* Nous étudions ces différentes possibilités dans cette partie.

En France, la loi oblige les fournisseurs d'accès à Internet à bloquer l'accès aux sites web qui ont été inscrits sur une « liste bloquée » à la suite d'une décision de justice[60] ou considérés par l'*office central de lutte contre la criminalité liée aux technologies de l'information et de la communication* comme ayant du contenu pédopornographique, provoquant « directement à des actes de terrorisme » ou en faisant « l'apologie »[61]. De plus, une ordonnance les oblige à procéder de même pour les sites web portant atteinte à un droit d'auteur ou à un droit voisin[62].

C'est ainsi qu'en octobre 2011, le tribunal de Grande Instance de Paris a ordonné à sept fournisseurs d'accès à Internet français de bloquer « par IP ou par DNS » le site web copwatchnord-idf.org[63] ; ce site était accusé de propos injurieux et diffamatoires, et de collecter des données à caractère personnel sur des policiers. En février 2012, le tribunal ordonnait le blocage de l'un des 35 sites miroirs[64] que le ministère de l'Intérieur voulait faire bloquer[65].

Par contre, le tribunal n'a pas ordonné le blocage des 34 autres miroirs référencés par le ministère de l'Intérieur, car ce dernier « n'indique pas s'il a tenté ou non d'identifier leurs éditeurs et leurs hébergeurs », ni celui des sites miroirs qui pourraient apparaître.

Plus récemment, le tribunal de Grande Instance de Paris a ordonné en 2019 à Bouygues Télécom, Free, Orange et SFR d'empêcher l'accès aux sites Sci-Hub et LibGen sous le motif d'atteinte à des droits d'auteur ou droits voisins[66]. Ces sites permettent un accès gratuit à des articles scientifiques qui autrement resteraient restreints par leurs éditeurs académiques derrière un verrou d'accès payant. Le blocage

57. Fabrice Epelboin, 2011, *Kadhafi espionnait sa population avec l'aide de la France* [https://web.archive.org/web/20150629233215/https://reflets.info/kadhafi-espionnait-sa-population-avec-l%E2%80%99aide-de-la-france/].

58. Reflets.info, 2011, *Qatar : Le Finger tendu bien haut d'Amesys* [https://web.archive.org/web/20200923032548/https://reflets.info/articles/qatar-le-finger-tendu-bien-haut-d-amesys].

59. Jean Marc Manach, 2011, *Amesys surveille aussi la France* [https://web.archive.org/web/20171011205936/http://owni.fr/2011/10/18/amesys-surveille-france-takieddine-libye-eagle-dga-dgse-bull/].

60. LCEN, *op. cit.*, article 6-3 [https://www.legifrance.gouv.fr/loda/article_lc/LEGIARTI000043969099], créé par Journal Officiel de la République Française, 2021, *loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République* [https://www.legifrance.gouv.fr/jorf/id/JORFARTI000043964844].

61. Légifrance, 2015, *décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique* [https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030195477/].

62. Légifrance, 2020, article L336-2 du code de la propriété intellectuelle modifié par *Ordonnance n° 2019-738 du 17 juillet 2019* [https://www.legifrance.gouv.fr/codes/id/LEGIARTI000033688218].

63. Tribunal de grande instance de Paris, 2011, *Jugement en référé du 14 octobre 2011* [https://data.over-blog-kiwi.com/1/13/34/21/20140707/ob_2fbf9e_jugement-tgi-paris-14-octobre-2011-gua.pdf].

64. Un site miroir est une copie exacte d'un autre site web.

65. Legalis, 2012, *ordonnance de référé rendue le 10 février 2012* [https://www.legalis.net/jurisprudences/tribunal-de-grande-instance-de-paris-ordonnance-de-refere-10-fevrier-2012/].

66. Numerama, 2019, Sci-Hub et LibGen luttent pour la diffusion gratuite du savoir scientifique : la France ordonne leur blocage [https://www.numerama.com/sciences/477218-sci-hub-et-libgen-luttent-pour-la-diffusion-gratuite-du-savoir-scientifique-la-france-ordonne-leur-blocage.html].

portant sur 57 domaines a été prononcé pour un an. Il est notable que les FAI n'ont pas souhaité s'opposer à cette mesure de censure. En 2021, un nouveau jugement a élargit la liste à 278 domaines[67].

28.4.1 Bloquer l'accès au fournisseur de ressources

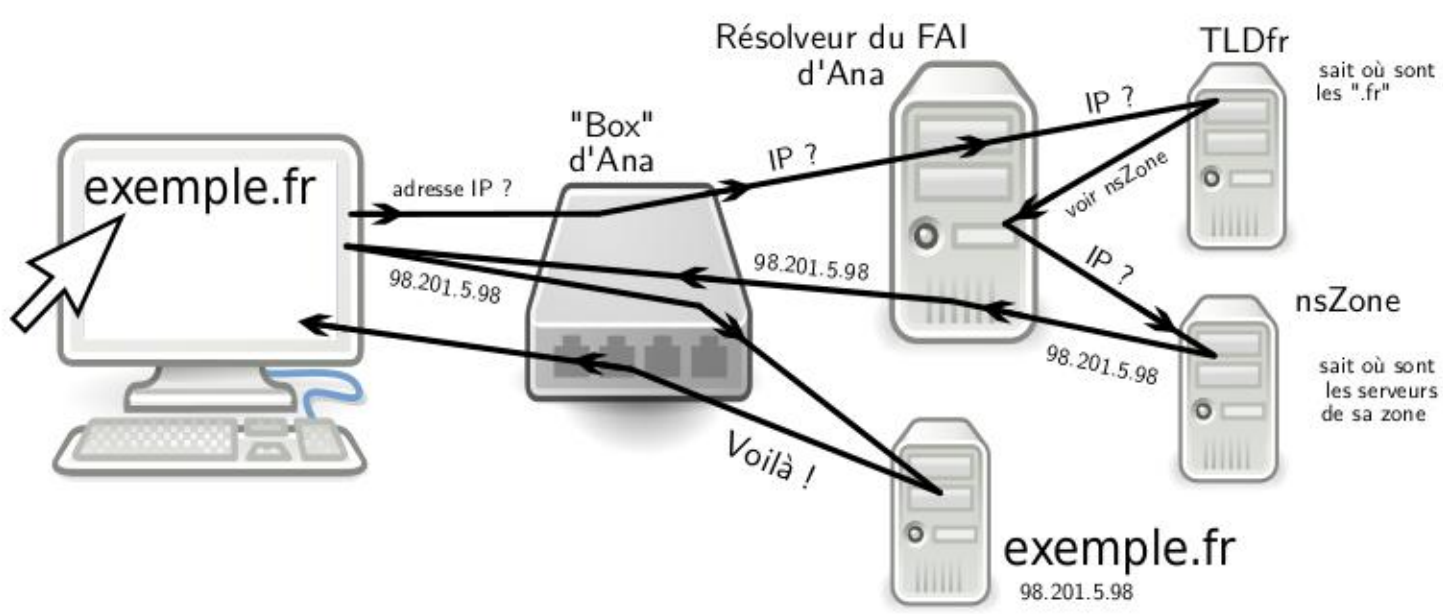
Penchons-nous maintenant sur les différents moyens qui permettent de bloquer l'accès à une ressource sur Internet.

Attaque sur les noms de domaines

Il est possible de détourner le trafic qui devait aller vers un certain serveur en modifiant l'annuaire utilisé pour passer de son nom de domaine à son adresse IP, c'est-à-dire le DNS.

page 210

Cela peut se faire à différents niveaux.



Les étapes clefs d'une requête DNS

Les organismes gestionnaires de l'annuaire des noms de domaines Pour des raisons d'efficacité et de robustesse, le système d'annuaire (DNS) est géré par diverses organisations, en un système d'information hiérarchisé et distribué. La base de données globale du DNS est donc répartie entre plusieurs serveurs de noms, chacun de ces serveurs ne maintenant qu'une partie de la base.

Certaines organisations ou entreprises se chargent du DNS des domaines dits *de premier niveau* (TLD, Top Level Domain), qui correspondent aux caractères situés après le dernier point du nom de domaine, tels que .com, .fr, .org, *etc.* Ainsi tous les domaines finissant par .fr relèvent du serveur de nom de l'AFNIC, une association créée à cet effet en 1997. Les domaines finissant par .com sont quant à eux gérés par Verisign, une Société Anonyme états-unienne cotée en bourse.

On peut lire la liste des organisations et entreprises qui sont chargées de gérer les TLD sur le site web de l'IANA[68] (Internet Assigned Numbers Authority), qui gère les serveurs racine du DNS, celui qui fait autorité sur tous les autres.

Si les gestionnaires au niveau des TLD ont un rôle purement technique (tenir à jour une liste des domaines dont ils ont la charge), ceux à qui ils délèguent sont généralement des entreprises commerciales (appelées *registrars*) qui vendent des noms de domaine.

On voit maintenant se dessiner une carte des points névralgiques où peut intervenir la censure.

---

67. The Sound Of Science, 2021, [Exclusif] Pourquoi les principaux FAI français bloquent de nouveau Sci-hub et Libgen [https://www.soundofscience.fr/2724].
68. IANA, 2014, *Root Zone Database* [https://www.iana.org/domains/root/db] (en anglais).



Pour aller plus loin…

Ainsi, louer un nom de domaine est une opération distincte d'avoir une IP : par exemple, pour monter son propre site web, il faudra d'une part acheter un nom de domaine et d'autre part trouver un hébergement pour le site, avec une adresse IP qui lui est attachée. Et ensuite mettre en place la liaison entre les deux. Certaines entreprises proposent tous ces services en même temps, mais ce n'est ni systématique ni obligatoire.

Saisie de domaines La saisie de nom de domaine la plus spectaculaire à ce jour fut certainement celle inscrite dans le cadre de la fermeture du site d'hébergement de fichiers megaupload.com par le Département de la Justice des États-Unis. Pour rendre inaccessibles les services de ce site, le FBI a notamment demandé à Verisign, l'entreprise qui gère les *.com*, de modifier ses tables de correspondance afin que cette adresse pointe non plus vers les serveurs de Megaupload mais vers un serveur du FBI indiquant que le site avait été saisi [69].

Cependant, une des premières censures connues par suspension d'un nom de domaine s'est produite, en 2007, au niveau d'un registrar : GoDaddy (le plus important au monde). Dans le cadre d'un conflit entre un de ses clients, seclists.org, et un autre site, myspace.com, GoDaddy prit le parti de ce dernier et modifia sa base de données, rendant, du jour au lendemain et sans avertir personne, le site injoignable [70] (sauf pour les personnes connaissant son adresse IP par cœur).

DNS menteur Enfin, si modifier les annuaires globaux n'est à la portée que de quelques États et sociétés, nombreux sont ceux qui peuvent simplement falsifier leur propre version de l'annuaire : on parle de « DNS menteur ». Ainsi, chaque fournisseur d'accès à Internet a en général ses propres serveurs de noms de domaines (DNS), qui sont utilisés par défaut par ses abonnées.

Quand un serveur de nom de domaines renseigne autre chose que ce qui a été enregistré chez les registrars, on parle aussi de « DNS menteur » [71] ; c'est une violation de la neutralité du net.

page 207

C'est à ce niveau que fonctionne le blocage administratif des sites en France : les FAI doivent modifier leur annuaire pour rediriger les adresses listées par l'*office central de lutte contre la criminalité liée aux technologies de l'information et de la communication* vers une page du ministère de l'intérieur [72].

Les personnes utilisant le FAI Orange ont pu expérimenter ce blocage malgré elles le 17 octobre 2016. À la suite d'une « erreur humaine » « lors de l'actualisation des sites bloqués » [73], le résolveur d'Orange a donné pendant une heure une réponse « fausse » à l'adresse *fr.wikipedia.org* en pointant non pas vers les serveurs de Wikipédia, mais vers une page sur laquelle on pouvait lire « Vous avez été redirigé vers cette page du site du ministère de l'intérieur car vous avez tenté de vous connecter à une page dont

69. Après cette coupure, des milliers d'internautes se sont vus privés de leurs contenus en un claquement de doigts (et pas que de leurs fichiers pirates, au vu des pétitions en ligne et de tous ces gens disant que leur vie professionnelle était ruinée car ils n'avaient plus accès à tous leurs documents).

70. Fyodor, 2007, *Seclists.org shut down by Myspace and GoDaddy* [https://seclists.org/nmap-announce/2007/0] (en anglais).

71. Stephane Bortzmeyer développe un peu le concept [https://www.bortzmeyer.org/dns-menteur.html].

72. Légifrance, 2015, *décret n° 2015-125 du 5 février 2015 relatif au blocage des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique* [https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000030195477].

73. Marc Rees, 2016, *Blocage de Google, OVH et Wikipédia : « on ne cherche pas à vous cacher la vérité » assure Orange*, Nextinpact [https://www.nextinpact.com/article/24123/101785-blocage-google-ovh-et-wikipedia-on-ne-cherche-pas-a-vous-cacher-verite-assure-orange].

le contenu incite à des actes de terrorisme ou fait publiquement l'apologie d'actes de terrorisme » [74].

Déréférencement

Enfin, une façon simple mais efficace d'empêcher l'accès à un site web est de le supprimer des moteurs de recherche et autres annuaires : on parle de déréférencement. Le site existe toujours, mais il n'apparaît plus sur les moteurs de recherche (par exemple Google).

En France, le déréférencement fait partie des techniques de blocage administratif des sites : l'*office central de lutte contre la criminalité liée aux technologies de l'information et de la communication* transmet aux moteurs de recherche ou aux annuaires une liste d'adresses qu'il considère comme ayant du contenu pédopornographique, « provoqu[ant] directement à des actes de terrorisme » ou en faisant « l'apologie » [75]. Ils ont alors 48 heures pour faire en sorte que ces adresses n'aparaissent plus dans leurs résultats. 4 138 demandes de déréférencement ont été faites en 2020, dont 4 ont été annulées après contrôle [76].

28.4.2 Hameçonnage

Dans le même ordre d'idée, l'hameçonnage [77] (appelé également filoutage, ou *phishing* en anglais) consiste à pousser l'internaute à se connecter à un site qui n'est pas celui qu'elle croit être, mais qui y ressemble beaucoup. Par exemple, un site qui ressemble comme deux gouttes d'eau à celui d'une banque, afin d'obtenir des mots de passe de connexion à une interface de gestion de comptes bancaires. Pour cela, les adversaires achètent un nom de domaine qu'on croira être le bon au premier coup d'œil. Il ne leur reste plus qu'à inciter la personne ciblée à se connecter à ce site, généralement en lui faisant peur, par exemple « Nous avons détecté une attaque sur votre compte » ou « Vous avez dépassé votre quota », suit alors la proposition de régulariser la situation en cliquant sur le lien piégé.

Pour que le nom de domaine affiché ressemble lui aussi comme deux gouttes d'eau à celui du site copié, il existe plein de techniques : l'adversaire peut par exemple utiliser des caractères spéciaux qui ont l'apparence des caractères de l'alphabet latin. Ainsi, en substituant un « е » cyrillique à un « e » latin dans *exemple.org*, on obtient une adresse qui s'affiche de façon (quasi) identique à l'originale, mais qui représente pour l'ordinateur une adresse différente ; on trouve parfois aussi des tirets en plus ou en moins (*ma-banque.fr* au lieu de *mabanque.fr*) ; il s'agit parfois d'un nom identique, avec un nom de domaine de premier niveau (*top-level domain*, ou TLD : .com, .net, .org, .fr, *etc.*) différent (*site.com* au lieu de *site.org*) ; certains utilisent aussi des sous-domaines (*paypal.phishing.com* renvoie vers le site de phishing, et non vers *paypal.com*), *etc.*

Une parade intégrée dans les navigateurs web consiste à avertir l'internaute du danger et à lui demander une confirmation avant d'accéder au site suspect [78]. Cela dit, cette

---

74. Yannux, 2016, Copie d'écran de la page du ministère de l'Intérieur, twitter.com [https://pbs.twimg.com/media/Cu9JoGNWAAAQAO9.jpg].

75. Légifrance, 2015, *décret n° 2015-253 du 4 mars 2015 relatif au déréférencement des sites provoquant à des actes de terrorisme ou en faisant l'apologie et des sites diffusant des images et représentations de mineurs à caractère pornographique* [https://www.legifrance.gouv.fr/loda/id/JORFTEXT000030313562/].

76. Alexandre Linden, 2021, *rapport d'activité 2020 de la personnalité qualifiée prévue par l'article 6-1 de la loi n° 2004-575 du 21 juin 2004 créé par la loi n° 2014-1353 du 13 novembre 2014 renforçant les dispositions relatives à la lutte contre le terrorisme*, CNIL [https://www.cnil.fr/sites/default/files/atoms/files/rapport_linden_2020.pdf], p. 9.

77. Voir à ce sujet Wikipédia, 2014, *Hameçonnage* [https://fr.wikipedia.org/wiki/Hameçonnage], qui explique notamment quelques parades (partielles) à cette attaque.

78. Mozilla, 2022, *Comment fonctionnent les protections contre l'hameçonnage et les logiciels malveillants ?* [https://support.mozilla.org/fr/kb/comment-fonctionne-protection-contre-hame%C3%A7onnage-et-logiciels-malveillants]

solution nécessite que le navigateur web contacte une base de données centralisée, recensant les sites considérés comme malveillants. Cela peut poser des problèmes de discrétion : le serveur hébergeant cette liste aura nécessairement connaissance des sites d'hameçonnage ou de logociels malveillants que l'on visite.

28.4.3 Attaquer le serveur

Une autre catégorie d'attaques consiste, pour l'adversaire, à s'en prendre à l'ordinateur qui héberge la ressource qui l'intéresse. Ça peut se faire physiquement ou à distance.

Saisie de serveurs

Il s'agit tout simplement pour une adversaire qui en a les moyens, par exemple la police ou la justice, d'aller là où se trouve l'ordinateur auquel elle s'intéresse. L'adversaire peut alors s'emparer de la machine, ou copier les données qu'elle abrite. Elle pourra ensuite étudier toutes les traces qui ont été laissées dessus par les personnes qui s'y sont connectées… du moins si son disque dur n'est pas chiffré.

page 27

page 47

Au moins quatorze serveurs ont été saisis par la justice en Europe entre 1995 et 2007 [79]. Ainsi en 2007, un serveur de Greenpeace Belgique a été emmené par la police belge suite à une plainte pour « association de malfaiteurs » d'une compagnie d'électricité belge [80] contre laquelle l'organisation écologiste avait appelé à manifester.

Plus récemment, au printemps 2017, un certain nombre de serveurs appartenant au réseau d'anonymisation Tor ont été saisis [81] en lien, ou au moins avec le prétexte d'une enquête sur une attaque informatique qui transitait par ce réseau [82].

page 261

Piratage de serveurs

Comme tout ordinateur, un serveur peut être *piraté* : cela consiste pour l'attaquante à s'introduire « par effraction » dans l'ordinateur. Des erreurs de conception ou de programmation, qui permettent de détourner le fonctionnement d'un programme et de s'introduire dans l'ordinateur sur lequel il fonctionne, sont régulièrement découvertes dans les programmes couramment utilisés sur les serveurs. Des erreurs dans la configuration des logiciels de la part des admins de ces serveurs sont aussi possibles.

Ainsi, en 2014, l'exploitation de failles dans le logiciel de publication utilisé sur le site de Gamma International, la société à l'origine du logiciel d'espionnage FinFisher, a permis à un pirate de s'introduire sur leur serveur [83]. Cela lui a donné accès à 40 giga-octets de documents incluant une liste de leurs clients, des documents sur le fonctionnement et l'efficacité de leur logiciel d'espionnage ou encore des portions de son code source [84].

page 39

Les failles qui rendent ce genre de piratage possible ne sont pas rares, et n'importe quel serveur peut être touché. Une fois introduits dans le serveur, les pirates peuvent potentiellement avoir accès à distance à toutes les données enregistrées sur celui-ci.

Même sans s'introduire dans le serveur, il est possible de découvrir puis d'exploiter des failles dans les logiciels pour en exfiltrer des informations auxquelles n'importe

79. Globenet, 2007, *Les saisies de serveurs en Europe : un historique* [https://www.globenet.org/Les-saisies-de-serveurs-en-Europe.html?start_aff=6].

80. Gérard De Selys, 2008, *Greenpeace, association de malfaiteurs !*, Articulations n°33, CESEP [https://archive.org/download/articulations-33/ARTICULATIONS_33.pdf], p. 7.

81. Guénaël Pépin, 2017, *WannaCrypt : des nœuds Tor saisis par les autorités françaises* [https://www.nextinpact.com/article/26455/104302-wannacrypt-nuds-tor-saisis-par-autorites-francaises].

82. Wikipédia, 2021, *WannaCry* [https://fr.wikipedia.org/wiki/WannaCry].

83. Phineas Fisher, 2014, *Hack Back – DIY Guide for those without the patience to wait for whistleblowers* [https://gist.github.com/vlamer/2c2ec2ca80a84ab21a32#file-gistfile1-txt-L171] (en anglais).

84. Wikipedia, Phineas Fisher [https://en.wikipedia.org/wiki/Phineas_Fisher] (en anglais).

qui ne devrait pas avoir accès. C'est ce qui a permis la fameuse fuite de données personnelles de 500 millions de comptes Facebook [85] diffusées à partir de juin 2020.

Attaque par déni de service

Sans saisir le serveur ni même le pirater, il est possible d'empêcher celui-ci de fonctionner en le saturant : l'adversaire fait en sorte que de très nombreux robots tentent en permanence de se connecter au site à attaquer. Au-delà d'un certain nombre de requêtes, le logiciel serveur est débordé et n'arrive plus à répondre : le site est alors inaccessible. On appelle cette attaque une *attaque par déni de service* [86]. Les robots utilisés pour ce type d'attaque sont souvent des logiciels malveillants installés sur des ordinateurs personnels à l'insu de leurs propriétaires.

page 210
page 32

28.4.4 Sur le trajet

Enfin, une adversaire qui contrôle une partie du réseau — comme un fournisseur d'accès à Internet — peut écouter ou détourner des paquets de plusieurs manières.

Filtrage

Comme évoqué précédemment, une adversaire qui contrôle l'un des routeurs par lesquels passe le trafic entre une internaute et une ressource peut lire plus ou moins en profondeur le contenu des paquets et éventuellement le modifier, et ce d'autant plus facilement s'il n'est pas chiffré.

page 217
page 206

De nos jours, quasiment tous les fournisseurs d'accès à Internet pratiquent ce genre d'inspection, le *DPI*, a minima à des fins de statistiques. De plus, ils sont de plus en plus nombreux, de façon plus ou moins discrète, plus ou moins assumée, à s'en servir pour faire passer certains paquets avant les autres, en fonction de leur destination ou de l'application à laquelle ils correspondent. Par exemple pour ralentir la vidéo à la demande, qui génère beaucoup de trafic (et donc leur coûte cher), et privilégier le téléphone par Internet [87]. Ce type de moyens est par exemple utilisé par SFR [88] afin de modifier les pages web visitées par ses abonnées en 3G [89].

page 229

Le déploiement massif d'équipements permettant cet examen approfondi des paquets rend beaucoup plus facile une surveillance aux portes des réseaux des FAI.

En analysant ce type de données, les gouvernements peuvent identifier la position d'une personne, de ses relations et des membres d'un groupe, tels que « des opposants politiques » [90]. De tels systèmes ont été vendus par des sociétés occidentales à la Tunisie, à l'Égypte, à la Libye, au Bahreïn et à la Syrie [91], et sont également en service dans certains pays occidentaux. Ceux-ci permettent, sur la base d'une surveillance de masse, de cibler des internautes et de filtrer, censurer du contenu.

page 229

L'utilisation de cette technique, en Espagne par exemple, a permis à certains FAI de surveiller le trafic [92] de ses utilisatrices pour les empêcher d'accéder au site web de

85. Elise Viniacourt, 2021, *Facebook : les données de 533 millions d'utilisateurs en fuite sur le Web*, Liberation.fr [https://www.liberation.fr/economie/economie-numerique/facebook-les-donnees-de-533-millions-dutilisateurs-en-fuite-sur-le-web-20210406_FNRIQR4PXBF5BK6ALSEREIOPOY/].

86. Wikipédia, 2021, *Attaque par déni de service* [https://fr.wikipedia.org/wiki/Attaque_par_d%C3%A9ni_de_service].

87. Wikipédia, 2021, *Deep packet inspection* [https://fr.wikipedia.org/wiki/Deep_packet_inspection]

88. bluetouff, 2013, *SFR modifie le source HTML des pages que vous visitez en 3G* [https://web.archive.org/web/20150629235630/https://reflets.info/sfr-modifie-le-source-html-des-pages-que-vous-visitez-en-3g/].

89. Wikipédia, 2021, *3G* [https://fr.wikipedia.org/wiki/3G].

90. Elaman, 2011, *Communications monitoring solutions* [https://wikileaks.org/spyfiles/docs/elaman/188_communications-monitoring-solutions.html] (en anglais).

91. Jean Marc Manach, 2011, *Internet massivement surveillé* [https://web.archive.org/web/20190411142441/http://owni.fr/2011/12/01/spy-files-interceptions-ecoutes-wikileaks-qosmos-amesys-libye-syrie/].

92. Sans Censure, 2020, *Sommaire du rapport technique et de la situation actuelle du site WomenOnWeb* [https://sindominio.net/sincensura/fr/post/censura/].

l'ONG Women on Web [https://www.womenonweb.org/fr/], qui fournit au niveau mondial des informations et de l'aide pour avorter.

Écoutes

À l'instar des bonnes vieilles écoutes téléphoniques, il est tout à fait possible d'enregistrer tout ou partie des données qui passent par un lien réseau : on parle d'« interceptions IP ». Cela permet par exemple d'écouter tout le trafic échangé par un serveur, ou celui qui passe par une connexion ADSL domestique.

En France, de telles interceptions sont autorisées dans le cadre d'une enquête judiciaire, mais aussi pour la « prévention du terrorisme » pour recueillir « des informations ou documents [...] relatifs à une personne [...] susceptible d'être en lien avec une menace » mais aussi relatifs à des « personnes appartenant à l'entourage de la personne concernée ».[93]

Si l'on ne prend pas de précautions particulières, une interception IP révèle à une adversaire une bonne partie de nos activités sur Internet : pages web visitées, emails et leurs contenus, conversations de messagerie instantanée... tout ce qui sort de notre ordinateur « en clair ». Le chiffrement des communications rend l'analyse du contenu issu de ces écoutes beaucoup plus difficile : l'adversaire a toujours accès aux données échangées, mais elle ne peut pas les comprendre et les exploiter directement. Elle peut alors essayer de casser le chiffrement utilisé... ou tenter de contourner la façon dont il est mis en œuvre. On parlera plus loin de ces questions liées au chiffrement. page 249 Dans tous les cas, l'adversaire aura toujours accès à un certain nombre d'informations précieuses, comme par exemple les adresses IP des différents interlocutrices impliqués page 202 dans une communication.

Analyse du trafic réseau

Lorsque le trafic est chiffré, il reste possible de mettre en place des attaques plus subtiles. Une adversaire pouvant écouter le trafic réseau, même sans accès au contenu des données, dispose d'autres indices comme la quantité d'informations transmises à un moment donné.

Ainsi, si Ana envoie 2 Mo de données chiffrées vers un site web de publication, et qu'un nouveau document de 2 Mo apparaît sur ce site quelques instants plus tard, cette adversaire pourra en déduire qu'il est probable que ce soit Ana qui ait envoyé ce document.

En étudiant la quantité d'informations transmises par unité de temps, les adversaires peuvent aussi dessiner une « forme » : on l'appellera le *motif de trafic* (*traffic pattern*)[94]. Le contenu d'une page web chiffrée n'aura ainsi pas le même motif qu'une conversation de messagerie instantanée chiffrée.

De plus, si un même motif de trafic est observé à deux points du réseau, les adversaires peuvent supposer qu'il s'agit d'une même communication.

Pour prendre un exemple précis : considérons des adversaires qui écoutent la connexion ADSL d'Ana, et qui observent du trafic chiffré qu'elles ne peuvent pas déchiffrer, mais qui soupçonnent Ana de discuter avec Bea par messagerie instantanée chiffrée. Considérons qu'elles ont également les moyens de mettre sous écoute la connexion de Bea. Si elles observent une forme similaire entre le trafic sortant de chez Ana et celles entrant chez Bea quelques (milli)secondes plus tard, elles seront confortées dans leur hypothèse — sans toutefois disposer d'une preuve formelle.

---

93. Légifrance, 2021, *Code de la sécurité intérieure*, article L851-2 [https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000043887533/].

94. Yin Zhang, Vern Paxson, 2000, *Detecting Stepping Stones*, Proceedings of the 9th USENIX Security Symposium [https://www.usenix.org/legacy/events/sec2000/full_papers/zhangstepping/zhangstepping.pdf] (en anglais).

Ce type d'attaque permet de confirmer une hypothèse préexistante, mais pas d'en élaborer une à partir des seules informations collectées, à moins que les adversaires n'aient les moyens d'écouter *tout* le réseau où se situe le trafic entre Bea et Ana, et qu'elles disposent d'une puissance de calcul colossale. L'existence d'adversaires globaux de ce type est techniquement possible, mais peu réaliste. Par contre, des agences comme la NSA sont capables de mener ce type d'attaque, au moins à l'échelle de leur pays : la NSA dispose d'une puissance de calcul qui peut être suffisante et des fuites indiquent qu'elle écouterait 75 % du trafic Internet des États-Unis [95].

28.4.5 Piratage du client

page 31

L'ordinateur de l'internaute, lui aussi, peut être une cible. De la même façon que dans un serveur, des attaquantes peuvent s'introduire par effraction dans un ordinateur personnel. Des erreurs de programmation ou d'autres failles dans le système d'exploitation ou dans les applications installées permettent parfois à des adversaires d'effectuer un tel piratage — légal ou illégal — depuis Internet, sans avoir d'accès physique à la machine. De plus, l'intrusion peut être facilitée par de mauvaises pratiques de la part des utilisatrices, comme ouvrir une pièce jointe frauduleuse ou installer des programmes trouvés au hasard sur le web.

Un groupe de hackers allemands renommé, le Chaos Computer Club, a mis la main sur un mouchard utilisé par la police allemande qui lui permettait d'espionner et de contrôler un ordinateur à distance [96]. De tels mouchards peuvent être installés à distance et sont autorisés par la loi française.

page 31

Mais « l'espionnage à distance » n'est pas seulement réservé aux pratiques policières. Aux États-Unis, c'est un lycée qui s'est lancé dans l'espionnage de grande ampleur. Sous couvert de vouloir « retrouver des ordinateurs portables volés ou perdus », le lycée avait installé une « fonction » permettant d'allumer, au bon vouloir de l'établissement, la webcam des quelques milliers d'ordinateurs distribués aux élèves. L'affaire a été révélée fin 2009 : un des élèves s'est vu reprocher d'avoir eu un « comportement inapproprié », en l'occurrence d'avoir consommé de la drogue. Le responsable accusant cet élève produisit, en guise de preuve, une photo qui s'est révélée avoir été prise à l'insu de l'étudiant, par la webcam de son ordinateur lorsqu'il était chez lui dans sa chambre [97] !

28.5 En conclusion

Identification de l'internaute par son adresse IP, lecture de l'origine et de la destination des paquets par le biais de leurs en-têtes, enregistrement de diverses informations à différentes étapes du parcours, voire accès au contenu même des échanges… tout ceci est plus ou moins simple en fonction de l'entité impliquée.

Pirate, publicitaire, gendarme de Saint-Tropez ou NSA n'ont en effet pas les mêmes possibilités techniques et légales d'accès aux traces évoquées dans ce chapitre.

On se contentera simplement d'observer, pour conclure, que la manière dont Internet fut conçu et est le plus couramment utilisé est quasiment transparente pour des adversaires un tant soit peu attentives… à moins d'utiliser toute une série de parades adaptées pour rendre ces indiscrétions plus difficiles ; ces parades seront évoquées plus loin.

---

95. latribune.fr, 2012, *À peine 25% du trafic web états-unien échappe à la surveillance du NSA* [https://www.latribune.fr/actualites/economie/international/20130821trib000781040/a-peine-25-du-trafic-web-americain-echappe-a-la-surveillance-du-nsa.html].

96. Mark Rees, 2011, *Le CCC dissèque un cheval de Troie gouvernemental troué*, PCInpact [https://www.nextinpact.com/archive/66279-loppsi-ccc-cheval-de-troie-faille-malware.htm].

97. Me, myself and the Internet, 2011, *Mais qui surveillera les surveillants ?* [https://web.archive.org/web/20180107033100/https://memyselfandinternet.wordpress.com/2011/02/14/%C2%AB-mais-qui-surveillera-les-surveillants-%C2%BB/].

Chapitre 29

Web 2.0

Le terme web 2.0 est de nos jours presque une banalité. Pour autant, il semble difficile d'en saisir la véritable consistance à force d'emploi à tort et à travers ou au contraire de définitions parfois trop techniques[1].

Il s'agit avant tout d'un terme marketing, qui définit une évolution du web à une époque où la massification de l'accès à l'Internet en fait un marché juteux. Nombre d'entreprises ne peuvent plus se permettre de l'ignorer, que leur domaine d'activité soit les médias, la communication ou le commerce. Il a bien fallu qu'elles adaptent leur « business model » à ce nouveau marché.

L'arrivée de ces nouveaux acteurs sur un web jusque-là composé principalement d'universitaires et de passionnées a transformé la conception des sites web, et de ce fait l'utilisation qu'en ont les internautes.

Au-delà de ces formulations marketing, nous allons tenter de voir plus précisément comment ces évolutions se manifestent aux internautes, et les changements sur le fonctionnement du réseau qu'elles impliquent.

29.1 Des « applications Internet riches »...

L'une de ces évolutions porte sur l'interactivité des sites web. Ce ne sont plus seulement des pages statiques à l'image de celles d'un livre ou d'un magazine. En utilisant des technologies pré-existantes au web 2.0 comme le JavaScript, les sites web ressemblent de plus en plus à des applications telles que celles que l'on trouve sur nos ordinateurs personnels : des sites web dynamiques répondant aux sollicitations de l'internaute.

page 210

De plus, la plupart des logiciels habituellement installés sur un ordinateur personnel sont transposés en version web, et deviennent accessibles depuis un navigateur web. On voit même apparaître des systèmes d'exploitation, comme Chrome OS, conçus entièrement selon ce principe. Ce mouvement, ce déplacement du logiciel installé sur l'ordinateur vers le web, est notamment une réponse aux soucis d'incompatibilité des logiciels, de licences et de mises à jour.

page 22

En effet, plus besoin d'installation : une simple connexion à Internet et on dispose, *via* un navigateur web, de la plupart des applications traditionnelles : traitement de texte, tableur, messagerie électronique, agenda collaboratif, système de partage de fichiers, lecteur de musique, *etc.*

Ainsi *Google Drive* permet entre autres de rédiger des documents ou bien de faire sa comptabilité en ligne. Mais ce service permet également de la partager avec des amies, des collègues, *etc.*

1. L'exposé d'ouverture de la conférence de O'Reilly et Battelle sur le Web 2.0, cité par Wikipédia, 2014, *Web 2.0* [https://fr.wikipedia.org/wiki/Web_2.0] est un bel exemple de définition trop technique.

Des personnes vont même jusqu'à voir dans cette possibilité d'accéder à ces outils en ligne depuis « n'importe quel ordinateur, dans n'importe quel pays et à n'importe quelle heure » [2] une façon de concilier le travail avec d'éventuels problèmes médicaux, météorologiques voir même en cas de pandémie...

Plus besoin d'aller au bureau, « un ordinateur connecté à Internet suffit à reconstituer immédiatement l'environnement de travail ».

29.2 ... et des internautes bénévoles

En arrivant sur le marché web, ces entreprises durent revoir leur modèle économique. L'audience de l'Internet grandissant, il n'était pas possible de financer un site web sur la seule publicité, tout en payant une armée de rédactrices pour fournir du contenu en quantité toujours plus importante.

Les fournisseurs de services utilisèrent une technique déjà présente sur le web depuis longtemps : miser sur la participation des internautes. Ce sont dorénavant celles-ci qui se chargent de rédiger le contenu qui alimente les sites. Les fournisseurs de services se contentent d'héberger les données et de fournir l'interface permettant d'y accéder, mais aussi et surtout d'ajouter de la publicité autour... et d'encaisser la monnaie.

Ainsi, la plateforme de partage de vidéo YouTube a, pendant de nombreuses années, permis à ses internautes de mettre en ligne et de visionner gratuitement les vidéos de leur choix sans contrepartie visible. Aujourd'hui, suite au succès et fort de son monopole, la plupart des personnes voulant visionner et partager des vidéos sont dépendantes de cette plateforme, ce qui permet alors à YouTube d'imposer petit à petit de la publicité. Au début, elle se situait sur un bandeau à côté de l'image, puis sur un bandeau transparent sur l'image et maintenant c'est tout simplement des vidéos incrustées au début ou au milieu de celle que l'on souhaite visionner.

Autre avantage de cette solution pour les fournisseurs de services, les internautes fournissent ainsi plus ou moins consciemment tout un ensemble de données [3] qu'il est ensuite possible de monnayer, notamment en constituant des profils de consommatrices et en adaptant les publicités affichées au public.

page 221

Il est ainsi courant que les internautes n'utilisent plus Internet uniquement pour télécharger des films ou aller y lire leur périodique favori. De plus en plus, par exemple *via* le remplissage de leur page Facebook, les internautes produisent du contenu et l'offrent pour ainsi dire aux hébergeurs ou autres entreprises qui fournissent ces services. L'internaute va « de sa propre initiative » mettre en ligne la liste de la musique qu'elle écoute, les photos de ses vacances en Meuse, ou encore ses cours d'histoire contemporaine pour les partager avec ses camarades de classe.

Bien sûr, en fournissant du contenu, on fournit aussi des informations sur soi, informations que les regards indiscrets des publicitaires et autres adversaires ne manqueront pas d'utiliser.

page 221

page 223

29.3 Centralisation des données

L'utilisation d'espace de stockage via Internet va en général de pair avec la centralisation des données des internautes. Les espaces de stockage en ligne les plus utilisés sont en effet aux mains des géants du web.

---

2. Lionel Damm et Jean-Luc Synave, 2009, *Entrepreneur 2.0, la boîte à outils de la compétitivité... à petit frais* [https://www.confederationconstruction.be/Portals/28/UserFiles/Files/WP2guideentrepreneurweb20.pdf].

3. Fanny Georges, Antoine Seilles, Jean Sallantin, 2010, *Des illusions de l'anonymat – Les stratégies de préservation des données personnelles à l'épreuve du Web 2.0*, Terminal numéro 105, Technologies et usages de l'anonymat à l'heure d'Internet [https://www.revue-terminal.org/articles/105/introDossierAnonymat105.pdf].

L'utilisation d'applications en ligne signifie entre autres que les documents ne sont plus stockés sur un ordinateur personnel, un disque dur ou une clé USB. Ils se retrouvent sur des serveurs distants comme ceux de Google[4], dans des centres de traitement de données, loin de l'internaute, géographiquement comme techniquement. Autrement dit, l'internaute perd du pouvoir sur ses données.

Une simple absence de connexion Internet et il devient impossible d'avoir accès à ses documents, à moins d'en avoir effectué une sauvegarde. Ce déplacement du stockage rend également impossible de pouvoir effacer avec certitude et de façon sécurisée les documents qui y sont placés.

page 42

Cette tendance à faire migrer données et applications de l'ordinateur personnel vers Internet crée du même coup une « dépendance à la connexion ». Quand toute sa musique, son carnet d'adresses et les cartes de sa ville n'existent plus que par Internet, il devient plus difficile d'imaginer utiliser un ordinateur *hors connexion*. Or toute connexion à Internet ouvre des portes. Et plus un ordinateur est exposé, plus il est difficile de garantir sa sécurité — de l'anonymat de l'internaute qui l'utilise à la confidentialité des données qu'on lui confie.

page 221

Rien ne nous garantit non plus que nos données stockées en ligne soient bien gardées. Même si une organisation nous donne aujourd'hui tous les gages de sécurité (et encore, qu'est-ce qui nous le prouve ?) elle n'est de toute façon pas à l'abri, demain, de la découverte d'une faille, ou d'une erreur de configuration d'un programme qui donnerait accès à ces données à n'importe qui, comme ce fut le cas pour le service de stockage chiffré de données en ligne Dropbox[5].

page 235

Les entreprises à qui on confie nos données peuvent aussi, à leur initiative supprimer un contenu[6], supprimer notre compte[7], voire fermer leurs services sans que l'on y puisse rien — ou simplement faire faillite. Et quand les états s'en mêlent, une décision de justice peut fermer un service comme dans le cas de Megaupload ou un simple signalement émanant d'une autorité d'un autre état pourra désormais forcer un fournisseur de service en ligne à retirer en moins d'une heure un contenu qualifié de terroriste[8].

page 233

29.4 Mainmise sur les programmes

La plupart du temps, ces applications en ligne sont développées de manière plus fermée que les applications libres que l'on peut installer sur son ordinateur. Lorsque Google ou Facebook décident de modifier l'interface ou de changer le fonctionnement du service, de « faire du rangement », l'internaute n'a pas son mot à dire.

page 39

De plus, l'interactivité de ces applications web implique qu'une partie de leur programme soit exécutée sur l'ordinateur client (le nôtre), à travers des technologies comme JavaScript ou Java. Ces technologies sont désormais activées, par défaut, dans nos navigateurs web, et ceci pour tous les sites. C'est sympa, pratique, moderne. Mais ces technologies posent quelques problèmes quant à la sécurité de nos ordinateurs, et

page 214

4. Le paragraphe *Éléments que vous créez ou que vous nous fournissez* des Règles de confidentialité [https://policies.google.com/privacy?hl=fr#infocollect] des services fournis par Google démontre assez clairement l'absence de pouvoir concret d'une internaute sur les contenus qu'elle a stocké en ligne. « Ce qui est à vous, reste à vous » mais libre à Google d'en faire ce qu'il en a envie tant que vous laissez votre contenu sur ses serveurs.

5. Vincent Hermann, 2011, *Dropbox admet posséder un double des clés d'accès aux données* [https://www.nextinpact.com/archive/64460-dropbox-conditions-utilisation-chiffrement-securite.htm].

6. Marie Claire, 2018, *Cancer du sein : Facebook censure (encore) des publications sur la mastectomie* [https://www.marieclaire.fr/cancer-du-sein-facebook-censure-publications-mastectomie,1249169.asp].

7. Owni, 2011, *Après 7 ans d'utilisation, il se fait supprimer son compte Google, donc les emails, le calendriers, les docs,* etc. [https://web.archive.org/web/20200224160152/http://owni.fr/2011/08/29/google-suppression-compte-donnees-personnelles-vie-privee-god/].

8. Article 17 du *règlement (UE) 2021/784 du Parlement européen et du Conseil du 29 avril 2021 relatif à la lutte contre la diffusion des contenus à caractère terroriste en ligne* [https://eur-lex.europa.eu/legal-content/FR/TXT/HTML/?uri=CELEX:32021R0784].

donc quant à la confidentialité de nos données [9]... Il est cependant possible [10] de n'autoriser leur usage que site par site, en fonction de la confiance qu'on leur accorde.

29.5 De la centralisation à l'auto-hébergement décentralisé

Face à une centralisation toujours croissante des données et des applications, peut-on profiter des avantages d'un réseau participatif et interactif sans perdre le contrôle sur nos données ? Le défi paraît ardu. Mais des travaux sont en cours pour développer des applications Internet qui fonctionneraient de façon décentralisée chez chaque internaute au lieu d'être centralisées sur quelques serveurs. Des projets comme les médias sociaux de pair à pair, Mastodon [11], Nextcloud [12], la distribution YunoHost [13], ou encore la BriqueInter.net [14] travaillent dans cette direction.

En attendant qu'ils soient aussi simples d'utilisation que les solutions proposées par les géants du web 2.0, il est d'ores et déjà possible, en mettant un peu les mains dans le cambouis, d'héberger soi-même la plupart des services qu'on souhaite offrir ou utiliser.

9. Nous n'avons pas de contrôle sur les programmes JavaScript ou Java qui sont envoyés par l'application web. Il est donc tout à fait possible que des mouchards ou d'autres fonctionnalités malveillantes [page 32] soient incluses parmi ces programmes et soient alors exécutées par notre navigateur.

10. Suivant le navigateur web qu'on utilise, il existe des *extensions*, comme noscript [https://noscript.net], qui permettent de gérer ces paramètres.

11. Mastodon [https://joinmastodon.org/].

12. Nextcloud [https://nextcloud.com/fr_FR/].

13. Page francophone du projet YunoHost [https://yunohost.org/#/index_fr].

14. La BriqueInter.net [https://labriqueinter.net/].

Chapitre 30

Identités contextuelles

L'un des présupposés de ce *guide* est le désir que nos faits, gestes et pensées ne soient pas automatiquement, voire pas du tout, reliés à notre identité civile.

Pour autant, il peut être nécessaire ou simplement préférable de savoir à qui on s'adresse : pour entamer une discussion sur un forum ou envoyer des emails par exemple. Dans ces cas-là, avoir une *identité*, c'est-à-dire être identifiable par notre correspondant, simplifie la communication.

30.1 Définitions

Pour commencer, deux définitions :

- l'*anonymat*, c'est ne pas laisser apparaître de nom ;
- le *pseudonymat*, c'est choisir et utiliser un nom différent de son identité civile.

De par son fonctionnement, il est très difficile d'être *anonyme* ou de rester un *pseudonyme* sur Internet.

30.1.1 Pseudos

Un *pseudo*, c'est une identité qui n'est pas celle assignée à une personne par l'état civil. On peut choisir de se faire appeler « Falaise », « Amazone enragée », « Zigouigoui », ou même « Jeanne Dupont ». En conservant un même pseudonyme lors de différents échanges, nos interlocutrices auront de bonnes chances de penser que les divers messages écrits par ce *pseudo* viennent de la même personne : ils pourront alors nous répondre, mais ne pourront pas venir nous casser la gueule en cas de désaccord.

Il faut néanmoins être conscient lors du choix d'un pseudonyme que celui-ci peut en lui-même être un indice qui permet de remonter à la personne qui l'utilise, au moins pour les personnes qui connaissent déjà ce pseudonyme par ailleurs.

30.1.2 Identité contextuelle

> *Bea télécharge aussitôt le document et l'ouvre dans l'éditeur de texte. Elle le parcourt rapidement, et supprime quelques informations qu'il vaut mieux ne pas laisser. Après avoir entré son identifiant et son mot de passe pour se connecter au blog, Bea copie-colle le contenu du document depuis sa boîte mail, et clique sur* Envoyer. *« Espérons que cela inspire d'autres personnes !*

En reprenant le fil de notre histoire introductive, l'identité contextuelle correspondrait à « une ou plusieurs personnes publiant des informations sur la mairesse », et la personne physique à Bea.

page 194

Que l'on discute avec des personnes avec qui on partage la passion de l'escalade, ou de notre projet professionnel avec une conseillère Pôle emploi ou encore avec notre banquière, la teneur des propos, la manière dont on en parle n'est pas la même. D'un côté on sera plutôt exaltée, aventureuse, de l'autre plutôt sobre, sérieuse, *etc.* : on peut donc parler d'identité contextuelle.

Il en va de même lors de l'utilisation d'un ordinateur : quand on poste un message sur un forum de rencontre, quand on annonce une grosse soirée sur son compte Facebook ou quand on répond à un email de papa, on fait appel à différentes identités contextuelles. Celles-ci peuvent bien évidemment être mélangées et donc rejoindre une même identité composée des trois identités contextuelles mobilisées ci-dessus, la célibataire, la fêtarde, la fille de.

Une identité contextuelle est donc un fragment d'une « identité » globale censée correspondre à une personne physique, ou à un groupe. Tout comme une photographie est un instantané d'une personne ou d'un groupe, sous un certain angle, à un certain âge, *etc.*

page 213

Être absolument anonyme sur Internet, c'est très compliqué : comme on l'a vu, de nombreuses traces sont enregistrées *via* le réseau lors de son utilisation. Ce phénomène est d'autant plus vrai avec les médias sociaux pour lesquels la génération d'une identité unique et traçable est un fond de commerce[1]. Il est impossible de ne laisser aucune trace, mais il est peut-être possible de laisser des traces qui ne ramènent nulle part.

On rencontre des difficultés similaires lorsqu'on fait le choix du pseudonymat : plus on utilise un *pseudo*, plus les traces qu'on laisse s'accumulent. Des petits indices qui, une fois recoupés, peuvent permettre de révéler l'identité civile qui correspond à un pseudonyme.

30.2 De l'identité contextuelle à l'identité civile

Il existe différentes manières, plus ou moins offensives, de mettre à mal un pseudonyme ou de révéler le lien entre une identité contextuelle et la ou les personnes physiques qui l'utilisent.

30.2.1 Le recoupement

page préc.

En partant de l'exemple des trois identités contextuelles, il est légitime de se demander ce que jongler entre ces différentes identités implique en termes d'anonymat. En imaginant qu'on utilise un pseudonyme et non son identité civile, il peut être plus pertinent d'avoir une identité, donc un *pseudo*, dans chaque contexte : une pour les sites de rencontres, une autre pour les médias sociaux, et une pour les relations familiales, *etc.*, afin d'éviter les recoupements. Si les informations émanant des dites identités ne sont pas compartimentées, c'est-à-dire si un même pseudo est utilisé, leur recoupement permet de réduire le nombre de personnes à qui elles peuvent correspondre. Il devient alors plus facile de faire le lien entre une présence numérique et une personne physique, et donc de mettre un nom sur l'identité contextuelle correspondante.

Considérons par exemple une personne qui utilise le pseudonyme *bruise76* sur un blog où elle dit être végétarienne et aimer les films d'action. Il n'existe qu'un certain nombre de personnes correspondant à ces critères. Ajoutons à cela le fait que ce même pseudonyme est utilisé pour organiser une fiesta dans telle ville *via* un média social et pour communiquer par mail avec Mme Unetelle. Il n'y a sans doute pas beaucoup de personnes végétariennes, aimant les films d'actions, organisant une fête dans cette même ville et communiquant par email avec Mme Unetelle.

1. Ippolita, 2012, *J'aime pas Facebook* [http://inventin.lautre.net/livres/Ippolita-J-aime-pas-Facebook.pdf].

Plus les utilisations d'un pseudonyme par la même personne sont nombreuses et variées, plus le nombre de personnes pouvant correspondre à ce pseudonyme est restreint. Ainsi en recoupant les utilisations d'un même pseudonyme il est possible d'affaiblir voire de casser le pseudonymat.

Voici un exemple qui montre la faiblesse du pseudonymat : AOL a publié le resulats de 3 mois de requêtes soumises à son moteur de recherche. Les requêtes d'une même personne étaient associées à un même pseudonyme. En faisant du recoupement, il était possible de briser le peudonymat associé aux requêtes[2].

De même gouverneur de l'État du Massachusetts a lui aussi fait les frais de ces recoupements lorsque son dossier médical, soit-disant anonymisé, a pu être identifié parmi ceux de toutes les citoyennes de cet État. Le chercheur ayant effectué cette démonstration de désanonymisation de données poussa l'ironie jusqu'à lui envoyer son dossier médical par la poste[3].

30.2.2 Corrélation temporelle

Procédé un peu plus technique cette fois-ci, la corrélation temporelle permet également de briser ou d'affaiblir un peu plus l'anonymat ou le pseudonymat. En effet, si dans un intervalle de temps réduit, il y a connexion vers la boîte mail amazone@exemple.org ainsi que jeanne.dupont@courriel.fr, la probabilité que ces deux adresses mail soient aux mains de la même personne augmente, et ce d'autant plus si cette observation se répète. Diverses parades, répondant à des besoins divers, seront explicitées plus loin.

30.2.3 Stylométrie

Il est possible d'appliquer des analyses statistiques sur la forme de n'importe quel type de données, et notamment aux textes. En analysant [4] différentes caractéristiques d'un texte, comme la fréquence des mots-outils [5], la longueur des mots, des phrases et des paragraphes, la fréquence des signes de ponctuation, on peut corréler des textes anonymes avec d'autres textes, et en retirer des indices sur leurs autrices.

Ce type d'analyse fut par exemple utilisé lors du procès de Theodore Kaczynski [6] pour accréditer le fait qu'il soit l'auteur du manifeste « La société industrielle et son avenir » [7].

Les autrices d'une étude récente [8] ont cherché à « simuler une tentative d'identification de l'autrice d'un blog publié de manière anonyme. Si l'autrice est suffisamment prudente pour éviter de révéler son adresse IP ou tout autre identifiant explicite, son adversaire (par exemple un censeur gouvernemental) peut se pencher sur l'analyse de son style d'écriture ». Leurs conclusions montrent que la stylométrie permet de réduire fortement, parmi de très nombreuses possibilités, le nombre d'autrices possibles d'un

---

2. Nate Anderson, 2006, *AOL releases search data on 500,000 users* [https://arstechnica.com/uncategorized/2006/08/7433/] (en anglais).

3. Paul Ohn, 2009, *Broken Promises of Privacy : Responding to the Surprising Failure of Anonymization* [http://www.uclalawreview.org/pdf/57-6-3.pdf] (en anglais).

4. Par exemple grâce à des logiciels comme *The Signature Stylometric System* [https://www.philocomp.net/texts/signature.htm] ou *Java Graphical Authorship Attribution Program* [https://evllabs.com/?page_id=42] (liens en anglais).

5. Les mot-outils sont des mots dont le rôle syntaxique est plus important que le sens. Il s'agit typiquement de mots de liaison [https://fr.wikipedia.org/wiki/Mot-outil].

6. Kathy Bailey, 2008, *Forensic Linguistics in Criminal Cases*, Language in Social Contexts [https://archive.org/download/bailey-forensic-linguistics-paper/Bailey_-_Forensic_Linguistics_Paper.doc] (en anglais).

7. Theodore Kaczynski, 1998, *La société industrielle et son avenir* [https://www.fichier-pdf.fr/2012/12/20/kaczynski/kaczynski.pdf].

8. Hristo Paskov, Neil Gong, John Bethencourt, Emil Stefanov, Richard Shin, Dawn Song, 2012, *On the Feasibility of Internet-Scale Author Identification* [https://www.cs.princeton.edu/~arvindn/publications/author-identification-draft.pdf] (en anglais).

texte anonyme — la précision augmentant évidemment avec le nombre d'échantillons « signés », c'est-à-dire dont l'autrice est connue, fournis au logiciel d'analyse.

Le plus souvent, cela leur permet de réduire la taille de l'ensemble des autrices possibles de 100 à 200 sur 100 000 initialement. « [...] ajouté à une autre source d'information, cela peut être suffisant pour faire la différence entre l'anonymat et l'identification d'une autrice ». À l'heure où sont écrites ces lignes, il est même possible dans 20 % des cas d'identifier directement l'autrice anonyme.

La particularité de ce travail est qu'il dépasse le cadre de petits échantillons (une centaine de possibilités) auxquels s'étaient cantonnées les études précédentes, pour s'intéresser à l'identification de l'autrice parmi un très grand nombre de possibilités ; en d'autres termes, il démontre que la stylométrie peut être employée pour confirmer l'origine d'un texte sur la base d'un très grand nombre d'échantillons.

Cependant, écrire en essayant de masquer son style, sans expertise particulière, semble permettre de rendre inefficaces les analyses stylométriques. Imiter le style de quelqu'une d'autre permet même de les tromper dans plus de la moitié des cas[9].

D'autres chercheuses développent des logiciels qui suggèrent les modifications à effectuer pour anonymiser un texte[10].

30.3 La compartimentation

Comme on vient de le voir, de nombreuses possibilités d'attaques permettent de faire correspondre une identité civile et une identité contextuelle. L'utilisation d'un seul et même nom pour ses différentes activités est sans doute la pratique la plus à même de nous confondre.

Face à cela, il est donc important de bien réfléchir à l'usage que l'on a de ses pseudonymes. Il est souvent dangereux de mélanger plusieurs identités contextuelles sous un même pseudo. La meilleure prévention reste de les séparer clairement dès le départ afin de limiter les ennuis par la suite. Après tout, une pratique ou une identité qui peut être utilisée à un moment donné peut d'un coup se transformer en source de problèmes en raison de conditions extérieures qu'il n'est pas forcément possible d'anticiper ou de maîtriser.

page 244

Cependant, ces pratiques ne sont pas toujours faciles à mettre en place. Car en plus des techniques décrites précédemment, la séparation entre ces différentes identités contextuelles dépend de beaucoup d'autres paramètres. Notamment des relations que l'on établit avec d'autres personnes, que ces relations soient numériques ou non. Il n'est pas forcément facile d'avoir une identité contextuelle différente pour absolument chacune des facettes de sa personnalité ou chacune de ses activités, ni d'éviter que certaines d'entre elles ne se recoupent. Ces identités évoluent au gré des activités qu'on leur attribue et au fil du temps. Plus longtemps on les utilise, plus leur séparation a tendance à s'amenuiser. Il est donc souvent difficile d'équilibrer et de mesurer les efforts nécessaires à la mise en place des multiples identités contextuelles avec les bénéfices escomptés. D'autant plus qu'il est généralement compliqué de faire marche arrière dans ce domaine.

Certains outils tels les médias sociaux les rendent même quasiment impraticables en imposant une transparence absolue.

---

9. M. Brennan, R. Greenstadt, 2009, *Practical attacks against authorship recognition techniques*, dans *Proceedings of the Twenty-First Innovative Applications of Artificial Intelligence Conference* [https://www.cs.drexel.edu/~greenie/brennan_paper.pdf] (en anglais).
10. Andrew W.E. McDonald, Sadia Afroz, Aylin Caliskan, Ariel Stolerman, Rachel Greenstadt, 2012, *Use Fewer Instances of the Letter "i" : Toward Writing Style Anonymization*, The 12th Privacy Enhancing Technologies Symposium [https://www2.seas.gwu.edu/~aylin/papers/Aylin_PETS12_anonymouth.pdf] (en anglais).

30.4 Les médias sociaux : centralisation de fonctions et identité unique

Les médias sociaux tendent en effet à centraliser des fonctions qui étaient auparavant assurées par différents outils, de l'échange de messages à la publication de nouvelles, en passant par les groupes de discussion. Ils tendent à se substituer à la fois à l'email, à la messagerie instantanée, aux blogs ainsi qu'aux forums.

Dans le même temps se développent de nouvelles fonctions, comme une certaine vie relationnelle numérique où l'existence d'une communication prime sur son contenu, poussée à son paroxysme avec les « pokes », ces messages sans contenu[11]. Le web 2.0 encourage l'expression sur des sujets qui étaient auparavant considérés comme intimes[12].

Finalement, pas grand-chose de bien nouveau, si ce n'est la centralisation de nombreuses fonctions et de pratiques variées vers un outil unique. C'est d'ailleurs le côté « tout-en-un » de ces plateformes, le graphisme ainsi que la facilité d'usage qui en font le succès. Mais cette centralisation pose question quant aux conséquences de l'utilisation de ces outils sur nos intimités.

La pression sociale pour utiliser les médias sociaux est très forte dans certains milieux : lorsque des groupes les utilisent pour la majorité de leurs communications, des messages interpersonnels aux invitations en passant par la publication d'informations, ne pas participer aux médias sociaux, c'est être marginalisée. Le succès de ces sites repose sur « l'effet de réseau » : plus il y a de personnes qui les utilisent, plus il est important d'y être présente.

Mais dans le même temps, ces médias sociaux permettent aussi de s'évader de ces pressions de groupes et d'assumer ou d'expérimenter plus facilement certaines parts de sa personnalité qui ne sont pas forcément tolérées par ces groupes.

La centralisation de toutes les activités sur une seule plateforme rend extrêmement difficile l'usage de pseudonymes différents pour différentes identités contextuelles. En effet, en mettant toutes les informations au même endroit, le risque de recoupement de différentes identités contextuelles est maximisé. Nombre de médias sociaux demandent une identité unique, celle correspondant à l'identité civile d'une personne physique. C'est là une différence clé par rapport à un modèle où un individu peut avoir plusieurs blogs avec des tons et des contenus différents, chacun sous un pseudonyme différent. De plus, à l'instar des sites de rencontres, où plus on est honnête, meilleurs sont les résultats, ici plus on fournit du contenu, plus on utilise cette plateforme, meilleures sont les interactions.

Ceci est d'autant plus vrai qu'utiliser son identité civile fait partie des règles de réseaux comme Facebook, qui met en place différents mécanismes pour traquer les pseudonymes[13]. Ces entreprises poussent jusqu'au bout le *business model* de la publicité ciblée et de la vente de profils : elles « mettent en place différents procédés techniques de captation de l'identité des usagères, depuis l'identité fondée sur leurs déclarations, jusqu'à l'identité agissante[14] et l'identité calculée fondée sur l'analyse

11. Fanny Georges, 2008, *Les composantes de l'identité dans le web 2.0, une étude sémiotique et statistique*, Communication au 76ème congrès de l'ACFAS : Web participatif : mutation de la communication ?, Québec, Canada [https://hal.archives-ouvertes.fr/hal-00332770/].

12. Alain Rallet et Fabrice Rochelandet, 2010, *La régulation des données personnelles face au web relationnel : une voie sans issue ?*, Réseaux numéro 167, Données personnelles et vie privée [https://www.cairn.info/revue-reseaux-2011-3-page-17.htm].

13. Nikopik, 2012, *Facebook et la délation* [https://geeko.lesoir.be/2012/09/24/facebook-demande-a-ses-membres-de-denoncer-les-pseudonymes/].

14. L'« identité agissante » désigne les messages qui apparaissent automatiquement sur la page d'une personne sur le média social et qui détaillent son activité sur la plateforme. Ces messages ne rendent donc pas compte de *ce que dit* la personne sur le site, mais de *ce qu'elle y fait*. Par exemple, « Ana a modifié sa photo de profil » ou « Ana est désormais amie avec Betty ». Fanny Georges, Antoine Seilles, Jean Sallantin, 2010, *Des illusions de l'anonymat – Les stratégies de préservation des données personnelles à l'épreuve du Web 2.0*, Terminal numéro 105, Technologies et usages de l'anonymat à l'heure d'Internet [https://journals.openedition.org/terminal/1876].

de leurs comportements (sites visités, nombre de messages, *etc.*). Il apparaît que l'anonymat total devient impossible dans un univers virtuel où les usagers sont avant tout des consommateurs qu'il s'agit d'observer. » [15]

Ainsi, en juillet 2011, Max Schrems a réussi à obtenir l'ensemble des données dont Facebook dispose sur lui en invoquant une directive européenne. Le dossier qu'il a reçu comprend 1222 pages [16], qui incluent non seulement l'ensemble des informations disponibles sur son profil, mais aussi tous les évènement auxquels il a été invité (y compris les invitations déclinées), tous les messages envoyés ou reçus (y compris les messages supprimés), toutes les photos chargées sur Facebook accompagnées de métadonnées concernant notamment la géolocalisation, tous les « pokes » émis ou reçus, toutes les « amies » (y compris les « amies » effacées), les journaux de connexions à Facebook (incluant l'adresse IP et sa géolocalisation), toutes les « machines » (identifiées par un cookie) utilisées par un profil, ainsi que les autres profils utilisant les mêmes « machines » ou encore la localisation de sa dernière connexion connue à Facebook (longitude, latitude, altitude).

page 30

page 214

Enfin, malgré les déclarations du fondateur de Facebook, comme quoi l'ère de la vie privée est révolue [17], nombre de stratégies restent à développer, à remanier, afin de jouer avec les différentes marges encore d'actualité. Et ceci dans l'optique d'avoir un peu de prise sur ces questions fondamentales : « Qu'est-ce que l'on souhaite montrer ? », « Qu'est-ce que l'on accepte de rendre visible ? » et « Qu'est-ce que l'on veut cacher et à quel prix ? ».

15. Chantal Enguehard, Robert Panico, 2010, *Approches sociologiques*, Terminal numéro 105, Technologies et usages de l'anonymat à l'heure d'Internet [https://journals.openedition.org/terminal/1868].

16. Damien Leloup, 2012, *Max Schrems : "L'important, c'est que Facebook respecte la loi"*, Le Monde [https://www.lemonde.fr/technologies/article/2011/11/23/max-schrems-l-important-c-est-que-facebook-respecte-la-loi_1607705_651865.html].

17. Bobbie Johnson, 2010, *Privacy no longer a social norm, says Facebook founder* [https://www.theguardian.com/technology/2010/jan/11/facebook-privacy] (en anglais).

Chapitre 31

Cacher le contenu des communications : la cryptographie asymétrique

Dans le premier tome de ce guide, nous avons vu que la piste la plus sérieuse pour protéger des données des regards indiscrets est le chiffrement : il permet de les rendre illisibles pour toute personne qui n'a pas la *clé secrète*.

page 47

31.1 Limites du chiffrement symétrique

Dans le cadre du chiffrement symétrique, c'est une même clé secrète qui permet à la fois d'effectuer le chiffrement et le déchiffrement.

Le chiffrement symétrique est tout à fait adapté pour chiffrer une clé USB ou un autre support de stockage.

page 50

Lorsqu'on souhaite chiffrer une communication, c'est plus délicat : la personne qui devra déchiffrer les données n'est pas la même que celle qui les a chiffrées.

Si la clé secrète était la même pour toutes les personnes avec qui l'on communique, alors chacune de ces personnes pourrait déchiffrer des messages qui ne lui sont pas destinés. Il faut donc autant de clés secrètes que de personnes avec qui on communique ; et il faut trouver le moyen de s'échanger ces clés secrètes de façon confidentielle.

31.2 Une solution : la cryptographie asymétrique

Dans les années 1970, des cryptographes ont trouvé une solution aux problèmes posés par le chiffrement symétrique en créant le chiffrement *a*symétrique.

page 47

Avec le chiffrement asymétrique, chaque personne qui communique possède une paire de clés : une clé *publique* pour qu'on puisse lui écrire des messages chiffrés, et une clé *privée* pour qu'elle puisse les déchiffrer et les lire.

À chaque échange, il faut imaginer que les communications voyagent dans une boîte munie d'un verrou spécial.

La clé publique permet de verrouiller la boîte au moment de l'envoi du message. Par contre, elle ne permet en aucun cas de la déverrouiller.

L'autre clé, la clé privée, permet uniquement de déverrouiller la boîte et donc d'accéder à son contenu.

La clé publique peut être distribuée à n'importe qui. Elle peut même être mise en ligne, puisqu'elle ne sert qu'à verrouiller la boîte. La clé privée, elle, ne se partage jamais.

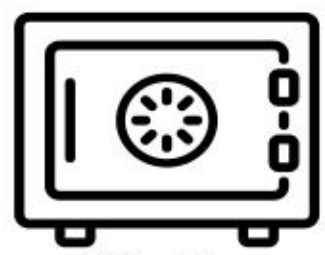
Dans notre exemple illustré, le chiffrement a lieu dans l'ordinateur de Bea et le déchiffrement dans celui d'Ana.



Ana possède une paire de clés.



Bea possède aussi une paire de clés.



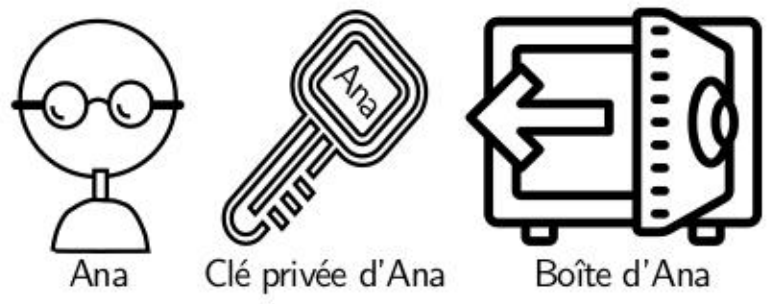
Les messages destinés à Ana seront placés dans une boîte qui sera verrouillée avec sa clé publique.



Bea récupère la clé publique d'Ana.



Bea dépose un message dans la boîte d'Ana puis la verrouille avec la clé publique d'Ana.



Ana utilise sa clé privée pour déverrouiller la boîte et récupérer le message. Seule sa clé privée permet de déverrouiller cette boîte.

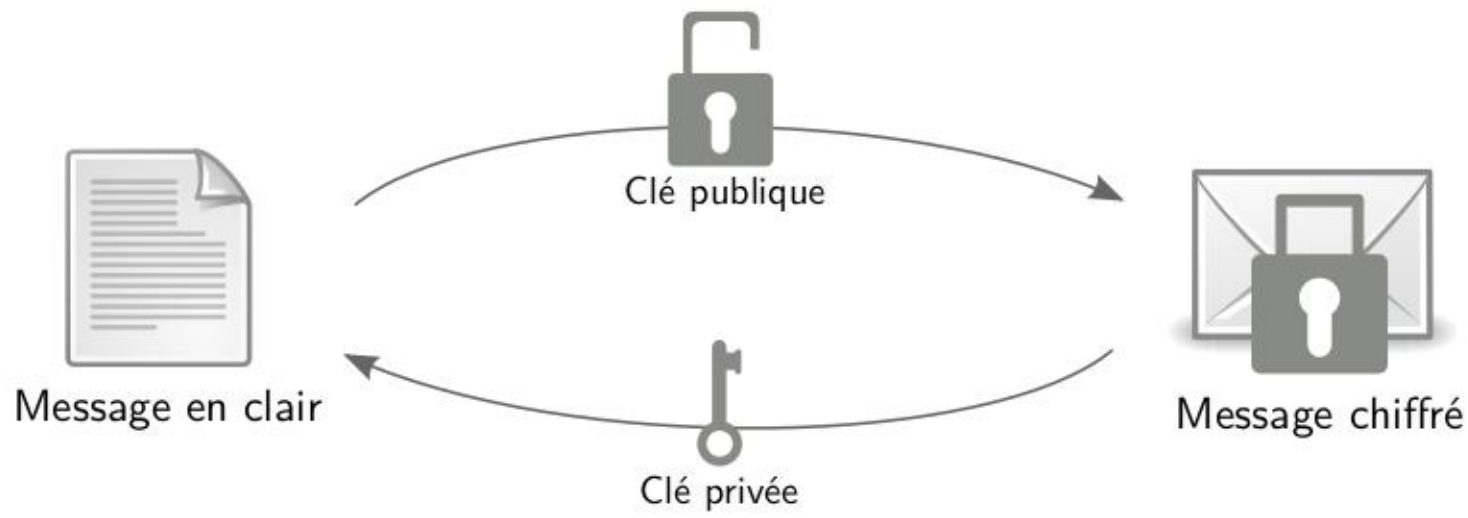
31.3 Chiffrement de bout en bout

Lorsque seules les personnes qui communiquent peuvent lire les messages échangés, on parle de *chiffrement de bout en bout*. En principe, cela empêche l'écoute électronique, y compris par les fournisseurs de télécommunications, par les fournisseurs d'accès Internet et même par le fournisseur du service de communication. Avec le chiffrement de bout en bout, personne n'est en mesure d'intercepter les clés cryptographiques nécessaires pour déchiffrer la conversation.

Les systèmes de chiffrement de bout en bout sont conçus pour résister à toute tentative de surveillance ou de falsification, car aucun tiers ne peut déchiffrer les données communiquées ou stockées. En particulier, les services qui offrent du chiffrement de bout en bout sont incapables de remettre une version déchiffrée des messages de leurs utilisatrices aux autorités [1].

31.3.1 Une affaire de nombres premiers...

Dans la réalité, la clé publique et la clé privée sont des nombres. Ce qu'une clé permet de chiffrer, l'autre permet de le déchiffrer :



La clé publique permet de chiffrer et la clé privée permet de déchiffrer

Mais comment est-il possible que la clé publique permette de chiffrer un message sans permettre de le déchiffrer ? La cryptographie asymétrique repose en fait sur des problèmes mathématiques extrêmement difficiles à résoudre. L'algorithme de chiffrement RSA, par exemple, repose sur la « factorisation de nombres entiers ». C'est-à-dire la décomposition d'un nombre entier en nombres premiers.

Étant donné le nombre 12, il est simple de le décomposer en $2 \times 2 \times 3$. De même, 111 est égal à 3×37. En revanche, comment décomposer le nombre suivant, composé de 232 chiffres ?

```
12301866845301177551304949583849627207728535695953347921973224521517264005072636575187452021997864693899564749427740638459251925573263034537315482685079170261221429134616704292143116022212404792747377940806653514195974598569021434 13
```

Le résultat est le produit de deux nombres premiers composés chacun de 116 chiffres.

Ce problème de factorisation d'entiers est étudié depuis plus de 2000 ans par des mathématiciennes ; pourtant, aucune solution pratique n'a encore été trouvée : la meilleure solution connue est d'essayer avec tous les nombres premiers possibles.

Avec un ordinateur actuel, ce calcul serait beaucoup plus long que la durée d'une vie humaine [2]. Les nombres les plus difficiles à factoriser sont les produits de deux

1. Cette section est reprise de Wikipédia, 2022, *Chiffrement de bout en bout* [https://fr.wikipedia.org/wiki/Chiffrement_de_bout_en_bout].

2. La factorisation de ce nombre de 768 bits en 2010 a nécessité 10^{20} opérations. Les chercheurs qui l'ont réalisée estiment que le calcul aurait pris environ 2000 ans sur un seul cœur d'un AMD

grands nombres premiers. On choisira donc des nombres suffisamment grands pour que même avec des ordinateurs extrêmement puissants, la factorisation ne puisse pas se faire en un temps réaliste.

Faire confiance à cette méthode revient donc à faire le pari que son adversaire dispose d'une puissance de calcul relativement limitée. La taille des clés, qui se mesure en bits, est d'une importance capitale. En effet, si on considère qu'une clé asymétrique de 2048 bits est sûre jusqu'en 2030[3], une clé de 512 bits se casse en quelques mois avec un ordinateur personnel haut de gamme actuel[4]. Il faut garder à l'esprit que ce qui est « cassable » par un ordinateur en dix ans pourrait l'être en un an avec dix ordinateurs identiques au premier.

De plus, si un jour une personne résout ce problème mathématique, il sera possible de déchiffrer sans trop de difficulté les échanges chiffrés qui auront ont été enregistrés — ce type de collecte et de stockage fait partie entre autres des activités de la NSA, agence de renseignement états-unienne[5]. Beaucoup de secrets militaires et commerciaux seraient alors révélés à ceux qui auront accès à ces enregistrements. En d'autres termes, on peut imaginer une sacrée pagaille entre entreprises concurrentes et agences de renseignements ennemies…

En attendant, les attaques utilisées à l'heure actuelle sur les systèmes de cryptographie asymétrique ciblent la façon de le mettre en œuvre dans tel ou tel logiciel, ou une erreur dans son code source, et non le principe mathématique du système.

page 39

31.4 Signature numérique

Les paires de clés utilisées pour la cryptographie asymétrique peuvent aussi être utilisées pour prouver l'authenticité d'un message. Comment cela fonctionne-t-il ? Reprenons l'exemple de Bea envoyant un message à Ana. Cette fois, Bea veut signer numériquement son message afin qu'Ana puisse être sûre qu'elle en est bien l'autrice.

page 53

Dans le premier tome de ce guide, on a parlé des sommes de contrôle, ou empreintes : un nombre qui permet de vérifier l'intégrité d'un message. Cette empreinte va également servir à signer des données numériques. Dans un premier temps, l'ordinateur de Bea calcule une *empreinte* du message qu'elle va envoyer à Ana.

Ensuite, cette empreinte est chiffrée avec la clé privée de Bea : c'est la *signature numérique*. Eh oui : l'empreinte est chiffrée avec la clé privée de Bea, dont elle est la seule à disposer, et non avec la clé publique d'Ana. Cette signature sert en effet à authentifier l'expéditeur, et non le destinataire. Or on vient de voir que clé publique et clé privée étaient en fait deux nombres choisis de telle façon que l'un permette de déchiffrer ce que l'autre a chiffré. Rien n'empêche donc de chiffrer quelque chose avec la clé privée. C'est alors la clé publique qui va permettre de le déchiffrer.

Bea envoie alors le message accompagné de sa signature à Ana.

Pour vérifier la signature, l'ordinateur d'Ana va lui aussi calculer l'empreinte du message et déchiffrer en parallèle la signature.

Puisqu'elle est chiffrée avec la clé privée de Bea, la clé publique de Bea suffit pour déchiffrer cette signature. Si l'empreinte du message reçu correspond à la signature

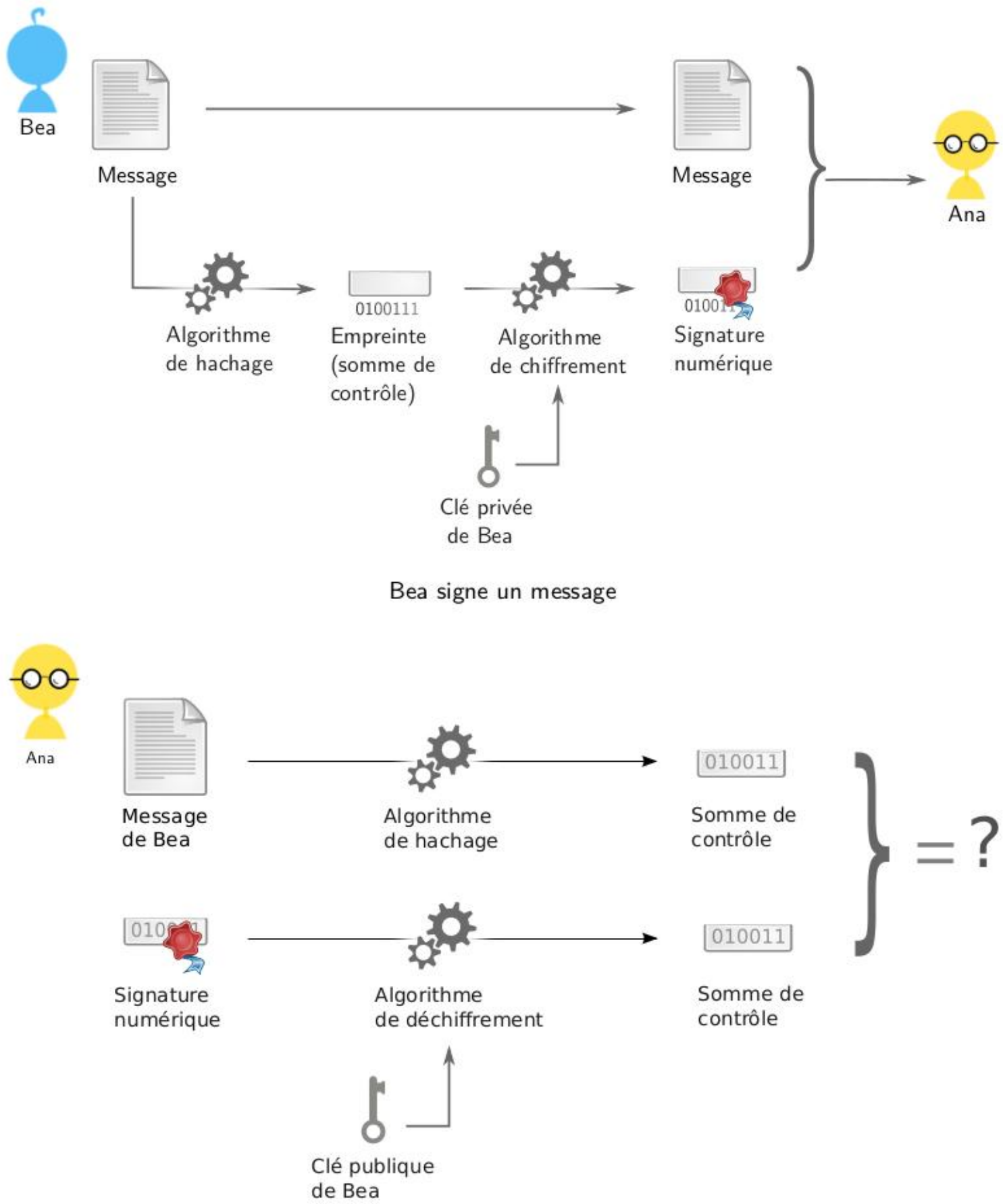
---

Opteron à 2,2 GHz, ce qui correspond à plusieurs centaines d'années sur un processeur actuel (Kleinjung *et al.*, 2010, *Factorization of a 768-bit RSA modulus* [https://eprint.iacr.org/2010/006.pdf] — en anglais).

3. Agence nationale de la sécurité des systèmes d'information, 2014, *Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* [https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf].

4. S. A. Danilov, I. A. Popovyan, 2010, *Factorization of RSA-180* [https://eprint.iacr.org/2010/270.pdf] (en anglais).

5. Nicole Perlroth, Jeff Larson et Scott Shane, 2013, *N.S.A. Able to Foil Basic Safeguards of Privacy on Web*, The New York Times [https://archive.org/details/n.-s.-a.-able-to-foil-basic-safeguards-of-privacy-on-web] (en anglais).



déchiffrée (celle-ci n'étant rien d'autre, comme on l'a dit, que l'empreinte du message calculée par l'ordinateur de Bea), Ana est sûre de l'authenticité du message qu'elle a reçu. En effet, Bea garde sa clé privée en lieu sûr. Elle est donc la seule à avoir pu chiffrer l'empreinte qu'Ana a déchiffré avec la clé publique de Bea.

L'inconvénient de cette certitude est que Bea, possedant la clé privée, pourra plus difficilement nier être l'autrice du message.

31.5 Vérifier l'authenticité de la clé publique

La cryptograhie asymétrique permet ainsi de chiffrer et de signer des messages sans avoir besoin de s'échanger préalablement un secret partagé.

Cependant, elle ne résout pas une question importante : comment s'assurer que je possède bien la *véritable* clé publique de ma destinataire, et que ce n'est pas une personne qui a usurpé sa clé publique pour pouvoir intercepter mes messages, tout en me donnant une fausse impression de sécurité ?

31.5.1 L'attaque du monstre du milieu

Reprenons l'exemple d'Ana qui souhaite recevoir un message chiffré de la part de Bea, en présence d'une adversaire Carole qui peut avoir accès aux messages échangés :

- Ana commence par envoyer sa clé publique à Bea. Carole peut la lire.
- Bea chiffre son message avec la clé publique qu'elle a reçue, puis l'envoie à Ana.
- Carole qui ne possède pas la clé privée d'Ana, mais seulement sa clé publique, ne peut pas déchiffrer le message.
- Ana elle, peut déchiffrer le message à l'aide de la clé privée qu'elle garde précieusement.

Cependant si Carole est en mesure de modifier les échanges entre Ana et Bea, les choses se corsent :

- Lorsqu'Ana envoie sa clé publique à Bea, Carole l'intercepte et renvoie à Bea, en lieu et place de celle d'Ana, une clé publique dont elle détient la clé privée correspondante.
- Bea chiffre son message avec la clé publique qu'elle a reçue, puis l'envoie à Ana. Mais la clé qu'elle a reçue appartenait à Carole : elle l'a substituée à celle d'Ana.
- Carole intercepte à nouveau le message. Mais cette fois, il est chiffré avec sa clé publique, dont elle a la clé privée. Elle peut donc déchiffrer le message pour le lire et éventuellement le modifier. Puis elle chiffre à nouveau le message avec la véritable clé publique d'Ana, avant de l'envoyer à Ana.
- Ana peut alors déchiffrer le message avec sa clé privée, sans se rendre compte de rien.

Ainsi, Bea est persuadée d'utiliser la clé d'Ana, alors qu'elle utilise en réalité celle de Carole. De la même manière, Carole peut usurper la clé publique de Bea et falsifier la signature du message transmis par Bea à Ana. Ana recevra un message chiffré et dûment signé… par Carole.

On appelle cette attaque l'*attaque du monstre du milieu* (courramment appelée *attaque de l'homme du milieu*, et *Man-in-the-Middle* ou *Monster-in-the-Middle attack*, soit *MitM* en anglais[6]). Dans notre exemple, Carole était le *monstre du milieu*, capable de lire et de modifier la communication chiffrée en se faisant passer, aux yeux de chaque partie de la communication, pour l'autre.

Une adversaire peut se positionner en *monstre du milieu* par différents biais.

Le fournisseur d'accès à Internet est par exemple particulièrement bien placé, car tout le trafic passera obligatoirement par lui. De même un *gros* nœud du réseau par lequel passe une quantité importante du trafic sera en bonne mesure de mettre en place cette attaque[7]. Enfin une adversaire ayant accès au réseau local que vous utilisez pourra toujours faire transiter le trafic réseau par son ordinateur utilisant pour cela des techniques plus spécifiques[8].

Pour se prémunir contre cette attaque, il faut que Bea ait une façon de vérifier que la clé publique qu'elle utilise est bien celle d'Ana. Si la clé publique n'est pas une information confidentielle, il faut donc toutefois s'assurer de son *authenticité* avant de l'utiliser.

Parfois, la façon la plus simple, pour Bea, est de rencontrer Ana afin de vérifier que la clé publique dont elle dispose est bien la sienne. Peu importe que Carole soit présente

---

6. L'usage courant est de parler d'*attaque de l'homme du milieu* [https://fr.wikipedia.org/wiki/Attaque_de_l%27homme_du_milieu]. La communauté hacktiviste questionne l'inclusivité de ce concept en utilisant des expressions alternatives : *humaine du milieu*, *personne du milieu*, *machine du milieu*, *monstre du milieu* [https://sindominio.net/sincensura/fr/post/informe/#inspection-approfondie-des-paquets], *etc.*

7. Pixellibre.net, 2011, *#OpSyria : les preuves parlent d'elle même.* [https://pixellibre.net/2011/10/opsyria-bluecoat-censure-leaks-censorship-syrie/], ou plus précis, mais en anglais Jakub Dalek and Adam Senft, 2011, *Behind Blue Coat, Investigations of commercial filtering in Syria and Burma*, The Citizen Lab [https://citizenlab.ca/2011/11/behind-blue-coat].

8. Wikipédia, 2014, *ARP poisoning* [https://fr.wikipedia.org/wiki/ARP_poisoning].

au moment de cette rencontre : seule une vérification de clé *publique* aura lieu, et aucun secret ne va être échangé (à part que Bea et Ana souhaitent communiquer, mais ça, vu sa position, Carole peut le savoir d'autres façons). Une fois cette vérification faite, du chiffrement de bout en bout pourra être mis en place entre Ana et Bea.
Entre les deux, un message dont le contenu sera chiffré circulera ; seul l'en-tête de la communication, que ce soit une requête HTTP ou un email, circulera *en clair*.

page 217

Cependant, il arrive souvent que Bea ne puisse pas rencontrer Ana — a fortiori si elle ne la connaît pas : si elle rencontre une personne qui se présente comme étant Ana, Bea ne peut pas être sûre qu'il s'agit bien d'Ana. Or, c'est généralement le cas lorsqu'on veut chiffrer ses connexions vers un site web : on ne connaît pas les personnes qui sont derrière.

31.5.2 Infrastructure à clé publique hiérarchique

La première solution couramment utilisée est de disposer d'autorités de confiance qui certifient les clés publiques en les signant numériquement : on parle de *certificats*. Ana demande à l'autorité de certifier sa clé publique. L'autorité vérifie l'identité d'Ana, par exemple en lui demandant sa carte d'identité, puis signe numériquement sa clé. Avant d'utiliser la clé d'Ana, Bea (ou son ordinateur) vérifie qu'elle est bien signée par une autorité qu'elle considère comme digne de confiance. On parle d'infrastructure à clé publique hiérarchique (*hierarchical public key infrastructure*, ou *hierarchical PKI* en anglais).

page 252

Le protocole TLS

C'est le principe qui est couramment utilisé pour authentifier les sites web ou les serveurs mail avec lesquels l'ordinateur établit une connexion chiffrée. Les enjeux les plus courants lors de l'établissement d'une connexion chiffrée vers un site web sont la protection de mots de passe — pour se connecter à son compte mail par exemple — ou la protection de données bancaires — pour effectuer des achats sur des sites de vente en ligne. Le protocole utilisé pour ce type de chiffrement est appelé TLS (anciennement SSL) [9].

page 208

page 199

Ce standard permet d'encapsuler le protocole applicatif utilisé habituellement dans une couche de chiffrement. Par exemple, le protocole web HTTP, quand il est encapsulé dans du TLS, donc chiffré, est appelé HTTPS. Il en va de même pour les protocoles mail POPS, IMAPS et SMTPS.

page 201

On peut expliquer le protocole TLS comme une salutation très cordiale entre l'ordinateur d'origine et le serveur de destination. Ils vont s'assurer du chiffrement de la communication en s'échangeant des clés de chiffrement.

Le problème des autorités de certification

Ce sont des autorités de certification (CA, par ses initiales anglaises) qui vont assurer que ces clés de chiffrement sont les bonnes et vont produire pour cela un *certificat électronique*. Cependant, une telle solution ne fait que déplacer le problème : il faut faire confiance à l'autorité de certification. En général, ce sont des entreprises commerciales, et plus rarement des administrations.

Ainsi Microsoft, Apple et Mozilla incluent chacun des autorités de certification de gouvernements parmi les autorités de certification reconnues par leurs navigateurs web [10]. Mozilla Firefox inclut [11] notamment des autorités de certifications de gouvernements

9. SSL pour Secure Sockets Layer ou « Couche de sockets sécurisée » est le prédécesseur de TLS pour Transport Layer Security ou « Sécurité de la couche de transport ».

10. Christopher Soghoian, Sid Stamm, 2011, *Certified Lies : Detecting and Defeating Government Interception Attacks Against SSL*, Financial Cryptography and Data Security [https://s3.amazonaws.com/files.cloudprivacy.net/ssl-mitm.pdf] (en anglais).

11. Common CA Database, 2017, *CA Certificates In Firefox* [https://ccadb-public.secure.force.com/mozilla/CACertificatesInFirefoxReport] (en anglais).

(chinois, catalan, espagnol, néerlandais, turc), d'entreprises de certification (Entrust, GoDaddy, Verisign), et d'entreprises de télécommunications (Amazon, Deutsche Telecom, Google).

Firefox inclut aussi l'autorité du groupe de recherche sur la sécurité d'Internet (Internet Security Research Group [12]). Ce groupe a mis en place Let's Encrypt [13], une autorité de certification gratuite, libre et automatisée lancée en 2016 qui simplifie l'accès à des certificats électroniques valides pour les petits serveurs.

page 254

Mais les gouvernements, qui peuvent souvent se positionner en *monstre du milieu*, ont le pouvoir de désigner n'importe quel certificat comme valide pour un site web en le signant avec leur autorité de certification : les navigateurs web qui l'incluent n'y verraient que du feu.

Dans le cas des entreprises, leur but premier n'est pas de certifier des identités mais de gagner de l'argent, en vendant comme service la certification d'identités. Mais vérifier une identité coûte cher. Qu'est-ce qui nous prouve qu'elles le font correctement ? Que

page 235

leurs clés privées utilisées pour signer sont stockées dans un endroit sûr ? Encore une fois, c'est une question de confiance. On peut espérer que, ne serait-ce que pour maintenir leur activité, ces autorités de certification font bien leur travail…

Sauf que… des exemples montrent qu'elles le font parfois très mal. Ainsi, en 2008, des chercheurs ont réussi à créer de faux certificats « valides », car six autorités de certifications utilisaient encore des algorithmes cryptographiques qui étaient, de notoriété publique, cassés depuis 2004 [14]. Les certificats ainsi créés sont de « vrais-faux » certificats : le navigateur web les reconnaît comme vrais, car malgré leur origine frauduleuse, tout laisse à penser qu'ils ont été établis par une autorité reconnue.

En 2011, neuf vrais-faux certificats signés par Comodo, une autorité de certification, ont été créés. Au moins l'un de ces certificats aurait été utilisé sur le web [15]. La société a mis plus d'une semaine à assumer publiquement cette compromission — et nombre d'entre elles ne le font probablement pas dans ce genre de situations, pour éviter la mauvaise publicité [16] et les pertes financières qui vont avec.

Par ailleurs, il semble que si la police ou la justice de leur pays le leur ordonne, certaines autorités de certification donnent aux flics de vrais-faux certificats, établis au nom d'entités qu'elles voudraient surveiller [17]. Cela dit, il faut quand même que ces vrais-faux certificats soient mis en place à l'endroit adéquat sur Internet et combinés à des attaques du monstre du milieu afin d'être exploités au mieux. Enfin, nos connexions passant en général par plusieurs pays, cette attaque peut tout à fait être déployée par un pays différent de celui depuis lequel on se connecte.

page 254

page 208

Dans une brochure commerciale, Packet Forensics, une compagnie états-unienne qui vend du matériel de surveillance réseau, écrit ainsi que « pour utiliser notre produit dans ce scénario, les utilisateurs gouvernementaux ont la possibilité d'importer une copie d'une clé légitime qu'ils peuvent obtenir (potentiellement grâce à une réquisition judiciaire) » [18]. Le PDG de Packet Forensics aurait confirmé oralement à l'auteur de

---

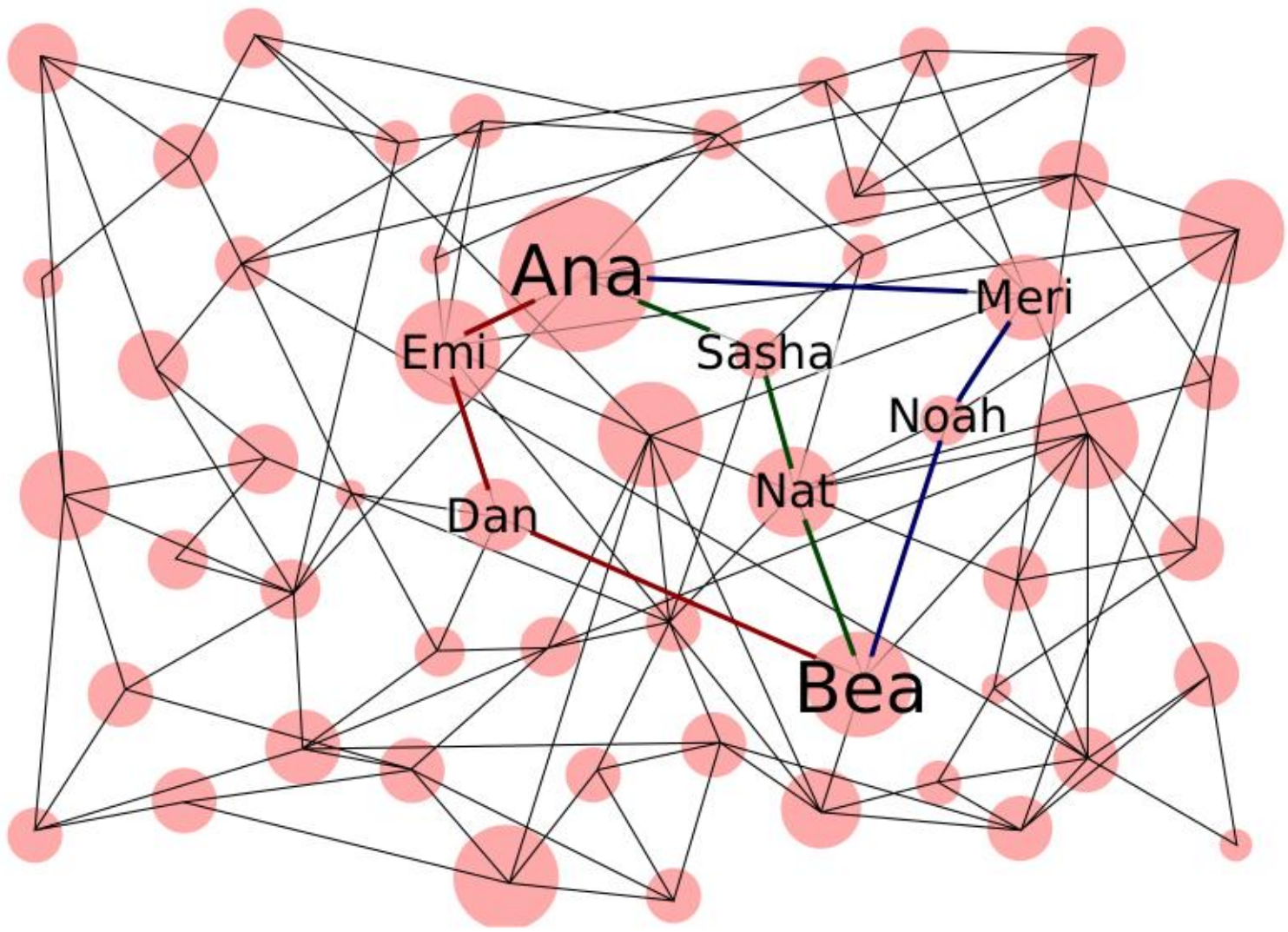
12. https://www.abetterinternet.org/about/
13. https://letsencrypt.org/fr/about/
14. Alexander Sotirov *et al.*, 2008, *MD5 considered harmful today – Creating a rogue CA certificate* [https://www.win.tue.nl/hashclash/rogue-ca/] (en anglais).
15. Comodo, 2011, *Comodo Fraud Incident* [https://www.comodo.com/Comodo-Fraud-Incident-2011-03-23.html] (en anglais).
16. Jacob Appelbaum, 2011, *Detecting Certificate Authority compromises and web browser collusion* [https://blog.torproject.org/detecting-certificate-authority-compromises-and-web-browser-collusion] (en anglais).
17. Christopher Soghoian, Sid Stamm, 2011, *Certified Lies : Detecting and Defeating Government Interception Attacks Against SSL*, Financial Cryptography and Data Security [https://s3.amazonaws.com/files.cloudprivacy.net/ssl-mitm.pdf] (en anglais).
18. « To use our product in this scenario, government users have the ability to import a copy of any legitimate key they obtain (potentially by court order) ». Citation extraite du papier de Christopher Soghoian et Sid Stamm cité ci-dessus, et traduite par nos soins.

l'étude que des clients gouvernementaux collaborent avec des autorités de certification pour obtenir des vrais-faux certificats à utiliser lors d'opérations de surveillance [19].

31.5.3 Toile de confiance

Une autre solution à la question de l'authenticité des clés publiques est la toile de confiance, ou *web of trust* en anglais.

Plutôt que de faire confiance à quelques autorités centralisées, il s'agit d'établir un lien de confiance de proche en proche. Ainsi, Bea ne connaît pas Ana, mais elle connaît Dan, qui connaît Emi, qui connaît Ana. Il y a donc un *chemin de confiance* entre Bea et Ana. S'il n'y avait que ce chemin de confiance, cela impliquerait que Bea place une forte confiance en Emi, qu'elle ne connaît pas directement. Mais Bea connaît aussi Nat, qui connaît Sasha, qui connaît lui aussi Ana. Elle connaît aussi Noah qui connaît Meri, qui connaît Ana. Il y a donc trois chemins de confiance entre Ana et Bea, qui n'a pas besoin d'avoir une confiance totale dans chacune des parties en jeu dans la certification.



Toile de confiance qui relie Ana et Bea

Ces toiles de confiance sont couramment utilisées pour l'authentification des logiciels et des communications personnelles, comme des courriers électroniques, en utilisant le standard OpenPGP. Elles ne sont hélas pas utilisées couramment pour authentifier des sites web, bien que ce soit possible techniquement [20].

Les toiles de confiance permettent donc de se prémunir des attaques du monstre du milieu sans devoir faire confiance à des autorités centralisées. Cependant, la participation à une toile de confiance nécessite de dévoiler les liens entre des personnes, des réseaux d'amies ou de militantes. Est-ce que l'on veut vraiment publier la liste de nos amies ou de nos camarades ?

page 254

19. Cette citation se trouve dans une version préliminaire, datant d'avril 2010, du papier de Christopher Soghoian et Sid Stamm cité ci-dessus ; cette version est disponible sur cryptome.org [https://cryptome.org/ssl-mitm.pdf] (en anglais).

20. Ainsi, le projet Monkeysphere [https://manpages.debian.org/bullseye/monkeysphere/monkeysphere.1.en.html] (en anglais) permet d'étendre l'utilisation des toiles de confiance d'OpenPGP à l'authentification de sites web.

31.6 Confidentialité persistante

page 249

Comme on l'a vu, quiconque possède une clé secrète peut l'utiliser pour déchiffrer un texte qui a été chiffré en utilisant la clé publique qui lui est associée. C'est une propriété très utile, mais qui dans certains cas peut se révéler embarrassante.

Admettons qu'une personne mal intentionnée enregistre une conversation en ligne chiffrée entre deux personnes. Elle ne pourra bien sûr rien lire du contenu de cette conversation dans l'immédiat. Mais elle peut avoir l'idée de s'introduire ensuite chez ces personnes ou dans leur ordinateur et de mettre la main sur leurs clés privées. Dans ce cas, elle sera en mesure de lire, *a posteriori*, toutes les conversations passées qu'elle aura conservées.

Ce fut le cas il y a quelques années, lorsque les admins du serveur *autistici.org* se rendirent compte lors d'un procès que la police avait mis la main sur les clés secrètes installées sur leur serveur, parce qu'ils produisaient au dossier des échanges d'emails qu'ils n'auraient normalement pas dû être capables de lire[21].

Pour éviter qu'un secret éventé ne compromette *a posteriori* de nombreux autres secrets qui en dépendent (comme par exemple le contenu de conversations en messagerie instantannée pourtant chiffrées, des échanges d'emails, *etc.*) certains logiciels incluent des fonctions dites de confidentialité persistante[22] (ou *Perfect Forward Secrecy*, en anglais).

Elles assurent que même si un jour un secret à long terme, typiquement une clé privée, est découverte par un adversaire, les échanges seront protégés d'une analyse a posteriori.

Dans les faits, au lieu d'utiliser directement la clé publique pour chiffrer les communications, ce type de chiffrement utilise un protocole d'échange de secrets conçu pour fonctionner même sur un canal de communication non sûr, en négociant une clé temporaire à chaque session de communication. La clé secrète d'une paire de clés ne sert, dans ce cas, qu'à s'assurer qu'on communique bien avec la bonne personne, en signant cet échange de secret.

page 55

C'est ensuite ce secret temporaire qui est utilisé pour chiffrer de façon symétrique les communications.

Une fois la communication terminée, il suffit que les logiciels impliqués oublient ce secret temporaire. Quand bien même quelqu'un mettrait la main sur les clés secrètes des deux parties, la confidentialité de la communication ne serait pas compromise : les participants de l'échange eux-mêmes n'y ont plus accès.

Pour protéger la vie privée des internautes, le protocole TLS implémente la confidentialité persistante.

31.7 Résumé et limites

La cryptographie asymétrique est donc un bon complément à la cryptographie symétrique dès qu'il s'agit non pas de protéger seulement nos données, mais plutôt le contenu de nos communications : échange d'emails, navigation sur le web, conversations par messagerie instantanée, *etc.* Son utilisation n'est pas aussi compliquée qu'on pourrait le craindre, et faire du chiffrement une routine permet aux informations particulièrement sensibles d'être noyées dans la masse.

Pour finir ce petit tour des techniques de cryptographie, il est bon de se rappeler que le chiffrement, aussi difficile à casser soit-il, a des limites, qu'on a évoquées dans le premier tome de ce guide. Ces limites touchent notamment à la confiance qu'on met

page 50

21. Austitci, 2005, *CRACKDOWN, violato autistici.org – some legal notes* [https://www.autistici.org/ai/crackdown/legal_en.html] (en anglais).

22. Wikipédia, 2014, *Confidentialité persistante* [https://fr.wikipedia.org/wiki/Confidentialit%C3%A9_persistante].

dans l'ordinateur et les logiciels auxquels on confie le chiffrement et le déchiffrement (et donc le texte *en clair*). Elles touchent aussi aux obligations légales de fournir aux autorités les moyens de déchiffrer des communications lorsqu'elles le demandent. Elles touchent enfin à l'évolution de la cryptographie : ce qui est sûr aujourd'hui ne le sera peut-être pas demain.

page 50

Enfin, si le chiffrement permet de cacher le contenu de la communication, les parties impliquées (qui communique avec qui) restent apparentes.

Chapitre 32

Tor ou le routage en oignon

Nous avons vu qu'il est possible de cacher le contenu des communications grâce au chiffrement. Cependant il est toujours possible pour des adversaires de déterminer la source et la destination des communications. Tor permet de résoudre ce problème.

32.1 La problématique : cacher l'origine et la destination

Les lettres en papier affichent l'adresse de la destinataire et celle de l'expéditrice. De même, sur Internet chaque paquet contient une adresse IP source (expéditrice) et une adresse IP de destination (destinataire). Les serveurs auquels on se connecte peuvent donc savoir d'où vient le paquet. Même en chiffrant les données, les adresses restent visibles.

page 258

La route entre l'expéditrice et la destinataire implique de passer par de multiples routeurs. Chacun de ces routeurs inspecte l'adresse IP de destination et transmet le paquet au routeur voisin le plus proche de cette destination. Ils voient ainsi que l'expéditrice communique avec la destinataire ; de même que les factrices voient d'où vient un colis et où il va.

page 208

Tout particulièrement, le fournisseur d'accès Internet est en mesure de faire un profilage exhaustif de l'utilisation d'Internet de ses abonnées. De la même façon, tous les routeurs de l'Internet qui voient passer nos paquets peuvent profiler nos comportements [1].

32.2 Une solution : Tor

Tor signifie *The Onion Router*, c'est-à-dire « le routeur oignon ». Il s'agit d'un logiciel libre.

page 39

De manière générale, Tor essaie de résoudre trois problèmes de vie privée [2] :

Premièrement, Tor empêche les sites web et autres services de connaître la localisation des internautes, qu'ils peuvent utiliser pour construire des bases de données sur leurs habitudes et leurs intérêts. Avec Tor, les connexions Internet ne dévoilent pas par défaut les données personnelles.

Deuxièmement, Tor empêche les gens d'espionner le trafic localement (comme les FAI ou une adversaire qui aurait accès au Wi-Fi domestique) et de voir quelles informations sont accédées sur quels serveurs. Cela les empêche aussi de restreindre ce que l'on peut consulter et publier.

1. L'essentiel de cette partie est une adaptation du site web de Tor : *Quelles sont les protections fournies par Tor ?* [https://support.torproject.org/fr/about/protections/].
2. Cette partie est issue du site web du projet Tor : *Quelles sont les protections fournies par Tor ?* [https://support.torproject.org/fr/#protections].

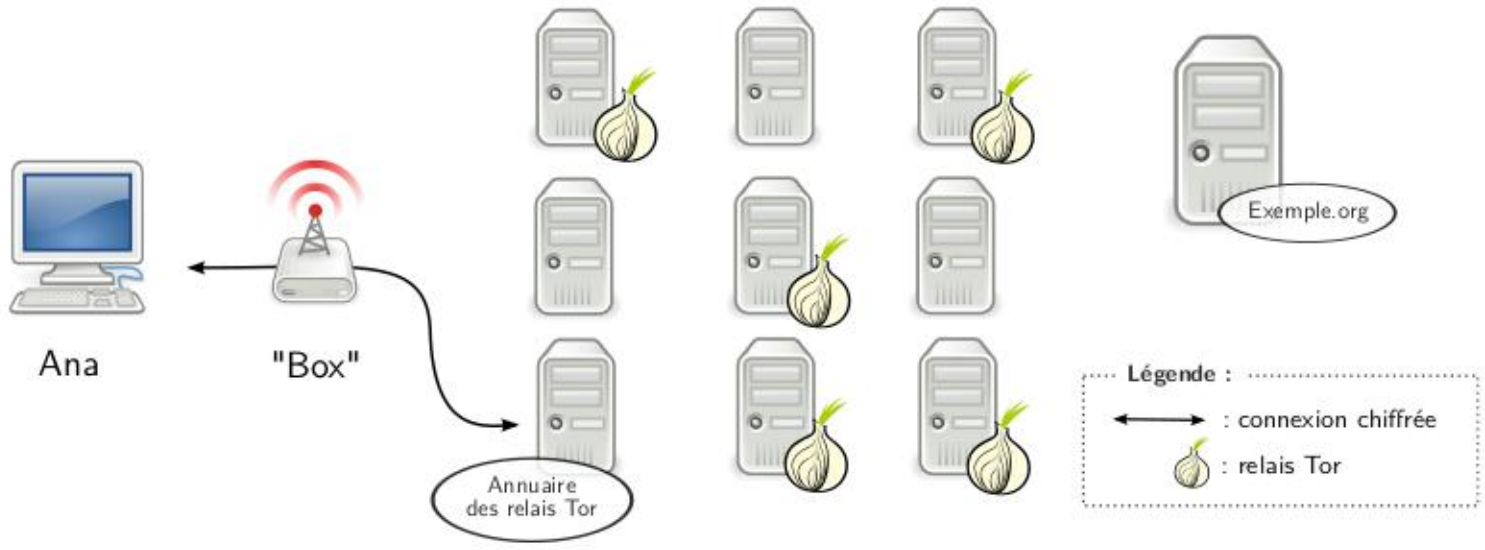
Troisièmement, Tor route les connexions à travers plusieurs relais Tor ; ainsi, aucun relai Tor ne peut savoir ce qui est fait. Du fait que ces relais sont opérés par des organisations ou par des personnes différentes, la distribution de la confiance fournit plus de sécurité qu'un simple VPN.

page 227

32.2.1 Création d'un circuit

Au lieu d'emprunter un itinéraire direct entre la source et la destination, les paquets de données suivent une trajectoire à travers plusieurs relais choisis en partie au hasard [3]. Des adversaires ne peuvent donc pas, en observant un seul point, associer la source et la destinataire.

Par exemple, lorsque Ana veut se connecter à *exemple.org* en utilisant Tor, son ordinateur commence par établir un circuit Tor.



Connexion à un annuaire de relais Tor

Pour cela :

1. Tor récupère une liste des nœuds Tor disponibles auprès d'un annuaire ;
2. Tor choisit dans cette liste un premier relai, puis établit une connexion chiffrée avec celui-ci ;
3. Tor choisit un second relai dans la liste et établit une connexion chiffrée vers ce second relai passant par le premier relai ;
4. enfin, Tor choisit dans la liste un troisième relai, appelé nœud de sortie, et établit une connexion chiffrée vers ce troisième relai passant par le premier et le second relai.

Cet ensemble de trois relais constitue ce qu'on appelle un *circuit Tor*.

32.2.2 Utilisation du circuit

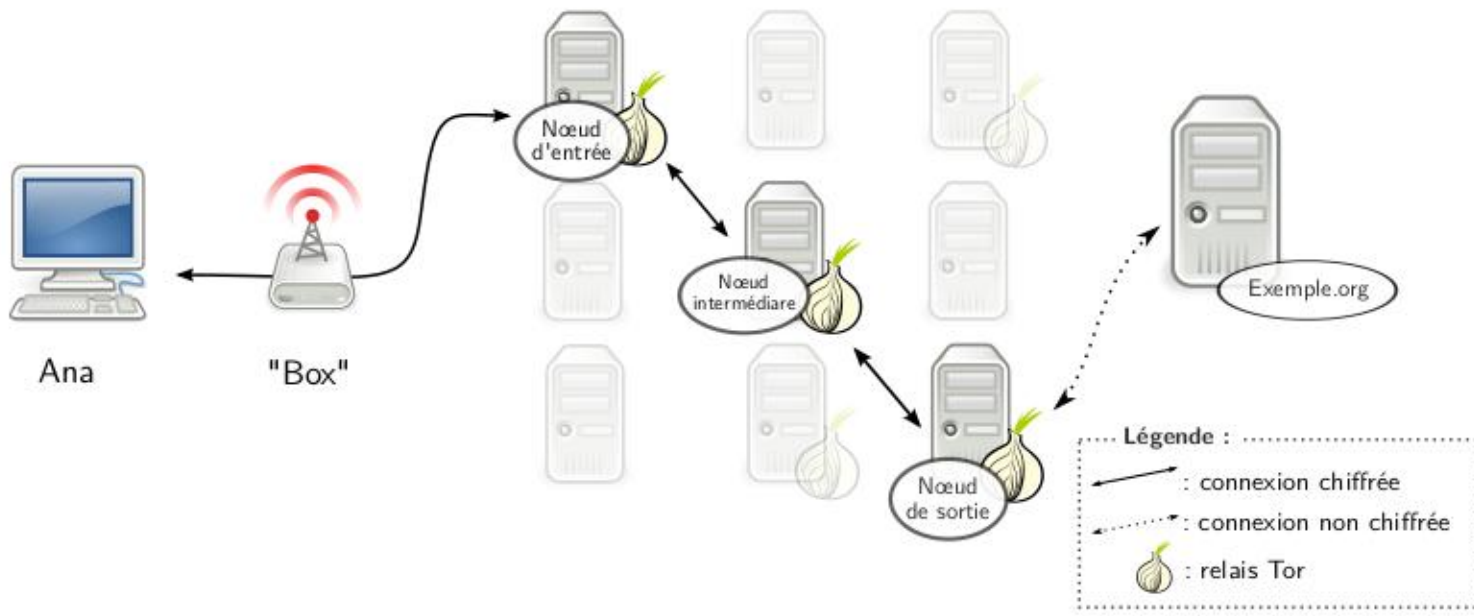
Ensuite, les données transiteront successivement par ces trois relais avant d'atteindre le serveur de destination (ici *exemple.org*). La réponse du serveur suivra le même chemin, dans le sens inverse.

Le circuit est parcouru étape par étape, et chaque relai le long du chemin ne connaît que celui qui lui a transmis les données, et celui auquel il va les retransmettre. Aucun relai ne connaît à lui tout seul le chemin complet pris par un paquet de données. Un éventuel intermédiaire ou un relai compromis ne peut pas aisément analyser le trafic réseau pour établir une relation entre la source et la destination d'une connexion. Aucun des ordinateurs ne sait donc que la machine d'Ana se connecte à *exemple.org*.

On note qu'un circuit Tor est composé de trois intermédiaires. Si le circuit était composé d'un seul relai, la compromission de celui-ci suffirait à mettre en péril notre

page 235

3. Le choix des relais est fait en obéissant à différentes contraintes qui sont listées dans la spécification de Tor (en anglais) : Roger Dingledine, Nick Mathewson, 2021, *Tor Path Specification* [https://gitweb.torproject.org/torspec.git/tree/path-spec.txt], section « 2.2. Path selection and constraints ».



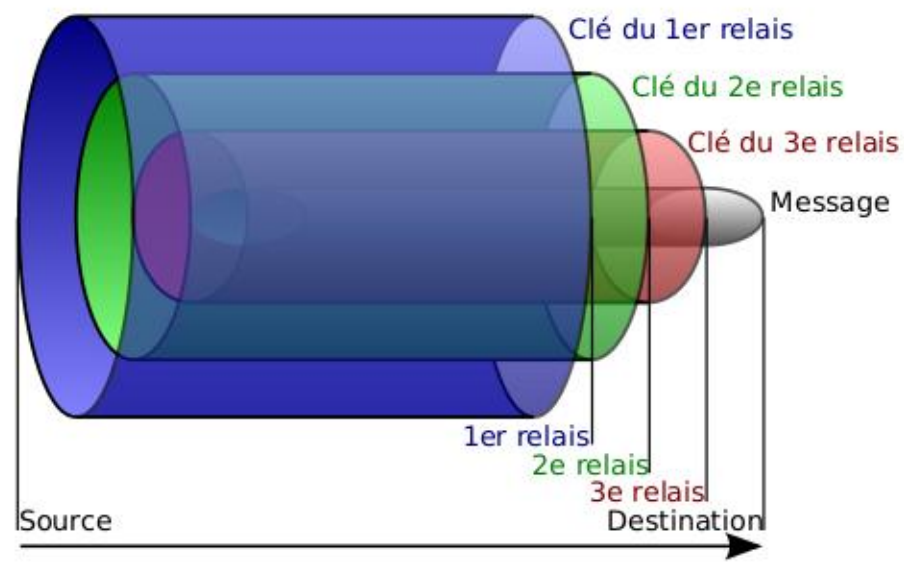
Utilisation d'un circuit Tor

confidentialité, car cet intermédiaire aurait connaissance à la fois de l'origine d'une communication et de sa destination. Le fait d'utiliser trois relais permet d'éviter ce recoupement sans ralentir la connexion de manière trop importante. Mis à part les nœuds de sortie, aucun relai ne peut connaître le contenu des communications qu'il transporte.

Les « nœuds de sortie » se distinguent des autres relais Tor par deux aspects : ce sont les seuls à potentiellement pouvoir voir du trafic en clair (si les personnes qui utilisent Tor n'utilisent pas HTTPS par exemple) et ce sont les seuls à être exposés sur Internet. C'est à dire que le trafic des personnes qui utilisent Tor semble provenir de ces nœuds de sortie. Aussi, les personnes qui font tourner des nœuds de sortie sont parfois considérées commes responsables du trafic qui passe par ce nœud et doivent alors donner des explications [4].

Précaution supplémentaire, le circuit Tor utilisé est modifié automatiquement toutes les dix minutes sans activité [5].

32.2.3 Chiffrement en oignon



Principe du routage en oignon

On a vu que l'ordinateur d'Ana négocie une connexion chiffrée avec chaque relai du circuit utilisé. Le résultat est que les données qu'elle veut transmettre à *exemple.org* possèdent plusieurs couches de chiffrement à la sortie de son ordinateur :

- le chiffrement de la connexion vers le premier relai ;

4. Nos oignons, 2020, *Rapport Moral* [https://nos-oignons.net/Association/Rapport_moral_2019-2020.pdf] p. 5, section Abuses.

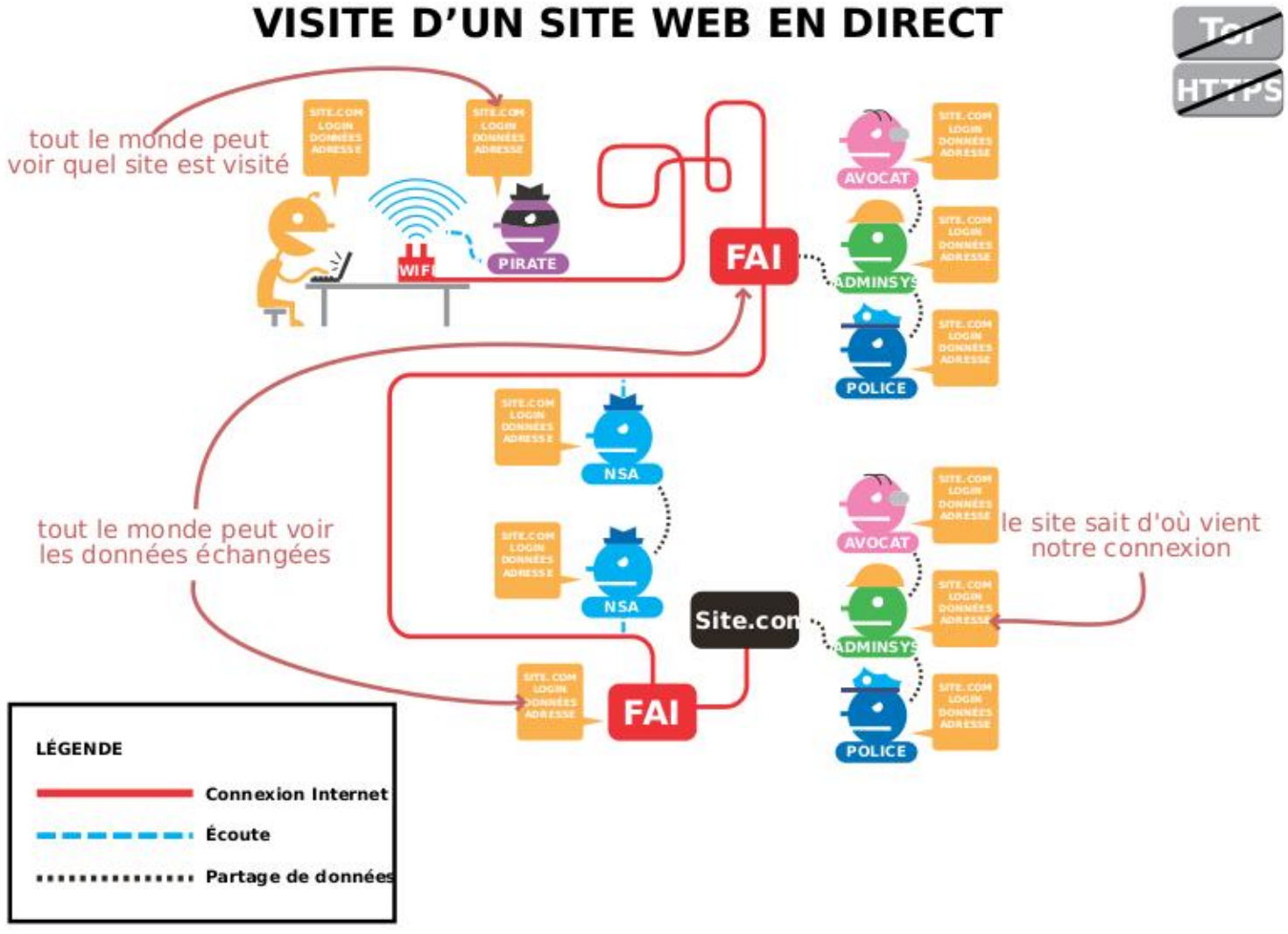
5. Tor Project, 2021, *À quelle fréquence Tor change-t-il ses chemins ?* [https://support.torproject.org/fr/about/change-paths/].

- le chiffrement de la connexion vers le second relai ;
- le chiffrement de la connexion vers le troisième relai.

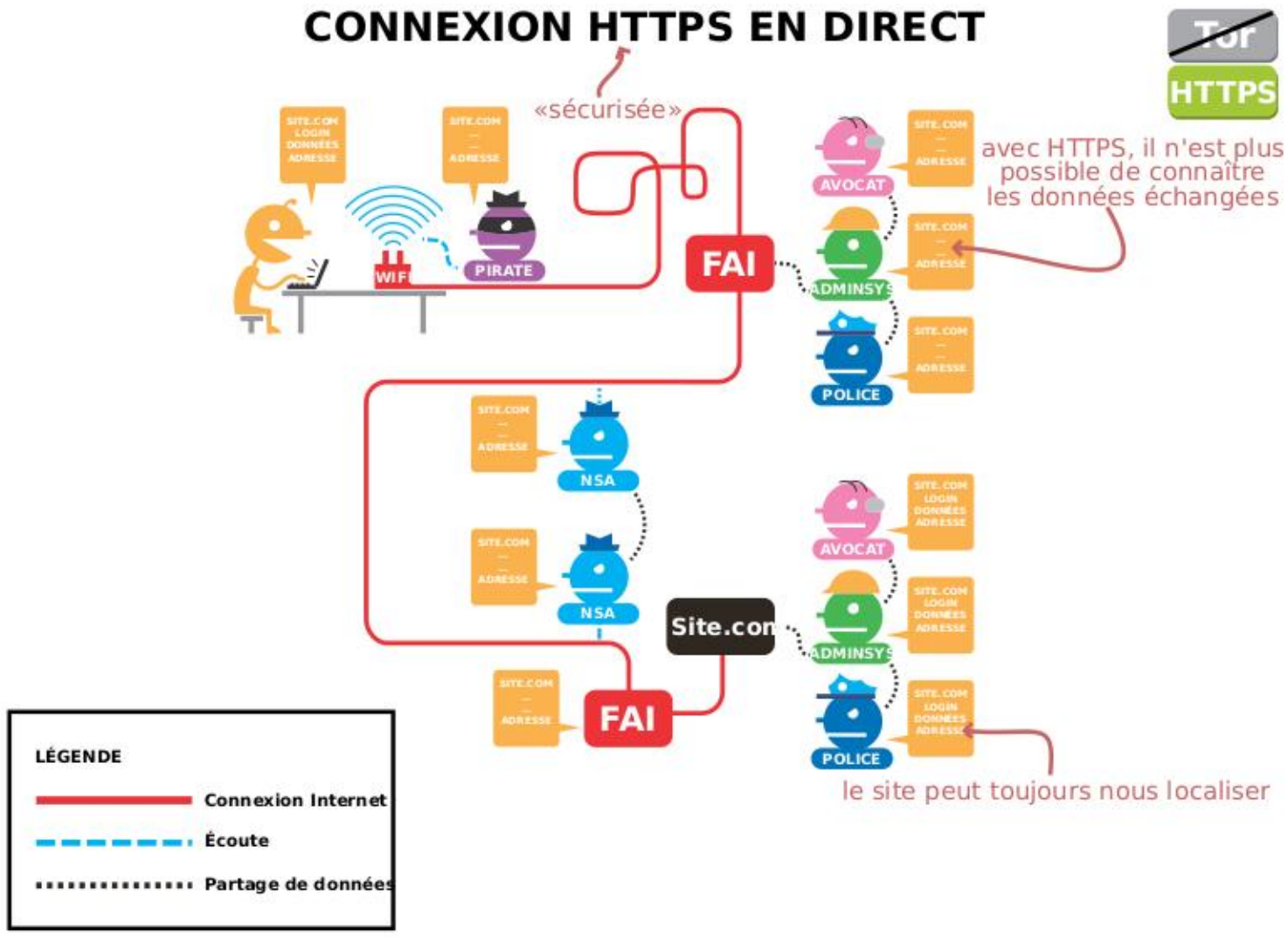
À l'image d'un oignon possédant plusieurs peaux, les données d'Ana seront *enrobées* dans plusieurs couches de chiffrement. C'est pour cela que l'on peut parler de *chiffrement en oignon*. À chaque passage par un relai, une couche de chiffrement sera *enlevée*. Chaque couche sera chiffrée pour ne pouvoir être lue que par le relai qui devra l'enlever. Aucun des relais ne peut donc déchiffrer les informations qui ne lui sont pas destinées.

32.2.4 Tor illustré

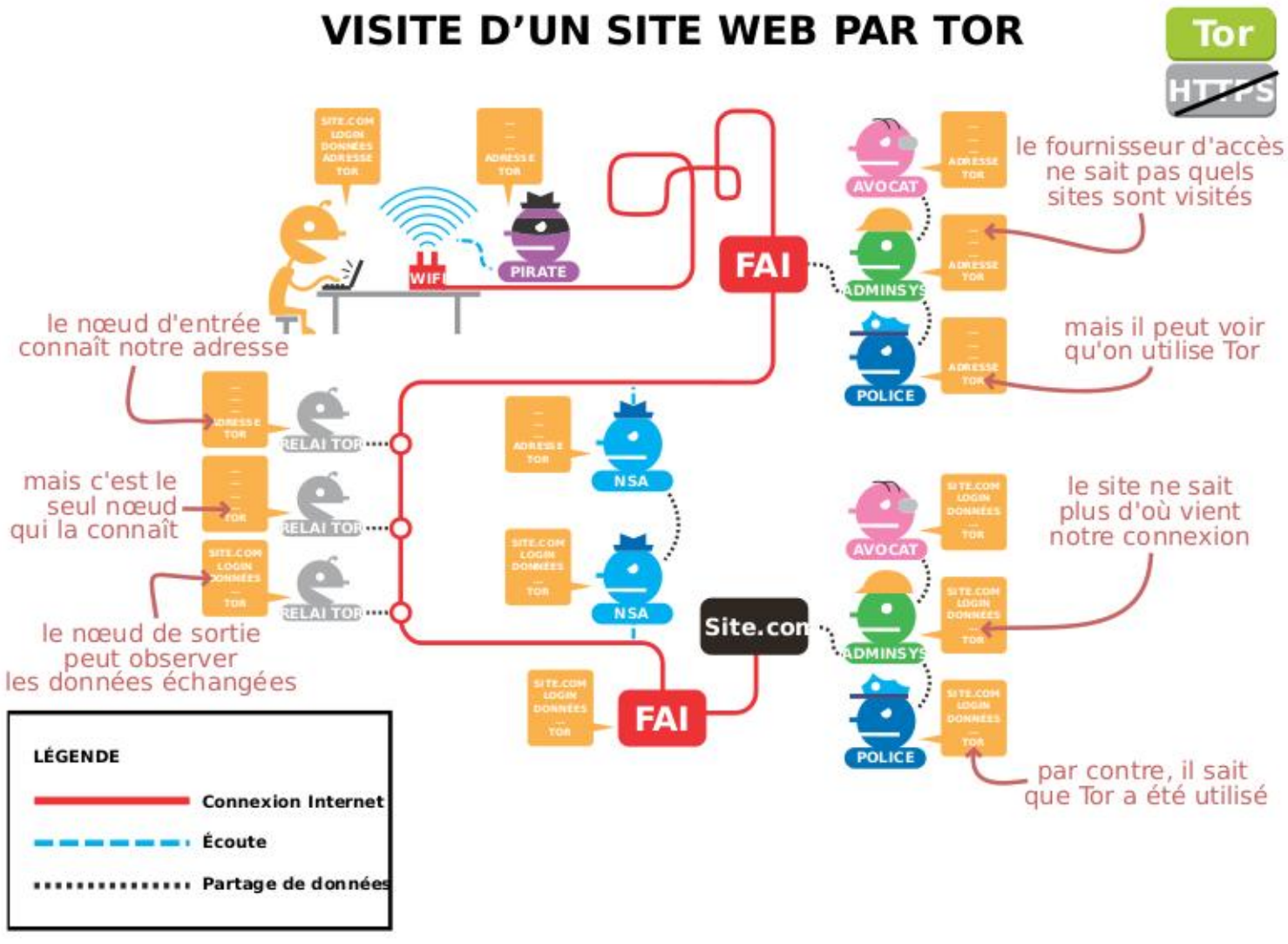
Voici quatre schémas qui illustrent ce que des tiers peuvent voir et/ou espionner en fonction de l'utilisation de HTTPS ou non, et de l'utilisation de Tor ou non lors de la consultation d'un site web.



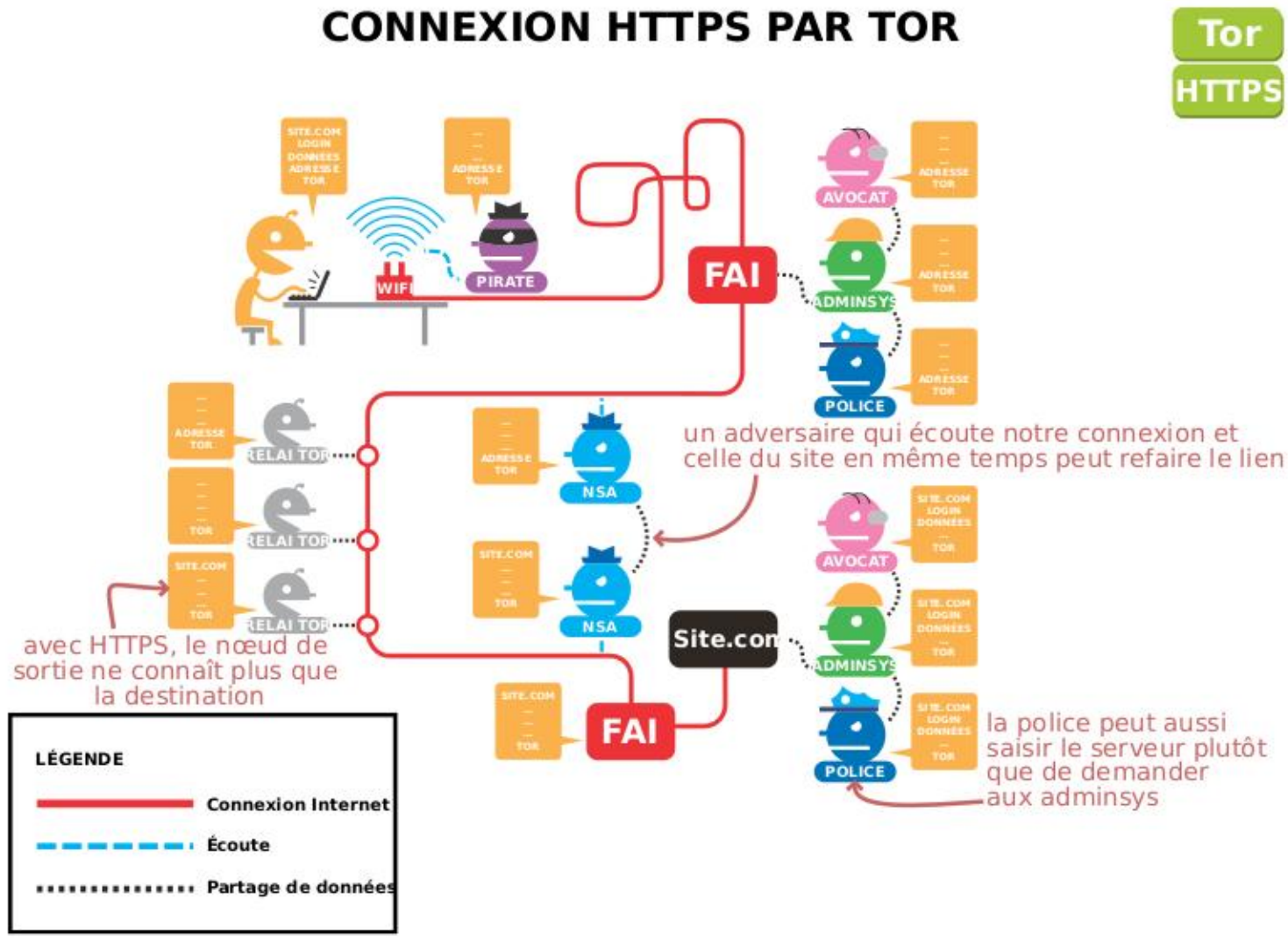
Visite d'un site web en direct



Connexion HTTPS en direct



Visite d'un site web par Tor



Connexion HTTPS par Tor

32.3 Les services onion

Si l'on souhaite fournir des services (un site web ou un serveur de messagerie instantanée par exemple), sans dévoiler l'addresse (IP) du serveur, il est possible d'utiliser un service onion [6]. De la même manière que pour chaque utilisatrice de Tor, l'adresse IP du serveur mis en place n'est pas dévoilée. Les personnes souhaitant s'y connecter devront nécessairement utiliser le réseau Tor. Ainsi, les services onion permettent de protéger à la fois la confidentialité du serveur et des personnes qui l'utilisent.

Afin de s'y connecter, les internautes utiliseront le système des « points de rendez-vous » de Tor. Le « point de rendez-vous » est le troisième relai pour chacun des deux protagonistes de l'échange : le client et le service onion. Le client construit un circuit Tor avec comme troisième relai ce « point de rendez-vous ». De son côté, le service onion fait de même. Client et service onion se « rencontrent » alors et peuvent échanger des informations.

Ces services onion peuvent par exemple permettre de mettre en place un site web sans craindre la censure. L'identification de l'emplacement physique du serveur (ou des personnes qui publient ou qui visitent le site web), est en effet rendue beaucoup plus difficile que dans le cadre d'un site web conventionnel : cela nécessite de mettre en place une attaque sur le réseau Tor.

page 268

32.4 Participer au réseau Tor

Le réseau Tor repose sur la base du volontariat. Il est ouvert à tout le monde puisque aucun relai ne peut connaître à la fois la provenance des communication et leur destination. Quiconque le souhaite peut donc faire tourner sur l'ordinateur de son choix un relai Tor. Ce dernier rejoindra le réseau public et relayera le trafic des personnes utilisant ce réseau.

6. The Tor Project, 2013, *How do onion services work?* [https://community.torproject.org/onion-services/overview/] (en anglais). Ces services onion ont des adresses en *.onion*.

32.4.1 Monter un relai Tor

Le fait que quiconque puisse mettre en place un relai introduit de la diversité, renforçant ainsi l'efficacité du réseau Tor dans son ensemble.

Les relais Tor sont considérés légalement comme des routeurs[7] et ne sont donc pas tenus de conserver de journaux, c'est-à-dire de garder la trace des communications. page 29 C'est une bonne chose car, si des adversaires avaient accès aux journaux de multiples relais Tor, il leur serait possible de découvrir les circuits a posteriori.

Comme on l'a vu plus haut, les personnes qui font tourner des nœuds de sortie sont parfois considérées commes responsables du trafic qui passe par ce nœud et doivent alors s'expliquer avec les autorités. C'est pourquoi, pour éviter de s'exposer individuellement, il vaut mieux configurer Tor pour que son relai ne puisse pas être un nœud de sortie et contribuer à une association dédiée à la gestion de nœuds de sortie[8].

32.4.2 Monter un bridge Tor

Il est aussi très utile de mettre en place des « bridges » ou « ponts » Tor[9]. Il s'agit de relais particuliers qui ne sont pas listés dans les annuaires publics[10] du réseau Tor. Ils peuvent permettre à des personnes dont le fournisseur d'accès à Internet filtre les connexions à Tor de se connecter tout de même au réseau.

32.5 Quelques limites de Tor

Tor peut facilement donner une fausse impression de sécurité. Il répond effectivement au besoin de dissimuler son adresse IP et à celui de masquer avec quels serveurs on est en communication. Tor ne résout cependant pas tous les problèmes[11] :

1. Tor ne protège pas si l'on ne l'utilise pas correctement ;
2. Même si l'on configure et que l'on utilise Tor correctement, il y a encore des attaques potentielles qui peuvent compromettre la protection fournie par Tor ;
3. Aucun système d'anonymisation n'est parfait à ce jour, et Tor ne fait pas exception : il serait imprudent de se reposer uniquement sur le réseau Tor si l'on a besoin d'une confidentialité absolue.

Détaillons à présent quelques-unes de ces limites.

32.5.1 La personne mal informée ou peu attentionnée

Quand on est mal informée, on a de grandes chances de se tromper. Lorsque l'on utilise un outil, il est capital de bien comprendre à quoi il sert, mais aussi et surtout à quoi il ne sert pas, ainsi que ses limites.

Par exemple, si on utilise le Navigateur Tor pour remplir des formulaires web avec des informations personnelles, le site web ne connaîtra pas notre emplacement d'origine, mais par contre il aura toutes les informations du formulaire. Donc on ne sera pas totalement anonyme.

---

7. Nos oignons, 2013, *Qu'est-ce que c'est ?* [https://nos-oignons.net/%C3%80_propos/index.fr.html].
8. Nos oignons, 2013, *Qu'est-ce que c'est ?* [https://nos-oignons.net/%C3%80_propos/index.fr.html].
9. Pour comprendre et utiliser les bridges Tor, on peut aller voir la Documentation de Tails, *Se connecter au réseau Tor* [https://tails.boum.org/doc/anonymous_internet/tor/index.fr.html#index1h1] et la page dédiée aux bridges Tor [https://bridges.torproject.org/?lang=fr] du projet Tor.
10. Il est en revanche possible d'obtenir des adresses de bridges Tor en visitant BridgeDB [https://bridges.torproject.org/?lang=fr].
11. Pour en savoir plus, consulter le site web de Tor : Projet Tor, 2021, *Suis-je complètement anonyme si j'utilise Tor ?* [https://support.torproject.org/fr/faq/staying-anonymous/].

Il faut se méfier des documents que l'on télécharge. Ils peuvent contenir des "ressources Internet" (images, vidéos ou autres) suceptibles de dévoiler notre adresse IP si on les ouvre avec une application qui n'est pas configurée pour se connecter avec Tor (un visionneur de PDF par exemple). Pour éviter de s'exposer, on peut ouvrir les documents téléchargés soit avec Tails qui ne se connecte à Internet que *via* Tor, soit avec un ordinateur déconnecté d'Internet.

32.5.2 Des adversaires voient que l'on utilise Tor

Le fournisseur d'accès à Internet, ou l'admin du réseau local d'Ana peut très facilement savoir qu'elle se connecte à un relai Tor, et non à un serveur web ordinaire [12]. En effet, la liste des IP des nœuds d'entrée Tor est disponible publiquement sur Internet. L'utilisation de *bridges* Tor permet plus de discretion vis à vis du FAI ou de l'admin du réseau local.

De la même manière, la liste de nœuds de sortie du réseau Tor est publique. Les admins d'un site web, qui peuvent voir la provenance des visites reçues, pourront donc identifier celles qui proviennent d'un relai Tor.

Tor ne protège pas en faisant ressembler les personnes qui utilisent Tor à n'importe quelle personne aléatoire d'Internet, mais en faisant en sorte que toutes les personnes qui utilisent Tor se ressemblent. Il devient impossible de savoir qui est qui parmi elles. Plus nombreuses seront les internautes utilisant Tor et plus variées seront leurs activités, moins l'utilisation de Tor sera incriminante. La solidité de ce réseau repose notamment sur cet ensemble non distinguable d'utilisatrices ; c'est ce qu'on appelle en anglais l'*anonymity set*.

32.5.3 Les nœuds de sortie Tor peuvent espionner les communications qu'ils relaient

Tor ne chiffre pas les communications en dehors de son propre réseau. Tor ne peut donc pas chiffrer ce qui transite entre le nœud de sortie et le serveur de destination. Tout nœud de sortie a donc la possibilité de capturer le trafic qu'il relaie vers Internet [13].

Par exemple, en 2007, un chercheur en sécurité informatique a intercepté des milliers d'emails privés envoyés par des ambassades et des ONG à travers le monde en écoutant le trafic du nœud de sortie qu'il administrait [14], avec une attaque de type « monstre du milieu ».

page 254

Pour se protéger contre de telles attaques, il est nécessaire d'utiliser du chiffrement de bout en bout, évoqué dans la partie sur le chiffrement asymétrique.

page 249

32.5.4 Attaque de type « motif temporel »

La conception de Tor ne permet pas de protéger contre certains types d'attaques, notamment de l'ordre de l'analyse de trafic [15]. L'attaque par « motif temporel » en est une. L'idée derrière cette attaque est d'observer le rythme d'envoi des données à deux endroits de leur trajet, par exemple sur le premier relai et sur le troisième relai (nœud de sortie). Envoyons par exemple un flux comme du code morse : trois paquets envoyés en salve, puis cinq secondes de silence, puis trois paquets, *etc.*

---

12. Cette section, ainsi que les suivantes, sont fortement inspirées du site web de Tails [https://tails.boum.org/doc/about/warnings/index.fr.html#doc-about-warnings.fr.tor].
13. Tor Project, 2021, *Quand j'utilise Tor, les écoutes électroniques peuvent-elles encore voir les renseignements que je partage avec les sites web, tels que les renseignements de connexion, et ce que je tape dans les formulaires ?* [https://support.torproject.org/fr/https/https-1/].
14. Kim Zetter, 2007, *Rogue Nodes Turn Tor Anonymizer Into Eavesdropper's Paradise* [https://www.wired.com/politics/security/news/2007/09/embassy_hacks] (en anglais).
15. Wikipédia, 2014, *Attaque par analyse du trafic* [https://fr.wikipedia.org/wiki/Attaque_par_analyse_du_trafic].

Des adversaires qui voient que l'ordinateur d'Ana envoie sur le premier relai un flux avec un motif temporel donné, et qui observent un flux avec ce même motif sur le nœud de sortie qui va vers *exemple.org*, peuvent en déduire que c'est probablement l'ordinateur d'Ana qui est connecté à *exemple.org*[16].

La force, mais aussi la faiblesse de Tor, c'est que n'importe qui peut l'utiliser, mais aussi administrer un relai Tor : Ana, Bea, une université, la CIA, *etc.* Si des adversaires n'ont les informations que d'un seul des relais par lesquels transitent les données, pas de problème. S'il se trouve que par malchance, des adversaires qui coopèrent ont la main sur plusieurs relais, ils peuvent mener une attaque de type « motif temporel ».

Les fournisseurs d'accès à Internet et les gros fournisseurs de contenu ou de ressources utilisées sur de nombreux sites web — encarts publicitaires, fonctionnalités de recherche et de médias sociaux — sont aussi en bonne position pour observer le trafic et donc collaborer à ce type d'attaque.

32.5.5 Tor ne protège pas contre les attaques par confirmation

On vient de voir que la conception de Tor ne permet pas de protéger contre des adversaires capables de mesurer le trafic qui entre et qui sort du réseau Tor. Car si les adversaires peuvent comparer les deux flux, il est possible de les corréler *via* des statistiques basiques.

Considérons maintenant des adversaires aient des raisons de penser que c'est Ana qui publie sur tel blog anonyme. Pour confirmer leur hypothèse, elles pourront observer le trafic qui sort de la connexion fibre d'Ana et le trafic qui entre sur le serveur qui héberge le blog. Si elles observent les mêmes motifs de données en comparant ces deux trafics, elles pourront être confortées dans leur hypothèse.

Tor protège Ana contre des adversaires qui cherchent à déterminer qui publie sur le blog anonyme. Mais il ne protège pas contre des adversaires ayant davantage de moyens qui essayent de confirmer une hypothèse en surveillant aux bons endroits dans le réseau puis en faisant la corrélation.

Ce type d'attaque peut aussi s'effectuer avec des hypothèses plus larges.

Considérons des adversaires qui suspectent un groupe de connexions ADSL de se connecter à un blog anonyme sur lequel les autrices ne publient qu'en passant par Tor. Imaginons que ces adversaires ont accès à la fois au trafic du groupe de connexions ADSL en question, et à celui du serveur — par exemple grâce à une réquisition ou à une boîte noire[17]. Ces adversaires peuvent alors grâce à une attaque de type « motif temporel », trouver quelle est la connexion parmi le groupe suspect qui est à l'origine de telle connexion au serveur. Ainsi, la publication d'un billet de blog peut être corrélé à une connexion parmi un groupe de personnes soupçonnées de participer à ce blog anonyme.

page 228

32.5.6 Tor ne protège pas face à une organisation globale adverse

Une organisation globale adverse est une entité capable d'analyser le trafic entre tous les ordinateurs d'un réseau. Par exemple, en étudiant les volumes d'informations des différentes communications à travers ce réseau à chaque instant, il serait statistiquement possible d'identifier un circuit Tor car le même flux d'information y apparaîtrait à quelques millisecondes d'intervalle à chaque nœud du circuit. L'adversaire pourrait ainsi faire le lien entre une utilisatrice de Tor et son serveur destinataire.

---

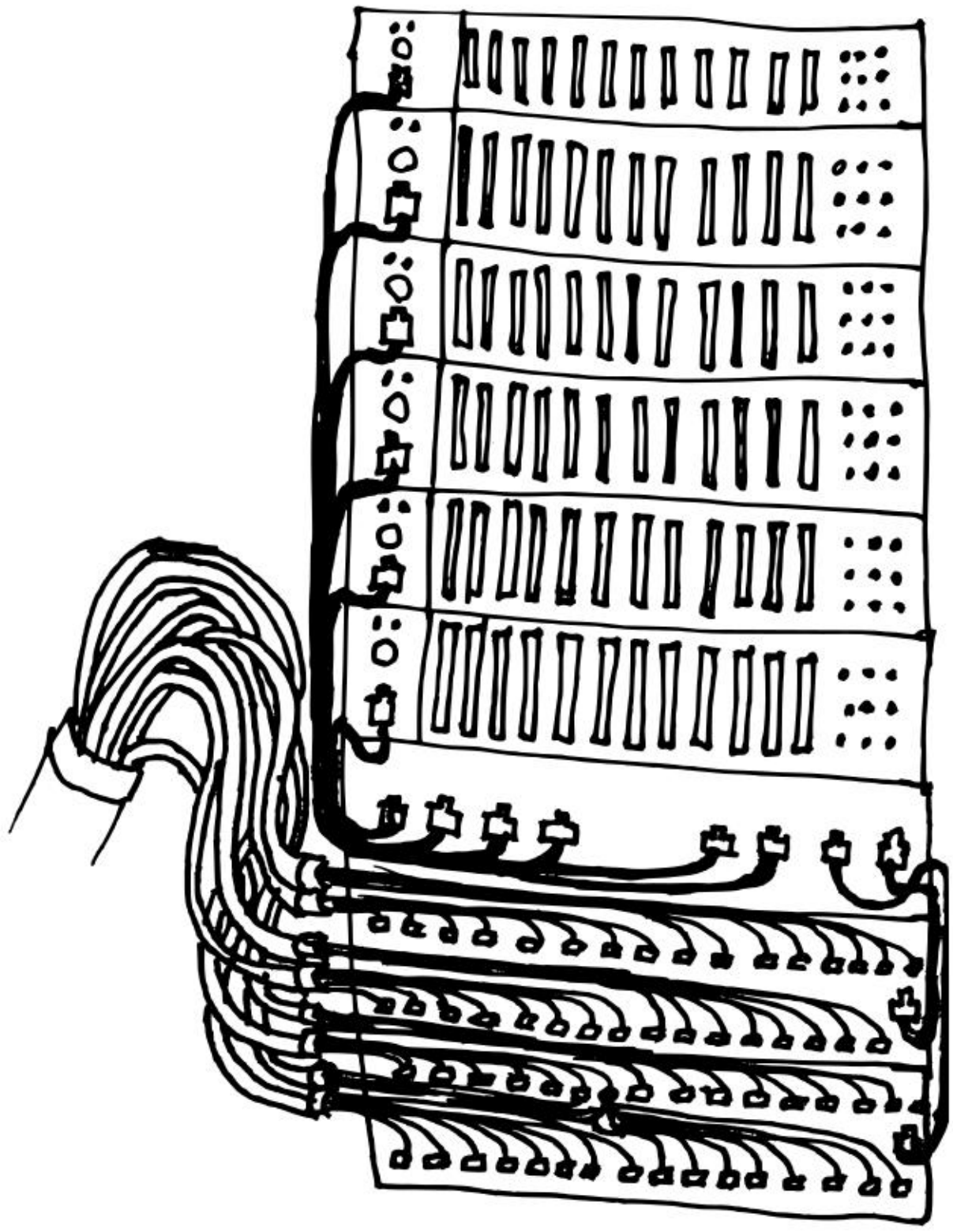
16. Voir à ce sujet Wikipédia, 2014, *Tor (réseau)* [https://fr.wikipedia.org/wiki/Tor_(r%C3%A9seau)].

17. Ici, on fait référence au dispositif qui permet aux services de renseignement d'analyser automatiquement les métadonnées des communications Internet en France (Le Monde, 2017, *Une première « boîte noire » de la loi sur le renseignement désormais active* [https://www.lemonde.fr/pixels/article/2017/11/14/les-boites-noires-de-la-loi-sur-le-renseignement-sont-desormais-actives_5214596_4408996.html]).

Une organisation globale adverse, ayant des moyens comparables à ceux de la NSA par exemple, pourrait également mettre en place d'autres attaques visant à briser la confidentialité apportée par le réseau Tor. C'est un compromis de Tor, qui permet une navigation raisonnable en termes de délais d'attente (pour le web ou la messagerie instantanée par exemple) [18].

Toutefois, les risques résultant de ces limites ne sont pas comparables à ceux rencontrés lors d'une navigation sans Tor. Tor est l'un des outils les plus efficaces en matière de confidentialité sur Internet. S'il faut les garder à l'esprit, ces risques ne devraient pas nous détourner de son utilisation avisée.

18. Roger Dingledine, Nick Mathewson, Paul Syverson, 2004, *Tor Project : The Second-Generation Onion Router* [https://svn.torproject.org/svn/projects/design-paper/tor-design.pdf], partie « 3. Design goals and assumptions » (en anglais).



Cinquième partie

Choisir des réponses adaptées

Introduction

Pas de panique ! Se protéger n'est pas impossible, ni trop compliqué. On peut aller doucement, concept après concept, pour dessiner notre propre stratégie d'autodéfense numérique.

Plein de possibilités s'offrent à nous : le pigeon voyageur, la lettre scellée... Avant Internet, on rencontrait nos potes chaque soir au coin de la rue. Des solutions encore possibles à ne pas oublier, ceci dit. Désormais, on peut utiliser des outils pour chiffrer notre message et l'envoyer en quelques millisecondes à l'autre bout du monde.

Dans cette partie, on décrira des exemples concrets, qu'on nomme *cas d'usage*, afin de proposer des solutions à quelques situations typiques.

Chapitre 33

Cas d'usage : consulter des sites web

33.1 Contexte

On s'intéresse ici à la consultation d'informations disponibles sur le web : lire un périodique, suivre un blog, *etc.* Autant d'activités ordinaires lorsqu'on est *en ligne*.

Cependant, on veut effectuer ces activités de façon discrète, pour diverses raisons, parmi lesquelles on peut citer :

- déjouer la surveillance ou contourner la censure, que ce soit celle d'une cheffe, d'une personne proche ou d'un État ;
- éviter la collecte et le recoupement d'informations personnelles à des fins commerciales ;
- généraliser l'utilisation de pratiques de discrétion, ce qui permet de protéger les personnes qui en ont vraiment besoin en les « noyant dans la masse ».

33.2 Évaluer les risques

33.2.1 Que veut-on protéger ?

Dans ce cas d'usage, ce qui nous importe en premier lieu est l'anonymat, ou tout du moins le pseudonymat : ce que l'on cherche à cacher n'est pas le contenu de *ce qui* est consulté, mais *par qui* il est consulté.

Nous avons vu précédemment que l'utilisation d'Internet, et notamment du web, laisse de nombreuses traces de diverses natures, à différents endroits. Nombre d'entre elles, telles de petits cailloux, esquissent un chemin qui va de la ressource consultée jusqu'à une maison, un ordinateur, voire la personne qui se trouve derrière. Ce sont donc ces traces sur le réseau dont on veut se débarrasser, au premier rang desquelles se trouve l'adresse IP. Cependant, l'IP étant nécessaire au bon fonctionnement du réseau, la stratégie sera ici de faire en sorte que quiconque suivant cette piste finisse dans une impasse.

page 202

Par ailleurs, on pourra éventuellement vouloir ne laisser aucune trace de notre navigation sur l'ordinateur utilisé, et en particulier sur son disque dur.

33.2.2 De qui veut-on se protéger ?

Cette question est importante : en fonction de la réponse qu'on lui donne, la politique de sécurité adéquate peut fortement varier.

Fournisseur d'accès à Internet

Ana travaille pour une grande entreprise et accède à Internet par l'intermédiaire du réseau de la société. Elle consulte ses blogs préférés pendant ses heures de boulot, mais ne souhaite pas que son employeuse le sache.

Dans ce cas, Ana souhaite se protéger de l'œil indiscret des personnes qui s'occupent du réseau, en l'occurrence de son entreprise. L'adversaire a ici accès à l'ensemble du trafic réseau qui transite par sa connexion puisque l'entreprise joue le rôle de factrice. Elle n'a, par contre, pas d'yeux placés en d'autres points d'Internet.

Fournisseurs de contenu

Bea est inscrite sur un forum de la police nationale, et passe — non sans un malin plaisir — un certain temps à semer la zizanie dans les discussions entre flics.

Dans ce cas, Bea ne souhaite pas rendre transparent au site hébergeant le forum qu'elle est la fauteuse de troubles. Comme vu précédemment, son adresse IP sera conservée plus ou moins longtemps par le site visité. L'adversaire aura ainsi accès aux en-têtes IP, ainsi qu'aux en-têtes HTTP.

page 225 page 217

Adversaires diverses et variées

page 217

Agathe va régulièrement consulter le site de publication de documents confidentiels sur lequel Bea a publié des relevés bancaires. Le sujet étant sensible, elle sait pertinemment que le blog en question pourrait être surveillé. Elle ne veut donc pas qu'on sache qu'elle va le consulter.

page 194

L'adversaire ici n'a pas de place fixe sur le réseau : elle peut se situer au niveau de l'ordinateur d'Agathe, au niveau de sa « box », au niveau du blog ou bien à tout autre endroit sur le chemin entre son ordinateur et le blog. L'adversaire peut également se situer à plusieurs endroits en même temps.

page 208

33.3 Définir une politique de sécurité

page 65

Posons-nous maintenant les questions exposées dans notre méthodologie :

1. Quel ensemble de pratiques et d'outils nous protègerait de façon suffisante contre nos adversaires ?
2. Face à une telle politique de sécurité, quels sont les angles d'attaque les plus praticables ?
3. Quels sont les moyens nécessaires pour les exploiter ?
4. Pensons-nous que ces moyens puissent être utilisés par nos adversaires ?

33.3.1 Première étape : avoir accès à l'un des serveurs

page 225

Angle d'attaque le plus praticable pour l'adversaire : analyser les données enregistrées par les serveurs fournissant la connexion ou hébergeant les ressources consultées.

Moyens nécessaires :

- se connecter au serveur qui fournit la connexion si l'adversaire est le fournisseur d'accès à Internet, ou collabore avec lui ;
- se connecter au serveur qui héberge la ressource consultée si l'adversaire est le fournisseur de contenu, ou collabore avec lui.

Si l'adversaire est le fournisseur d'accès Internet ou le fournisseur de contenu, il lui suffira de consulter ses journaux de connexions. Mais il est également possible à d'autres adversaires d'accéder à ces informations, par le biais d'une réquisition, d'un contrat commercial, d'une collaboration volontaire[1], voire d'un piratage.

page 226 page 228

Crédibilité d'une telle attaque : probable si notre connexion ou le site visité attirent l'attention de l'adversaire.

page 235

Contre ce type d'attaque, une solution efficace est d'utiliser le routage en oignon[2]

page 261

1. Jacques Follorou, Le Monde, 2014, *Espionnage : comment Orange et les services secrets coopèrent* [https://www.lemonde.fr/international/article/2014/03/20/dgse-orange-des-liaisons-incestueuses_4386264_3210.html].

en passant par le réseau Tor selon des modalités que l'on présentera plus loin. Pour bien cloisonner nos identités contextuelles, on veillera à ne pas mélanger nos activités quotidiennes avec celles que l'on souhaite plus discrètes.

page 243

33.3.2 Deuxième étape : regarder sur l'ordinateur utilisé

Si nous utilisons le routage en oignon, l'adversaire observant les données circulant sur le réseau ne peut savoir d'où viennent ces données, ni où elles vont. Elle doit alors trouver un autre moyen d'y parvenir.

Angle d'attaque le plus praticable : avoir accès aux traces laissées sur l'ordinateur par les sites visités.

page 27

Moyens nécessaires : accéder à l'ordinateur utilisé.

Crédibilité d'une telle attaque : dans le cas d'Ana qui utilise l'ordinateur de son boulot, cela est très facile pour son adversaire. Dans d'autres cas et selon l'adversaire, cela nécessite soit un cambriolage (également appelé perquisition, quand il est légal), soit de corrompre l'ordinateur cible de l'attaque, par exemple en y installant un logiciel malveillant.

page 31

Pour se prémunir contre cette attaque, il est nécessaire de chiffrer son disque dur pour rendre les traces laissées difficiles d'accès. Mieux encore, il s'agit d'éviter de laisser des traces dès le départ en utilisant un système *live* amnésique, qui n'enregistrera rien sur l'ordinateur utilisé.

page 119
page 113

33.3.3 Troisième étape : attaquer Tor

Angle d'attaque : exploiter les limites de l'anonymat fourni par Tor, par exemple en effectuant une attaque par confirmation.

page 267
page 269

Moyens nécessaires : être capable de surveiller plusieurs points du réseau, par exemple la connexion utilisée *et* le site consulté.

Crédibilité d'une telle attaque : une adversaire comme une entreprise qui chercherait à surveiller ses salariées a peu de chances de monter une telle attaque. Idem pour les gendarmes de Saint-Tropez. Elle peut cependant être à la portée d'un fournisseur de services réseau d'envergure nationale ou mondiale, voire de flics spécialisées. Encore une fois, n'oublions pas qu'il y a une différence notable entre « avoir la capacité technique de mettre en place une attaque » et « mettre effectivement en place cette attaque ». Cette différence tenant principalement au coût économique et au retour sur investissement d'une telle attaque ciblée.

Rappelons au passage que de nombreuses autres attaques contre Tor sont possibles ou envisagées. Retenons surtout qu'il est nécessaire de bien comprendre les objectifs et les limites du routage en oignon pour ne pas se tirer une balle dans le pied.

page 261
page 267

33.4 Choisir parmi les outils disponibles

En fonction de nos besoins et de notre politique de sécurité, il nous faudra choisir parmi différents outils.

33.4.1 Le Navigateur Tor sur notre système ou dans Tails

Le Navigateur Tor sur notre système d'exploitation

Le Navigateur Tor est un *pack* de logiciels : il fournit un navigateur web préconfiguré pour surfer de façon confidentielle, en utilisant le réseau Tor, à partir de notre système

2. Contre certaines des adversaires listées ici, d'autres solutions techniques peuvent suffire, comme l'utilisation d'un VPN [https://fr.wikipedia.org/wiki/R%C3%A9seau_priv%C3%A9_virtuel] par exemple. Cependant, le routage en oignon protège contre beaucoup plus des attaques possibles qu'un VPN, qui n'insère entre nous et la ressource consultée qu'un seul intermédiaire.

page 313 d'exploitation habituel[3]. Une fois le Navigateur Tor installé, on peut choisir d'utiliser ce navigateur web utilisant Tor, ou notre navigateur web habituel[4].

Avantages Le Navigateur Tor permet de naviguer sur le web avec Tor depuis notre système d'exploitation habituel. Il permet par exemple de travailler sur un document avec nos outils habituels, tout en cherchant des informations sur le web de façon anonyme.

Inconvénients Le Navigateur Tor s'exécutant sur le système d'exploitation habituel, cela implique qu'une faille dans ce dernier permettrait à des adversaires de contourner la protection offerte par l'usage du réseau Tor. Mais surtout, utilisé en dehors d'un système amnésique, le Navigateur Tor laissera probablement des traces sur le disque dur de l'ordinateur utilisé.

Le Navigateur Tor est basé sur Firefox et il peut y avoir un délai plus ou moins long pour que les mises à jour de ce dernier soient prises en compte. Pendant ce délai, le Navigateur Tor présentera des failles de sécurité connues et publiées.

Si le Navigateur Tor vient à planter, on peut perdre définitivement toutes ses lectures et recherches en cours[5].

Le Navigateur Tor n'empêche pas d'autres programmes de se connecter à Internet sans passer par Tor, et ce, même s'ils sont ouverts depuis le Navigateur Tor (logiciels P2P, lecteur de fichiers PDF, lecteurs multimedia, *etc.*).

Tails

page 113 *Tails*[6] est un système *live* dont le but est de préserver la confidentialité et l'anonymat des personnes qui l'utilisent. Il permet d'accéder à Internet de manière anonyme quasiment partout et depuis n'importe quel ordinateur. De plus, il ne laisse aucune trace des activités effectuées sur l'ordinateur, à moins qu'on ne le lui demande explicitement.

Avantages En ayant recours à Tails, non seulement on ne laisse pas de trace sur l'ordinateur utilisé, mais les logiciels ayant besoin d'accéder à Internet sont configurés pour passer par le réseau Tor, et les connexions directes (qui ne permettent pas l'anonymat) sont bloquées.

De plus, comme il s'agit d'un système *live*, Tails démarre à partir d'un DVD ou d'une clé USB, sans modifier le système d'exploitation installé sur l'ordinateur. On peut ainsi l'utiliser à la maison, sur l'ordinateur d'une autre personne ou même celui de la bibliothèque du coin.

Pour plus d'informations, consultez la page « Fonctionnement de Tails » [https://tails.boum.org/about/index.fr.html].

page 22 **Inconvénients** Tout d'abord, Tails étant un système d'exploitation à part entière, il faut redémarrer l'ordinateur pour l'utiliser[7]. Il est aussi plus complexe à installer

3. Dans notre cas, il s'agit de Debian, mais le Navigateur Tor fonctionne aussi avec n'importe quelle autre distribution GNU/Linux, tout comme avec Windows ou macOS.

4. Il est possible de configurer un navigateur web pour qu'il utilise Tor, mais ce n'est pas conseillé car même avec de bonnes connaissances techniques il est difficile de s'assurer que toutes les requêtes du navigateur passeront bien par Tor. Le Navigateur Tor existe notamment pour pallier cette difficulté.

5. Il est possible de modifier ce comportement en modifiant les réglages par défaut de Tor, réglages qui visent à rendre la navigation presque amnésique.

6. Voir le site de Tails [https://tails.boum.org/index.fr.html].

7. On peut aussi utiliser Tails dans une machine virtuelle [page 163] dans le système habituel. Dans ce cas, la mémoire de la machine virtuelle sera visible pour celui-ci, et toutes les données, mots de passe compris, seront à la portée d'une faille de programmation ou d'un éventuel logiciel malveillant. De plus, si le système d'exploitation utilise de la mémoire virtuelle (*swap*) [page 25], il est possible que des données de la machine virtuelle finissent par être écrites sur le disque dur. L'amnésie du système Tails utilisé de cette façon est donc quasiment impossible à garantir.

que le Navigateur Tor. Enfin, il est nécessaire d'avoir sur soi une clé USB (d'une capacité d'au moins 8 Go) ou bien un DVD, contenant Tails.

Ensuite, du fait de l'amnésie du système, si jamais le navigateur web vient à planter, on perd toutes les pages que nous étions en train de consulter, tout comme dans le cas du Navigateur Tor.

Pour ne pas mélanger ses activités quotidiennes normales avec celles que l'on souhaite plus discrètes lorsqu'on utilise Tails, il est nécessaire de redémarrer sa machine quand on passe d'une identité contextuelle à une autre.

Au chapitre des inconvénients inhérents à Tails, il y a aussi le délai entre les mises à jour de sécurité de programmes par ailleurs inclus dans Tails, et les mêmes mises à jour de ces mêmes logiciels dans Tails. Cet inconvénient est similaire à celui du Navigateur Tor concernant le délai entre les mises à jour de Firefox et leur prise en compte dans le Navigateur Tor.

Pour plus d'informations, se reporter à la page « Avertissements » de Tails [https://tails.boum.org/doc/about/warnings/index.fr.html].

33.4.2 Faire son choix

On doit donc, en fin de compte, faire son choix entre :

- utiliser son système d'exploitation habituel ;
- utiliser un système *live* amnésique.

En d'autres termes, quelles traces (éventuellement chiffrées) est-on prête à laisser sur l'ordinateur ou la clé USB utilisées ? A-t-on besoin du reste de son environnement lors de la navigation anonyme ?

Encore une fois, il n'y a pas de bonne ou de mauvaise réponse : il s'agit de choisir la solution qui nous convient le mieux. De plus, il est tout à fait possible de tester une solution puis de passer à une autre si nécessaire.

Au final, les deux possibilités suivantes s'offrent à nous :

- utiliser le Navigateur Tor depuis une Debian chiffrée. Cela permet de naviguer de manière presque anonyme tout en utilisant son système habituel. Par contre, des traces (chiffrées) seront probablement laissées sur le disque dur de l'ordinateur. page 119
- utiliser le navigateur web de Tails. On ne laisse pas de traces sur le disque dur de l'ordinateur utilisé, voire pas de traces du tout si l'on n'utilise pas la persistance. page 116

Une fois notre choix fait, on peut consulter ci-dessous le paragraphe correspondant.

33.5 Naviguer sur des sites web avec le Navigateur Tor

Si, après avoir pesé le pour et le contre, on décide d'utiliser le *Navigateur Tor*, certaines précautions sont bonnes à prendre.

33.5.1 Préparer sa machine et installer le Navigateur Tor

Tout d'abord, comme nous n'utilisons pas un système *live*, des traces de navigation (marque-pages, fichiers téléchargés, voire parfois cookies ou historique) seront inscrites sur notre disque dur. Appliquer la même politique que pour un nouveau départ est une bonne piste. page 71 Ensuite, il faut télécharger et installer le Navigateur Tor. Le chapitre installer le Navigateur Tor décrit cette procédure. page 313

33.5.2 Utiliser le Navigateur Tor

page 313

Dans le chapitre concernant l'installation du Navigateur Tor, il est également expliqué comment le démarrer. Cet outil est spécialement conçu pour être le plus simple possible à utiliser. Au moment de son lancement, tous les logiciels dont nous avons besoin (Tor et le Navigateur Tor) démarreront et seront paramétrés. Il suffira donc d'attendre que la fenêtre du Navigateur Tor s'ouvre et nous pourrons commencer la navigation *via* le réseau Tor.

page 261

Attention : seule la consultation de sites web *via* la fenêtre du Navigateur Tor garantit une connexion confidentielle. Toutes vos autres applications (client mail, messagerie instantanée, Torrent, *etc.*) laisseront apparaître votre véritable adresse IP.

page 202

De plus, une fois cette fenêtre fermée, il vous faudra relancer le Navigateur Tor et attendre qu'une nouvelle fenêtre s'ouvre pour reprendre une navigation passant par le réseau Tor.

33.5.3 On perçoit vite les limites

Le Navigateur Tor est un très bon outil de par son utilisation simplifiée, mais on en perçoit vite les limites. En effet, seules les connexions initiées par le Navigateur Tor passent par le réseau Tor. Si l'on veut utiliser un autre navigateur web, la connexion ne passera alors plus par ce réseau, ce qui peut être fâcheux. En cas d'inattention on peut vite se tromper de navigateur et penser que notre navigation passe par le réseau Tor alors que ce n'est pas le cas. De plus, il ne permet d'utiliser Tor que pour naviguer sur le web, ce qui, même si c'est énormément utilisé, n'est qu'une partie d'Internet comme expliqué auparavant.

page 200

Ajoutons à cela que la confidentialité en ligne ne tient pas seulement à la falsification de l'adresse IP. Toutes les autres traces que nous laissons sur le web et sur notre ordinateur peuvent nous trahir un jour ou l'autre, et le Navigateur Tor ne protège pas contre cela.

33.6 Naviguer sur des sites web avec Tails

33.6.1 Obtenir et installer Tails

page 39

Tails est un logiciel libre et peut donc être téléchargé, utilisé et partagé sans restriction. Il fonctionne sur un ordinateur indépendamment du système déjà installé. En effet, Tails se lance sans utiliser le disque dur, depuis un support externe : un DVD ou une clé USB.

Il nous faut d'abord télécharger Tails (voir page 114). Afin de s'assurer que le téléchargement s'est bien déroulé, on doit ensuite vérifier l'image ISO du fichier (voir page 114).

Une fois la vérification effectuée, on peut procéder à l'installation sur une clé USB ou un DVD (voir page 115).

33.6.2 Démarrer Tails

Maintenant que l'on a installé Tails et redémarré (voir page 115), on peut commencer à l'utiliser sans altérer le système d'exploitation présent sur l'ordinateur.

33.6.3 Se connecter à Internet

Une fois le démarrage de Tails achevé, c'est-à-dire lorsque le bureau a terminé de s'afficher, il ne nous reste plus qu'à nous connecter à Internet : voir la documentation de Tails sur comment « Se connecter à un réseau local » [https://tails.boum.org/doc/anonymous_internet/networkmanager/index.fr.html]. On peut alors naviguer sur le web.

33.6.4 Limites

Une telle solution repose sur l'utilisation de Tor et de Tails, et hérite donc des limites de ces deux outils :

Concernant les limites de Tor, elles ont été évoquées précédemment dans le paragraphe « Troisième étape : attaquer Tor ». page 279

Pour les limites de Tails, vous trouverez une liste approfondie d'avertissements sur le site web du projet [https://tails.boum.org/doc/about/warnings/index.fr.html].

Nous ne pouvons que vous inviter à lire attentivement ces deux documents.

Chapitre 34

Cas d'usage : publier un document

34.1 Contexte

Après avoir terminé la rédaction d'un document sensible, on souhaite le publier sur Internet tout en conservant notre anonymat (le fait qu'il ne puisse être associé à aucun nom) ou notre pseudonymat (le fait qu'il ne puisse être associé qu'à un nom choisi et différent de notre identité civile).

page 79

En prime, on voudrait pouvoir y inclure une adresse de contact public correspondant à ce pseudonyme.

34.2 Évaluer les risques

34.2.1 Que veut-on protéger ?

Le contenu du document est public. On ne s'intéresse donc pas à sa confidentialité. Par contre, on cherche à cacher les liens entre le document et les personnes qui l'ont rédigé. C'est donc ici l'**anonymat** ou le **pseudonymat** qui nous intéresse.

De plus, si nous rendons public un document sensible dont la simple consultation pourrait être retenue à charge, nous devons aussi chercher à limiter la possibilité d'identifier des personnes qui y accèderaient.

34.2.2 Contre qui veut-on se protéger ?

Comme dans le cas d'usage précédent, nous chercherons ici à nous protéger des regards indiscrets qui chercheraient à savoir *qui* fait *quoi* sur le web.

page 277

On fera d'autant plus attention aux traces laissées qu'il s'agit justement ici de publier un document dont on suppose qu'il peut déplaire à une ou plusieurs personnes ayant un certain pouvoir de nuisance. Il est alors probable que débute une recherche d'indices pour tenter de retrouver la ou les personnes ayant réalisé le document (ou bien celles l'ayant consulté), par exemple en adressant des demandes à l'hébergeur.

page 228

page 209

34.3 Définir une politique de sécurité

Nous allons traiter successivement la publication et la consultation de documents, puis enfin l'utilisation d'un contact public lié à ceux-ci.

34.3.1 Publication

Publier un document revient techniquement à « sauvegarder » celui-ci sur un serveur connecté à Internet, que l'on appelle l'*hébergeur*. On passe souvent par un site web pour réaliser cette opération. Cependant, on ne va pas utiliser les mêmes sites si l'on veut publier du texte, du son ou de la vidéo.

page 209

page 211

Il s'agit donc de bien choisir notre hébergeur en ayant à l'esprit les nombreux critères entrant en jeu : type de document, disponibilité, conditions d'hébergement, résistance de l'hébergeur aux pressions judiciaires, risques que notre document fait courir à celui-ci, possiblité de consulter le document sans risque d'identification, *etc.* Une liste plus exhaustive de ces critères est disponible dans la partie « Outils ».

page 319

Une fois notre choix effectué, il va falloir être sûres que notre document reste consultable : en effet, si notre publication ne plaît pas à notre hébergeur, qu'il reçoit des pressions, voire une demande exigeant sa suppression, notre œuvre pourrait devenir indisponible.

Pour éviter ce genre de désagréments, on peut multiplier les hébergements d'un même fichier, si possible sur des serveurs situés dans différents pays. La mise en ligne d'un fichier étant beaucoup plus rapide qu'un recours judiciaire, cela semble être une bonne solution pour éviter la censure.

Quels seront alors les angles d'attaque à la portée d'une éventuelle adversaire ?

Première étape : lire le document

L'adversaire dispose de prime abord d'un gros volume de données au sein duquel chercher des traces : le contenu du document.

Ainsi, une éventuelle signature comme un pseudonyme ou une ville, une date, la langue dans laquelle le document est écrit, voire tout simplement le thème du document sont autant d'indices qui peuvent mener à ses autrices. Un texte qui décrit les pratiques abusives de la société Machinex en novembre 2012 a probablement été rédigé par des employées de cette société ou par des gens qui partageaient leur lutte à cette date.

page 245

L'adversaire peut aussi tenter une analyse stylométrique pour le comparer à d'autres textes, anonymes ou non, et essayer d'en déduire des informations sur les autrices. À notre connaissance, ce type d'attaque n'est réellement effective que lorsqu'on a déjà de forts soupçons sur un sous-ensemble d'autrices potentielles, mais c'est un champ de recherche récent. Vu que l'on souhaite diffuser largement ce document, on ne pourra pas masquer le contenu. Cependant, si l'on pense nécessaire de s'en donner la peine, on pourra avoir une attention particulière à changer son style d'écriture.

page 30

Enfin, si l'on publie notre document sans prendre de plus amples précautions, l'adversaire peut chercher d'éventuelles métadonnées qui lui fourniraient quelques informations.

Ces différentes méthodes ne demandent pas de grandes compétences techniques et sont donc à la portée de beaucoup d'adversaires.

Pour s'en protéger, on suivra les recettes suivantes :

page 79

- si possible, on travaillera sur notre document en utilisant dès le début des méthodes limitant les métadonnées qui pourront être enregistrées ;

page 185

- dans tous les cas, il est bon de supprimer d'éventuelles métadonnées avant publication.

Deuxième étape : demander à celles qui voient

En l'absence de traces facilement exploitables à l'intérieur du document, l'un des angles d'attaque le plus praticable est alors de chercher les traces de la publication sur le réseau.

page 228

Selon ses pouvoirs, notre adversaire peut effectuer une réquisition auprès de l'hébergeur du contenu ou trouver une autre façon de se procurer ses journaux de connexion

page 225

et ainsi obtenir l'adresse IP utilisée. Elle peut ensuite se tourner vers le FAI correspondant à cette adresse IP pour avoir le nom de l'abonnée.

page 226

Ici aussi, pour faire face, on utilisera Tor pour se connecter à Internet en brouillant cette piste avant de publier notre document.

Quant au choix de l'hébergement, les questions discutées ci-dessus s'appliquent toujours. De plus, certaines des plateformes sur lesquelles on voudrait déposer notre document sont susceptibles de ne pas fonctionner si Tor est utilisé, ou, comme Facebook, d'imposer des vérifications d'identité difficiles à contourner et incompatibles avec notre besoin d'anonymat : cela restreindra les hébergeurs utilisables.

Pour publier notre document sur un serveur web *conventionnel*, on commencera en pratique par suivre la recette pour trouver un hébergement web. page 319

Dans la plupart des cas, la publication se fera grâce à un navigateur web. On suivra donc la piste « navigateur web » du cas d'usage précédent. page 281

Il est aussi possible d'héberger nous-mêmes notre document grâce aux *services onion* de Tor : ils permettent de rendre disponible un serveur web ou un autre type de serveur sans avoir à révéler son adresse IP. Ils n'utilisent pas d'adresse publique et peuvent donc fonctionner aisément même derrière un pare-feu ou une autre « box » faisant de la traduction d'adresse réseau (NAT). page 266 page 203 page 205

Si l'on préfère héberger notre document sur un service onion, il faudra suivre la recette détaillant comment utiliser OnionShare. page 359

Troisième étape : regarder sur l'ordinateur utilisé

Cet angle d'attaque est similaire à celui décrit dans la section « regarder sur l'ordinateur utilisé » du cas d'usage précédent. Retournons donc lire (ou relire) ce chapitre pour réviser tout cela. page 279

Quatrième étape : attaquer Tor

En désespoir de cause, l'adversaire peut aussi tenter d'attaquer Tor (voir la section « attaquer Tor » du cas d'usage précédent). page 279

34.3.2 Consultation du document

Parmi les critères à prendre en compte lors du choix de l'hébergeur se trouvent aussi les risques que nous faisons prendre aux personnes qui viendraient consulter notre document. On privilégiera ainsi des hébergeurs qui permettent de limiter la possibilité qu'une éventuelle adversaire puisse identifier ces personnes.

Les moyens d'attaque que l'adversaire peut mettre en œuvre sont ceux déjà couverts dans le cas d'usage précédent. Reprenons-les brièvement ici pour les adapter au cas de la consultation d'un document. page 278

Première étape : demander à celles qui voient

Comme vu dans le cas d'usage précédent, une personne qui viendrait consulter notre document pourra être identifiée par son fournisseur d'accès à Internet ou par l'hébergeur, car l'accès au document apparaîtra dans leurs journaux de connexion. page 226

Afin de réduire ce risque, nous pouvons donc conseiller aux personnes qui souhaiteraient accéder au document d'utiliser le réseau Tor pour cela. Il nous faudra aussi nous assurer que l'hébergeur retenu est bien accessible par Tor, voire qu'il offre la possibilité d'y accéder par un service onion. page 261 page 266

Il est aussi important de choisir un hébergeur qui ne soit pas une plateforme sur laquelle des personnes risqueraient d'être déjà authentifiées et seraient donc « reconnues » par l'hébergeur lorsqu'elles accéderaient au document, quand bien même elles utiliseraient Tor. Ainsi, les médias sociaux ou les plateformes d'hébergement de contenu des géants du web 2.0 sont à proscrire, par exemple. page 239

Enfin, nous pouvons aussi privilégier des hébergeurs qui ne conservent pas les journaux de connexion, ou bien qui refuseront de les donner aux flics en cas de réquisition.

page 228

Deuxième étape : regarder sur l'ordinateur utilisé

Face à ce cas de figure, nous n'avons nous-mêmes que peu de prise. Nous pouvons cependant conseiller aux personnes souhaitant consulter notre document de suivre les recommandations du cas d'usage précédent de ce guide afin de laisser le moins de traces possibles sur leur ordinateur.

page 278

Troisième étape : attaquer Tor

Tout comme lors de la publication du document, l'adversaire peut aussi tenter d'attaquer Tor pour chercher à identifier les personnes qui le consulteraient (voir la section « attaquer Tor » du cas d'usage précédent).

page 279

34.3.3 Contact public

Lorsqu'on publie un document, on peut vouloir que les personnes qui vont nous lire puissent nous contacter. Ce contact ouvre de nouvelles possibilités d'attaques à notre adversaire en quête de failles à exploiter.

Si l'on a pris toutes les précautions afin d'être aussi anonyme que possible lors de la publication du document, mais que notre adresse de contact est nom.prenom@exemple.org, ces précautions seront sans intérêt : l'adresse de contact donne directement notre nom à l'adversaire.

Pour éviter cette erreur, on veillera donc à avoir un pseudonyme qui sera utilisé uniquement pour ce document — ou pour un groupe de documents — en fonction de l'identité contextuelle que l'on souhaite adopter.

page 243
page 244

L'adversaire cherchera alors à savoir qui se cache derrière ce pseudonyme. Pour tenter de masquer « qui utilise cette adresse mail », le cas d'usage « Échanger des emails en cachant son identité » pourra nous aider.

page 293

Enfin, on pourrait avoir envie de cacher le contenu des emails échangés, mais ceci peut apparaître très complexe : dans la mesure où l'on souhaite avoir une adresse de contact public, l'*accessibilité* peut rentrer en conflit avec la discrétion. Néanmoins, il reste toujours possible d'indiquer, en plus de l'adresse mail de contact, une clé publique OpenPGP associée afin de laisser la possibilité aux personnes qui le souhaiteraient de nous envoyer des messages chiffrés. Les recettes pour créer une paire de clés OpenPGP et pour exporter sa clé publique indiquent comment mettre cela en œuvre.

page 295
page 333
page 339

On peut ainsi prendre tout un ensemble de précautions pour augmenter l'anonymat de notre contact, mais l'on peut difficilement agir sur l'autre « bout du tuyau ». Les personnes qui vont nous contacter peuvent alors prendre des risques en dialoguant avec nous, sans penser à leur anonymat. Rappeler et expliciter les conditions de confidentialité et d'anonymat est alors indispensable. De plus, on ne sait jamais vraiment qui nous contacte, il faudra alors faire attention à ce que l'on raconte si l'on ne veut pas se compromettre.

Chapitre 35

Cas d'usage : échanger des messages

35.1 Contexte

On souhaite maintenant échanger des messages avec d'autres personnes, que ce soit pour souhaiter une bonne année à mamie, ou pour travailler sur un document sensible. On ne se soucie pas de la synchronicité de l'échange, à l'inverse d'une conversation téléphonique ou d'un dialogue en messagerie instantanée : on parle dans ce cas de communication *asynchrone*.

page 79

Un autre cas d'usage sera consacré au dialogue synchrone. Concentrons-nous plutôt, pour l'instant, sur le courrier électronique, ou email.

page 299

35.2 Évaluer les risques

35.2.1 Que veut-on protéger ?

Lorsqu'un courrier électronique est envoyé, diverses informations sont potentiellement dévoilées à nos adversaires. Lesquelles ?

Quand on se pose cette question, c'est bien souvent le *contenu* du message qui vient à l'esprit en premier lieu. Si tous les messages que nous échangeons ne sont pas nécessairement top-secrets, certains méritent plus de discrétion que d'autres : afin d'éviter que les détails de nos relations intimes soient étalés, ou encore car le contenu d'un message peut nous attirer des ennuis, allant de la perte d'un boulot à un séjour en prison. Plus généralement, nous ne débordons pas d'enthousiasme à l'idée que la factrice puisse lire aujourd'hui toutes les lettres qu'on a reçues ces dernières années, pour se mettre en bouche, avant d'attendre avidement celles qui arriveront demain. Pourtant, lorsqu'on échange du courrier électronique sans précautions particulières, les intermédiaires peuvent lire nos communications de façon totalement transparente, comme s'il s'agissait de cartes postales.

Au-delà du contenu de ces cartes postales, il peut être intéressant de masquer les informations contextuelles, telles que la date de l'échange, les identités des protagonistes, leurs localisations, *etc.*, qui peuvent être révélées par exemple dans les en-têtes HTTP, les en-têtes des emails, ou dans le corps du message lui-même.

page 217
page 218

Le fait qu'une certaine personne écrive à telle autre peut constituer en soi une information sensible. En effet, il arrive que les relations entre des gens soient visées par certaines formes de surveillance, afin de reconstituer un réseau d'opposants politiques [1] par exemple. Ces traces persisteront généralement dans les en-têtes des emails et les journaux de connexion.

page 219
page 218
page 224

1. Jean-Marc Manach, 2011, *Réfugiés sur écoute* [https://web.archive.org/web/20221019100157/http://owni.fr/2011/12/01/amesys-bull-eagle-surveillance-dpi-libye-wikileaks-spyfiles-kadhafi/index.html].

35.2.2 Contre qui veut-on se protéger ?

On peut vouloir dissimuler tout ou partie de ces informations aux diverses machines qui peuvent y avoir accès, ainsi qu'aux personnes ayant accès à ces machines.

page 217

Parmi ces machines, viennent tout d'abord les serveurs impliqués. Au minimum, pour un message envoyé par Ana (*ana@exemple.org*) à Bea (*bea@fai.net*), il s'agira :

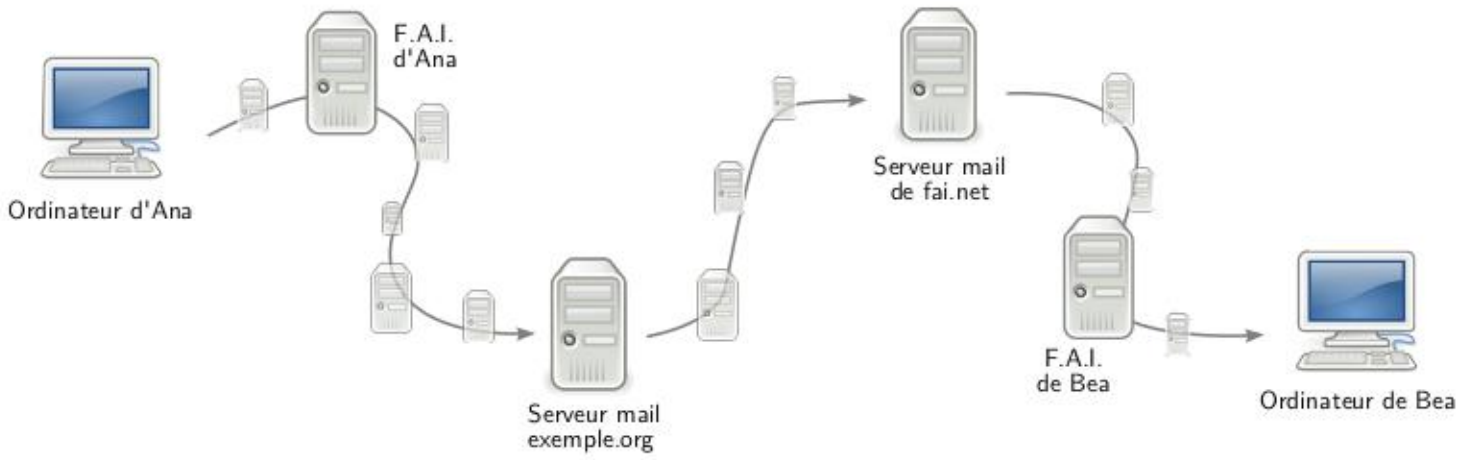
- du serveur chargé par Ana d'envoyer le message : généralement, ce sera *exemple.org* ;
- du serveur chargé de recevoir un message et de le stocker dans la boîte mail de Bea : *fai.net*.

page 205

Mais ce n'est pas tout. De nombreux autres ordinateurs (les *routeurs*) sont situés le long du trajet, et ont accès à l'information qu'ils transportent :

page 217

- entre l'ordinateur d'Ana et son FAI ;
- entre le FAI d'Ana et son serveur mail *exemple.org* ;
- entre *exemple.org* et le serveur mail de Bea *fai.net* ;
- lorsque Bea consultera sa boîte mail, le message cheminera entre le serveur mail *fai.net* et son FAI,
- enfin, entre le FAI de Bea et son ordinateur.



Un email transite par de nombreux intermédiaires

Les personnes administrant ces machines sont les premières à avoir accès aux informations que celles-ci traitent, mais n'en ont pas forcément l'exclusivité. Ces informations peuvent se retrouver aux mains de pirates plus ou moins gouvernementaux, munis ou non de réquisitions.

page 235

page 228

Pour finir, chaque consultation d'une boîte mail, chaque envoi de message, est susceptible de laisser des traces sur l'ordinateur utilisé. Il peut être pertinent de dissimuler celles-ci aux personnes qui seraient en mesure de jeter un œil au contenu de nos disques durs.

page 27

35.3 Deux problématiques

On peut avoir comme souci de protéger à la fois notre identité — voire celles de nos destinataires — et le contenu des échanges. Il s'agit donc des informations contenues dans les deux parties de notre carte postale numérique, à gauche le texte, à droite les en-têtes. Ces informations apparaissent tout au long du parcours de nos messages et peuvent être la cible d'attaques. La politique de sécurité que l'on va définir va notamment dépendre de la façon dont nous consultons nos emails. En effet, son utilisation peut impliquer divers protocoles qui n'ont pas les mêmes conséquences en termes de traces.

page 200

35.4 Webmail ou client mail ?

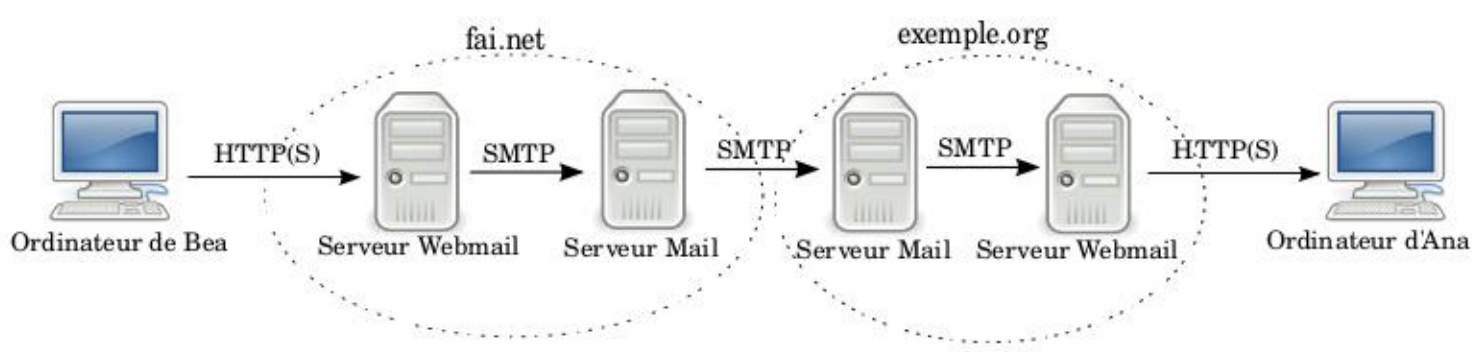
Il existe deux manières d'utiliser l'email, permettant les mêmes actions : l'utilisation du webmail ou d'un client mail. Ce choix repose sur différents critères, sachant que

les deux sont utilisables pour une même adresse mail, et que le choix de l'un ou de l'autre n'est pas irréversible.

35.5 Webmail

Un **webmail** est un site web permettant de consulter ses emails *via* un navigateur web. Son usage s'est répandu comme une traînée de poudre depuis le début des années 2000, à tel point qu'on en aurait presque oublié les autres manières de faire de l'email. Hotmail et Gmail sont des exemples très populaires d'hébergeurs qui favorisent son utilisation (même s'ils ne sont pas utilisables qu'en webmail). Ici encore, on a affaire à une tendance du web 2.0, plus besoin d'avoir son système d'exploitation pour accéder à sa boîte mail (que ce soit sur son ordinateur ou sur la clé USB contenant un système *live*) : un accès à Internet suffit.

page 239



Bea envoie un email à Ana, toutes deux utilisent un webmail

Le webmail c'est en fin de compte une interface web qui nous permet d'agir sur des serveurs mails. Schématisons un échange d'email entre Ana et Bea, qui utilisent toutes deux le webmail :

- le « chemin réseau » entre l'ordinateur de Bea et sa boîte mail hébergée par *fai.net* sera parcouru *via* un protocole web (HTTP ou HTTPS)
- s'ensuivra un petit bout de chemin chez *fai.net* qui assurera le passage du webmail à l'email
- suivi d'un voyage en protocole mail (SMTP) entre *fai.net* et *exemple.org*
- de nouveau un petit bout de chemin, chez *exemple.org* cette fois-ci, entre protocole mail et web
- puis du web (HTTP ou HTTPS) jusqu'à l'ordinateur d'Ana.

35.5.1 Avantages

Parmi les avantages du webmail, de même que pour chaque application web, on peut noter l'absence d'installation, de mise à jour, de configuration, pour le logiciel de mail. On y retrouve également un argument phare du web 2.0 : la possibilité d'accéder à sa boîte mail depuis n'importe quel ordinateur connecté à Internet, n'importe quand, n'importe où.

Dans le cas où l'on utilise un système *live* et que l'on ne chiffre pas ses emails, ceci a pour avantage de ne pas laisser de traces sur le disque.

35.5.2 Inconvénients

Côté inconvénients, il y a le fait qu'en cas d'absence de connexion, toute notre correspondance nous est inaccessible (à moins qu'on en ait sauvegardé tout ou partie sur un support à portée de main : clé USB, disque dur, *etc.*).

page 151

Le fait qu'il soit possible d'utiliser n'importe quel navigateur web pour accéder à notre boîte mail peut vite nous inciter à utiliser effectivement *n'importe quel* navigateur web, et par là des ordinateurs en lesquels nous n'avons que très peu de raisons de placer notre confiance.

Ensuite, en fonction de la confiance que l'on place dans notre hébergeur mail, il convient de se poser la question de la centralisation de nos données. L'usage massif du webmail nous amène à une situation où des milliers de boîtes mail, avec tout leur contenu, se retrouvent entre les mains des plus gros fournisseurs de service mail, leur confiant ainsi la garde d'une montagne de données personnelles. Ces hébergeurs peuvent les utiliser à des fins commerciales, les livrer à diverses autorités, ou tout simplement les perdre. De plus, si l'on considère que notre correspondance est sensible d'une manière ou d'une autre, peut-être préfèrera-t-on ne pas la laisser reposer sur les épaules de personnes - car il y en a encore derrière les machines - qui n'ont pas particulièrement envie d'en porter la responsabilité. Tel fut probablement le cas courant août 2013 pour la société d'hébergement mail Lavabit [2], qui hébergeait un compte mail d'Edward Snowden et qui décida de stopper ses activités. Fermeture intervenue suite aux requêtes voire pressions de la part d'agences gouvernementales telles que la NSA ou le FBI.

Enfin, l'utilisation du webmail peut nous faire profiter pleinement d'un tas de publicités s'affichant dans notre navigateur web, lors de la consultation de notre boîte aux lettres informatique. Publicités qui peuvent d'ailleurs être choisies en fonction du contenu de nos emails.

page 221

35.6 Client mail

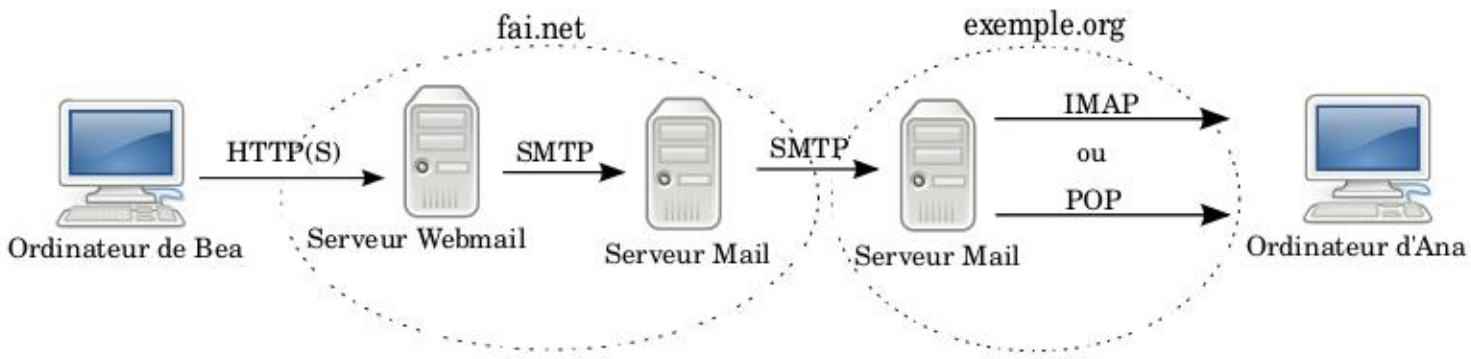
Un client mail ou client de messagerie est un logiciel qui sert à gérer ses emails : les recevoir, les lire, les envoyer, *etc.* Des clients mails connus sont par exemple Outlook de Microsoft ou Thunderbird de Mozilla. Il en existe de nombreux autres qui, malgré leurs différences, possèdent une interface globalement similaire, proche de celle des webmails.

Contrairement au webmail, où l'on va consulter ses emails stockés chez l'hébergeur en utilisant son navigateur web, ici la lecture des emails se fait grâce à un logiciel installé sur l'ordinateur. On se sert d'un périphérique de stockage local (disque dur de l'ordinateur utilisé, clé USB, *etc.*) comme espace de stockage des emails.

Pour reprendre notre petit schéma précédent, il faut remplacer les protocoles web par des protocoles mail. Deux protocoles différents existent afin de recevoir son courrier, *IMAP* (pour *Internet Message Access Protocol*) et *POP* (pour *Post Office Protocol*).

Le premier, IMAP, permet de manipuler les emails stockés sur les serveurs mail de notre hébergeur. À chaque connexion vers la boîte mail, une synchronisation a lieu afin d'avoir le même état (nombres d'emails, de brouillons, de dossiers, *etc.*) sur le serveur mail que sur notre client mail, et inversement. Et cela sans pour autant télécharger le contenu présent sur le serveur mail. Seule la liste des emails et leurs en-têtes peuvent être rapatriés sur notre client mail par exemple.

Le second protocole, POP, téléchargera les différents contenus de la boîte mail directement sur notre client mail, sans forcément en laisser de copie sur le serveur distant.



Bea envoie un email à Ana, Bea utilise un webmail, Ana un client mail

2. Wikipédia, 2014, *Lavabit* [https://fr.wikipedia.org/wiki/Lavabit].

35.6.1 Avantages

Les avantages et inconvénients peuvent être spécifiques au protocole utilisé afin de recevoir son courrier, cela dit certains leur sont communs.

Il est possible avec un client mail de retrouver sa boîte mail dans le même état qu'au dernier relevé de courrier, même en l'absence de connexion à Internet. Il sera donc possible de lire, rédiger ou supprimer des emails hors connexion. Et de les envoyer ou d'en recevoir à nouveau lorsque l'on retrouve une connexion. De plus, l'usage d'un client mail nous évite d'avoir à subir la myriade de publicités dont le web est parsemé.

En utilisant le protocole POP, on profitera d'autres avantages comme la décentralisation des emails. Au lieu de laisser toute notre correspondance sur des serveurs distants, les courriers électroniques sont rapatriés sur l'ordinateur. Cela évite de laisser indéfiniment tous nos emails aux hébergeurs d'emails majeurs, mais aussi de dévorer trop d'espace disque chez les petits hébergeurs d'emails. Le fait que les emails finissent leur course sur le système du destinataire permet également plus de prise sur leur gestion : concernant la suppression effective d'emails qui pourraient s'avérer être critiques par exemple. Enfin, on laisse moins de données à des entreprises qui n'ont que faire de la confidentialité de la correspondance. Attention cependant : l'hébergeur pourra tout de même faire une copie de l'email avant qu'il soit rapatrié dans le client mail.

35.6.2 Inconvénients

Pour utiliser un client mail, il va falloir le configurer pour qu'il sache quelle boîte relever, à quel serveur se connecter et quel protocole utiliser.

Il est plus compliqué de consulter de cette manière ses emails depuis un ordinateur qui n'est pas le nôtre (chez des amies ou au travail par exemple), à moins d'utiliser le client mail d'un système *live* persistant (comme celui de Tails), installé sur une clé USB.

De plus, dans le cas où le client mail est configuré pour ne pas laisser notre correspondance sur le serveur, celle-ci ne sera plus que sur le support de stockage de notre client mail. En cas de perte de celui-ci (que ce soit le disque dur d'un ordinateur ou la clé USB sur laquelle on a installé un système live Tails persistant), on peut dire adieu à nos précieux messages… sauf si on en a fait une sauvegarde. page 151

35.7 Échanger des emails en cachant son identité

L'objectif sera ici de cacher à une adversaire que nous sommes l'une des correspondantes d'un échange d'emails. Il s'agit peut-être d'un échange d'emails avec une dissidente politique recherchée ou bien avec une amie perdue de vue.

35.7.1 Définir une politique de sécurité

Notre souci principal va être de masquer les noms des personnes échangeant par mail, ou du moins de rendre leur identification aussi difficile que possible. Que ferait une adversaire pour les retrouver ?

Première étape : demander aux factrices

Notre fournisseur mail est un nœud du réseau par lequel transitera obligatoirement notre correspondance numérique. Une adversaire s'y intéressant aurait donc de bonnes raisons de jeter un coup d'œil à cet endroit, d'autant plus que cela peut lui être très aisé.

De la même manière, les intermédiaires entre Bea et Ana (dont leurs FAI respectifs) voient passer les en-têtes mail, qui peuvent livrer nombre d'informations (notamment, chez certains hébergeurs, les adresses IP des correspondantes). Une telle attaque est page 218

plus que probable si le contenu des emails ou les protagonistes des échanges attirent l'attention d'autorités ayant des pouvoirs suffisants. Il est juste de se dire qu'en premier lieu, ne pas avoir une adresse mail du genre *nom.prenom@exemple.org* est déjà un bon réflexe. Il va tout d'abord falloir penser à utiliser un pseudonyme, pour mettre sur pied une identité contextuelle.

page 243

Ceci dit, si « Kiwi Poilu » écrit régulièrement à Caroline Carot, Sofiane Carot et Francine Carot, une adversaire *pourrait* se dire qu'elle appartient à la famille Carot, ou fait partie des intimes : les identités des gens à qui on écrit sont elles aussi révélatrices.

De plus, si l'on utilise un pseudonyme, mais qu'une adversaire observe que les emails qu'elle surveille sortent de telle maison ou tel appartement, elle peut effectuer le rapprochement. C'est pourquoi comme pour la navigation sur le web, l'utilisation du routage en oignon ou l'utilisation d'un système *live* amnésique prévu à cet effet permettent de brouiller des pistes remontant jusqu'à notre ordinateur.

page 261

page 113

Enfin, le contenu des échanges peut permettre d'en apprendre suffisamment sur leurs autrices pour mettre des noms dessus. Cacher une identité nécessite donc de faire attention non seulement aux en-têtes, mais aussi au contenu de l'email.

Pour protéger le contenu des emails des regards curieux, que ce soit pour lui-même ou pour ce qu'il peut divulguer sur les autrices des emails, on utilisera le chiffrement d'emails.

page ci-contre

Deuxième étape : regarder sur l'ordinateur utilisé

Si le réseau Tor ainsi qu'un pseudonyme sont utilisés afin de protéger son identité, une attaquante potentielle peut essayer d'accéder aux traces laissées sur l'ordinateur afin de prouver que la personne qu'elle suspecte est bien en possession du compte mail en question.

page 27

Pour se prémunir contre cette attaque, il est nécessaire de chiffrer son disque dur ou d'utiliser un système *live* amnésique.

page 119

page 113

C'est d'autant plus important si l'on utilise un client mail, car ce ne sont pas seulement des traces qui seraient laissées sur le système, mais également les emails eux-mêmes.

Troisième étape : attaquer Tor

Une attaquante capable de surveiller plusieurs points du réseau, par exemple la connexion utilisée *et* l'hébergeur mail, pourrait être en mesure de défaire l'anonymat fourni par le réseau Tor.

Rappelons encore une fois que de nombreuses autres attaques sont envisageables contre le réseau Tor, et qu'il est impératif de bien saisir contre quoi il protège et contre quoi il ne protège pas.

page 261

page 267

35.7.2 Choisir parmi les outils disponibles

Plusieurs outils sont disponibles pour communiquer par mail, le choix se fait donc en fonction des différents critères évoqués précédemment. On peut par exemple préférer ne pas laisser ses emails sur le serveur de notre hébergeur, les lire et y répondre hors ligne ou au contraire ne pas vouloir télécharger de copie de ses emails et y accéder toujours en ligne.

35.7.3 Webmail

Le webmail étant un usage particulier du web, on se réfèrera pour les questions relatives au Navigateur Tor ou à Tails — leurs avantages, leurs inconvénients, leur utilisation — au cas d'usage traitant de la navigation sur le web (voir page 277). Les certificats ou autorités de certification utilisés pour le chiffrement de la connexion

vers le serveur de mail devront être authentiques, car un attaquant ayant les moyens de duper l'utilisateur à cet endroit-là sera en mesure de récupérer en clair tous les échanges avec le serveur de mail, dont login et mot de passe de la boîte mail. Il faudra donc prendre soin de les vérifier (voir page 323).

De plus, si l'on utilise le webmail depuis Tails sur un ordinateur douteux, notamment face à une attaque de type keylogger, on prendra soin d'utiliser un clavier visuel (aussi appelé « clavier virtuel ») lors de la saisie du mot de passe de son compte mail.

page 35
page 327

35.7.4 Client mail

Dans le cas où l'on préfère utiliser un client mail plutôt que faire du webmail, on peut au choix :

- Utiliser Tails (voir page 113), et suivre l'outil configurer et utiliser Thunderbird (voir page 329). Les traces laissées localement seront alors effacées à l'extinction du système.
- Utiliser Tails et Thunderbird en configurant la persistance (voir page 116), puis suivre l'outil configurer et utiliser Thunderbird (voir page 329). Le contenu de sa boîte mail sera stocké sur une clé USB, qui contiendra donc des traces chiffrées.
- Installer un client mail sur son système chiffré (voir page 119). Pour cela, installer le paquet `thunderbird-l10n-fr`[3] en suivant la recette installer un logiciel (voir page 135), puis suivre l'outil configurer et utiliser Thunderbird (voir page 329). Des traces seront alors laissées sur le disque dur chiffré de l'ordinateur.

Mais de la même manière que pour un webmail, il faudra veiller à vérifier les certificats ou autorités de certification qui offrent un chiffrement de la connexion vers le serveur de mail.

page 323

35.8 Échanger des emails confidentiels

On souhaite ici cacher le contenu de nos emails, afin d'éviter qu'une autre personne que la destinataire ne puisse les lire, ce qui peut être utile lorsque le contenu de nos messages est *sensible* ou qu'il en dit long sur la personne l'ayant rédigé.

Pour définir notre politique de sécurité, il nous faut envisager l'utilisation du chiffrement selon plusieurs modalités. Reprenons le point de vue de l'adversaire et voyons comment nous en prémunir.

35.8.1 Première étape : demander aux factrices

Sans mesure de protection particulière, les services d'hébergement mail pourront lire le contenu des emails qui nous sont destinés. En effet, ce sont sur leurs serveurs que sont acheminés et stockés nos emails. Il n'y a ici pas de grande différence entre l'usage de tel ou tel protocole, d'un client mail ou du webmail.

Nos messages peuvent être ainsi conservés pendant des années jusqu'à ce que nous les rapatrions ou les supprimions, voire plus longtemps encore si l'un des serveurs en fait une copie, dans le cadre d'une sauvegarde par exemple. D'où l'importance, notamment, de fermer des boîtes mail une fois leur raison d'être dépassée. Ceci a également l'avantage de ne pas occuper de l'espace disque et de ne pas consommer de ressources pour rien chez l'hébergeur mail.

3. Le protocole OpenPGP, servant au chiffrement [cette page] des emails, est intégré et activé par défaut depuis la version 78.2.1 de Thunderbird. Nous n'avons donc plus besoin d'installer le module complémentaire Enigmail, qui était nécessaire avec les versions précédentes.



Pour aller plus loin…

À condition d'aimer bidouiller, il est toujours possible de mettre en place et d'auto-héberger son propre serveur de mail sur un service onion (voir page 266).

La lecture de nos messages, qui relève de la violation du secret de la correspondance — tout comme lire une lettre qui ne nous serait pas destinée — ne demande aucun effort technique, pas même celui d'ouvrir une enveloppe. Elle est si simple que son utilisation a notamment été automatisée par Gmail, qui fait lire le contenu des emails de ses utilisatrices par des « robots » afin de détecter le *spam*, mais aussi afin de leur « simplifier la vie » par exemple en détectant quel avion elles vont prendre et les avertir si il est retardé [4].



Précision

Ces « robots » ne sont ni des automates, ni des androïdes, mais de petits programmes qui parcourent « automatiquement » du contenu pour identifier quelque chose : par exemple, les « robots » de Google parcourent les pages web pour indexer les mots-clés pertinents qui pourraient être recherchés. De tels robots sont aussi utilisés par les flics pour leur signaler chaque fois qu'une personne utilise certains mots de leur supposé « dictionnaire des terroristes ».

Concernant les intermédiaires situés entre les ordinateurs des protagonistes de l'échange d'emails et les serveurs des hébergeurs mail respectifs, on peut avoir affaire à deux situations. La première, désormais plutôt rare, est celle où la connexion entre l'ordinateur et le serveur mail n'est pas chiffrée.

Dans ce cas-là, les différents intermédiaires verront passer l'équivalent de cartes postales. Ils seront donc dans une situation similaire à celle des hébergeurs mail, à la différence près que les cartes postales ne feront que transiter… sauf s'ils sont configurés pour inspecter plus profondément le courrier qu'ils transportent, que ce soit pour faire des statistiques afin d'améliorer la qualité de leur service ou pour nous surveiller.



Connexion non-chiffrée aux serveurs mail

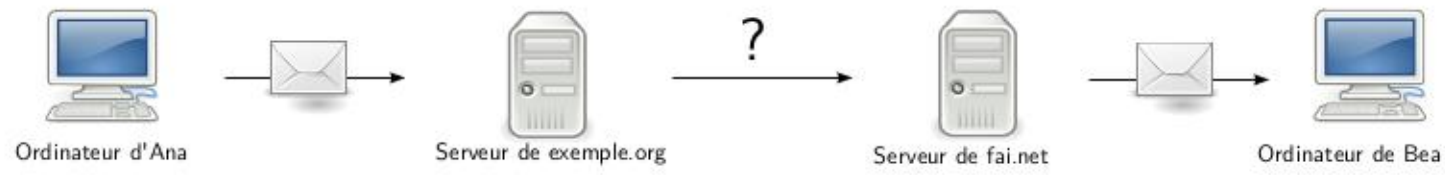
page 249

La seconde situation est celle où la connexion entre l'ordinateur et le serveur mail est chiffrée avec le protocole *TLS* [5]. Ceci est possible quel que soit le protocole utilisé. Les intermédiaires entre les deux machines verront cette fois-ci des cartes postales mises dans des enveloppes. L'hébergeur mail ne sera pas affecté par le chiffrement et aura toujours accès à l'email dans son intégralité.

4. Janko Roettgers, 2017, *Google Will Keep Reading Your Emails, Just Not for Ads* [https://variety.com/2017/digital/news/google-gmail-ads-emails-1202477321/] (en anglais).

5. Lorsqu'on veut chiffrer une connexion avec un serveur web ou email, on utilise le protocole TLS. C'est un standard qui permet d'encapsuler [page 201] le protocole utilisé habituellement. Par exemple, le protocole web HTTP, quand il est encapsulé dans du TLS, donc chiffré, est appelé HTTPS. Il en va de même pour les protocoles mail POPS, IMAPS, et SMTPS.

Enfin, rien n'assure que la connexion entre le serveur mail d'Ana et celui de Bea est chiffrée, auquel cas, le trajet de l'email se fera en partie à la manière d'une lettre, en partie à la manière d'une carte postale.



Connexion chiffrée aux serveurs mail

Chiffrer ses emails

Afin de s'assurer que le contenu de nos messages n'est lisible par aucun des intermédiaires, factrice comprise, il nous est possible de les chiffrer directement sur notre ordinateur, avant même de les envoyer. Pour cela, on utilisera le standard de cryptographie asymétrique OpenPGP. Il serait également possible d'utiliser la cryptographie symétrique, mais ses limites nous amènent à le déconseiller fortement. page 249

En utilisant la cryptographie asymétrique, seule la personne destinatrice, pour laquelle on aura effectuée le chiffrement, sera en mesure de déchiffrer le message. N'oublions pas cependant que la cryptographie asymétrique possède également des limites qui peuvent permettre à une adversaire de révéler le contenu chiffré. page 258

En pratique, si ce n'est pas déjà fait, on commencera par importer la clé publique de notre destinataire. Il faudra alors vérifier son authenticité. De plus, si on compte établir une correspondance et donc recevoir des emails en retour il nous faudra également disposer d'une paire de clés : l'une sera utilisée par nos correspondants pour chiffrer des emails à notre intention, l'autre nous permettra de les déchiffrer. Si l'on n'a pas encore de paire de clés de chiffrement, suivre la recette pour en créer une et en avoir une bonne gestion. page 337 page 338 page 333

Attention cependant, cette méthode permet de chiffrer le contenu de l'email et seulement le contenu. Elle ne modifiera en rien les en-têtes de l'email. page 218

Selon qu'on a choisi d'utiliser un client mail ou le webmail, la méthode à employer pour chiffrer ses emails sera différente.

Chiffrer ses emails dans Thunderbird

Suivre la recette chiffrer ses emails dans Thunderbird (voir page 333).

Chiffrer ses emails pour un webmail avec Tails

Si l'on préfère chiffrer ses emails en utilisant un webmail, éviter de rédiger son message dans la fenêtre du navigateur web pour le chiffrer ensuite. En effet, certaines attaques, notamment *via* JavaScript, sont susceptibles d'accéder à notre texte depuis ce même navigateur web. De plus, le texte rédigé au sein du webmail pourrait être automatiquement enregistré de façon non chiffrée dans les brouillons. Il serait fort regrettable d'offrir en clair un texte que l'on souhaite chiffrer. page 214

On ne va pas expliquer comment chiffrer ses emails pour un webmail avec une Debian chiffrée, mais uniquement avec Tails.

La méthode actuellement conseillée pour chiffrer un email, de même que pour chiffrer un texte, est décrite dans la documentation de Tails.

Une fois Tails démarré (voir page 115), afficher le bureau et double-cliquer sur l'icône *Documentation de Tails*. Dans l'index qui s'ouvre, chercher la section *Chiffrement et vie privée* et cliquer sur la page *Chiffrer du texte et des fichiers avec* GnuPG *et* Kleopatra. Cette page n'est pas encore traduite en français au moment du bouclage de cette édition. Suivre la section *Working with encrypted text* (*Travailler avec du*

texte chiffré) sur cette page de documentation, et en particulier la partie *To encrypt text* (*Pour chiffrer du texte*).

La personne qui reçoit l'email devra, elle, suivre la partie *To decrypt text* (*Pour déchiffrer du texte*) sur cette même page de documentation.

35.8.2 Deuxième étape : regarder sur l'ordinateur utilisé

Supposons qu'une personne attaquante n'a pas accès aux données de nos hébergeurs, et ne peut pas écouter le réseau, mais qu'elle peut venir se servir chez nous : quelles traces de nos échanges trouvera-t-elle sur notre ordinateur ?

page 31

Si cette personne peut mettre la main sur notre ordinateur, ou sur celui de notre destinataire, que ce soit en s'en emparant ou en arrivant à y installer un logiciel malveillant, elle pourra avoir accès à tous les emails stockés sur ces derniers ainsi qu'aux traces laissées ; que ces traces soient dues au fonctionnement de la machine ou laissées par les protagonistes.

page 119

Afin de se protéger d'une adversaire qui pourrait s'emparer de notre ordinateur, on prendra soin de chiffrer son disque dur pour lui compliquer l'accès aux données stockées sur celui-ci. Cela ne nous protègera pas contre un logiciel malveillant voulant exfiltrer ces données, d'où l'importance de n'installer que des logiciels de confiance. On pourra aussi utiliser un système *live* amnésique.

Notons que si les emails stockés font partie d'un échange qui a été chiffré en utilisant la cryptographie asymétrique, quand bien même elle a accès à l'ordinateur et aux données stockées sur celui-ci, l'adversaire ne pourra pas les lire, à moins qu'elle ait aussi accès à la clé secrète. Si l'on utilise Thunderbird pour envoyer nos emails chiffrés,

page 330

cette clé secrète est protégée par le mot de passe principal de Thunderbird, à condition d'en avoir défini un ; dans le trousseau de clés OpenPGP du bureau, la clé secrète est protégée par une phrase de passe. Sans ce mot de passe principal ou cette phrase de passe, l'adversaire ne pourra pas retrouver la clé secrète, et ne pourra donc pas lire les emails chiffrés.

35.8.3 Troisième étape : attaquer le chiffrement du support

Si l'on consulte ses emails sur une Debian chiffrée, les traces sur le disque dur de l'ordinateur seront chiffrées, que l'on utilise le webmail ou un client mail. Elles n'apprendront donc rien à un adversaire en l'état. Cependant certains adversaires pour-

page 50

raient avoir des moyens d'attaquer ce chiffrement. De plus, si la personne avec qui l'on converse par email ne fait pas de même, le niveau global de protection du contenu sera nivelé par la plus faible des deux protections. En effet, avoir pris énormément de précautions et échanger des emails avec une personne ayant par exemple une Debian non chiffrée, ou allumée en permanence[6], peut être plus dangereux car l'on pourrait avoir une impression trompeuse de sécurité. D'autant plus s'il est aisé de localiser ou de mettre un nom sur les protagonistes de l'échange.

En utilisant un logiciel de mail dans un système *live* amnésique, il n'y aura aucune trace sur l'ordinateur utilisé après extinction, mais il y en aura dans la partition persistante si on l'a configurée. Celles-ci seront chiffrées, ce qui revient au cas précédent d'une Debian chiffrée.

Pour ne pas laisser de traces sur l'ordinateur utilisé, chiffrées ou non, on pourra utiliser le système live Tails sans persistance et de profiter ainsi de son amnésie.

35.8.4 Quatrième étape : attaquer le chiffrement des messages

Une adversaire qui a accès à des emails chiffrés, peut essayer d'exploiter les limites

page 50

du chiffrement pour déchiffrer les messages.

6. Lorsqu'elle est allumée, une machine dont le disque dur est chiffré contient de nombreuses informations déchiffrées dans sa mémoire vive [page 18].

Chapitre 36

Cas d'usage : dialoguer

36.1 Contexte

Dans le cas d'usage précédent, on échangeait des messages de façon asynchrone, tout comme dans un échange épistolaire. Cependant on peut vouloir une communication synchrone, comme lors d'une communication téléphonique, que ce soit pour une réunion de travail sur un document sensible ou pour dialoguer avec une amie. Le plus simple pourrait être de se déplacer pour se rencontrer, ou de s'appeler — mais ce n'est pas toujours possible ou souhaitable. Parfois, la messagerie instantanée est une bonne alternative.

page 289
page 79

Beaucoup de gens connaissent et utilisent régulièrement la messagerie de Skype (remplaçant de MSN ou Windows Live Messenger fournie par Microsoft) ou la messagerie interne de Facebook, pour ne citer que les exemples les plus connus. C'est pratique, oui, mais il est possible d'avoir quelque chose de pratique sans renoncer à être discret !

36.2 Évaluer les risques

36.2.1 Que veut-on protéger ?

Les réponses possibles à cette question sont les mêmes que dans le cas de l'échange de messages. On peut vouloir protéger le contenu de l'échange, la localisation des protagonistes, leurs identités, leur lien, *etc.*

page 289

36.2.2 De qui veut-on se protéger ?

Ici aussi, les réponses sont proches de celles données dans le cas d'usage échanger des messages : on peut vouloir dissimuler tout ou partie de ces informations aux diverses machines par lesquelles elles transitent aussi bien qu'aux personnes qui pourraient y avoir accès.

page 289

Parmi lesdites machines, viennent tout d'abord les serveurs de messagerie instantanée utilisés par les différentes correspondantes.

page 217

Viennent ensuite les routeurs, situés sur le trajet entre les protagonistes de l'échange, notamment ceux de leurs FAI (Fournisseurs d'Accès à Internet) respectifs.

page 217

Enfin, des traces sont laissées sur les ordinateurs utilisés.

page 226

36.3 Définir une politique de sécurité

Posons-nous maintenant les questions exposées dans notre méthodologie en adoptant le point de vue de notre adversaire.

page 65

36.3.1 Première étape : toutes les infos à disposition des personnes curieuses

Les messageries internes de Facebook, Skype, *etc.*, permettent à beaucoup de gens de prendre connaissance d'informations qui ne les concernent pas : Facebook ou Microsoft verront passer l'intégralité de nos conversations sur leurs machines, et peuvent les archiver pour pouvoir y accéder ensuite. Les flics n'auront qu'à demander pour bénéficier des informations, et une faille de sécurité sur le serveur peut donner accès à de nombreuses autres personnes. Sans oublier que Facebook change régulièrement ses réglages de confidentialité sans prévenir, et peut décider demain de rendre public ce qui est « privé » aujourd'hui.

Par ailleurs, Skype enregistre l'historique des conversations sur l'ordinateur utilisé, et donc n'importe qui qui aurait accès à l'ordinateur pourrait aussi accéder à cet historique (amie, cambrioleuse, amant jaloux…).

Mais Microsoft et Facebook n'ont pas inventé la messagerie instantanée et de multiples alternatives sont disponibles. Il existe de nombreux logiciels que l'on peut installer sur son ordinateur, qui permettront de communiquer selon divers protocoles : Skype, IRC, XMPP, *etc.*

Le fait d'utiliser un logiciel de confiance nous permettra de désactiver l'archivage des conversations, et donc de limiter les traces laissées sur notre ordinateur.

Il existe également des serveurs qui fournissent des adresses de messagerie instantanée et qui ne sont pas dans une position leur permettant de faire autant de recoupements que Google, Microsoft ou Facebook.

Pour suivre cette piste sur un système Debian (chiffré) installé précédemment (voir page 119), se référer à l'outil installer un logiciel (voir page 131) pour installer `pidgin`. Si l'on utilise Tails, ce logiciel est déjà installé [1].

36.3.2 Deuxième étape : demander aux hébergeurs

En utilisant un client de messagerie instantanée et des serveurs variés, on ne centralise pas tous les liens et les dialogues entre les mêmes mains. Cependant, le contenu des conversations tout comme les parties qui communiquent restent accessibles à partir des ordinateurs par lesquels ils transitent.

S'il est souvent possible de paramétrer notre logiciel pour chiffrer la connexion jusqu'au serveur de messagerie, les dialogues restent accessibles au serveur. De plus, on ne peut en général pas garantir que le lien entre le serveur et l'autre correspondant soit aussi chiffré.

page 228 page 235

Une adversaire qui en a les moyens pourra donc s'adresser aux admins du serveur utilisé, voire aux organisations qui fournissent le réseau, pour obtenir des informations sur les conversations. Elle pourra aussi tenter de « pirater » leurs machines. La confidentialité des dialogues reste donc fortement liée à la confiance qu'on met dans les serveurs de messagerie que l'on utilise, voire dans les infrastructures du réseau et en particulier notre fournisseur d'accès.

page 249

Pour fortement compliquer la tâche d'une adversaire qui voudrait lire le contenu de nos dialogues, on pourra utiliser le chiffrement de bout en bout et disposer alors de **confidentialité**.

Pour suivre cette méthode sur un système Debian (chiffré) installé précédemment (voir page 119), suivre les outils installer un logiciel (voir page 131) pour installer le paquet `pidgin-otr`, puis utiliser la messagerie instantanée avec OTR (voir page 351).

1. Des discussions ont lieu dans Tails pour remplacer Pidgin par un autre logiciel de messagerie instantanée. Cette proposition de modification est suivie sur le gitlab de Tails [https://gitlab.tails.boum.org/tails/tails/-/issues/8573] (en anglais).



Pour aller plus loin…

Il existe des solutions techniques en cours de développement et d'intégration dans Debian pour pouvoir utiliser le chiffrement de bout en bout dans les conversations de groupe. On pourra s'intéresser à Dino [2] qui annonce l'intégration du protocole de chiffrement OMEMO [3]

36.3.3 Troisième étape : les liens restent visibles

Si on utilise le chiffrement de bout en bout dans le cadre d'un dialogue en messagerie instantanée, une adversaire ne peut alors plus avoir accès au contenu de la conversation, à moins de casser le chiffrement utilisé, d'accéder à notre ordinateur, voire de le pirater.

page 258

page 238

Cependant, une adversaire qui a accès au réseau ou au serveur de messagerie utilisé peut toujours voir avec qui nous parlons. Pour cacher les liens, il faudra utiliser des identités contextuelles et se connecter de façon anonyme, par exemple en utilisant Tor. On a alors *confidentialité* grâce au chiffrement, mais aussi *pseudonymat*.

page 243

page 261

En utilisant un système *live* amnésique comme Tails, on s'occupe du même coup de la question des traces qui pourraient être laissées sur l'ordinateur utilisé. Sauf si on utilise la persistance, auquel cas des traces chiffrées seront conservées dans la partition persistante de la clé USB de Tails.

Pour suivre cette piste il nous faudra donc dans un premier temps, si l'on n'en a pas déjà, faire une clé USB ou un DVD Tails (voir page 113).

Ensuite, après avoir démarré sur le support contenant Tails (voir page 107), il nous faudra définir une identité contextuelle à utiliser et mettre en place la persistance de Tails (voir page 116) pour cette identité en activant l'option « Pidgin ».

Nous pourrons enfin suivre l'outil utiliser la messagerie instantanée avec OTR (voir page 351).

On combine ici deux critères : confidentialité et anonymat. À l'étape précédente, on a vu comment disposer de *confidentialité* avec le chiffrement OTR. Ici on vient de voir comment avoir *anonymat et confidentialité* en utilisant le chiffrement OTR sous Tails ainsi qu'une identité contextuelle. Cependant, on peut désirer l'*anonymat ou le pseudonymat seul*, c'est-à-dire sans confidentialité. En effet, on peut vouloir cacher qui on est sans cacher le contenu de nos conversations, par exemple pour discuter dans des « salons » publics traitant de pratiques sexuelles considérées comme transgressives. Pour suivre cette piste on démarrera (voir page 115) alors Tails puis on utilisera Pidgin (voir page 351) sans utiliser le chiffrement OTR, avec un compte créé pour l'occasion.

36.4 Les limites

Tout d'abord, cette méthode reste vulnérable aux éventuelles attaques sur le chiffrement, dont on vient de parler et aux attaques sur Tor.

page 279

Mais il existe aussi quelques limites spécifiques aux conversations en temps réel. Ainsi, l'état « en ligne » ou « hors ligne » d'une identité est en général accessible publiquement. Un adversaire peut ainsi voir quand une identité est connectée, et éventuellement corréler plusieurs identités : parce qu'elles sont toujours en ligne en même temps ; ou au contraire parce qu'elles ne sont jamais en ligne en même temps mais souvent successivement, *etc.*

2. Dino [https://prism-break.org/fr/projects/dino/].
3. Protocole OMEMO [https://prism-break.org/fr/protocols/omemo/] (en anglais).



Précision

Pour que des identités apparaissent comme étant « toujours en ligne », il est possible d'utiliser un « ghost » ou proxy [4] sur un ordinateur en qui l'on a confiance, qui est toujours allumé et connecté au serveur de messagerie instantanée. C'est ainsi cet ordinateur, et non pas le serveur, qui « voit » quand on est connecté ou pas, et cet état n'est plus public. La mise en place d'une telle infrastructure dépasse toutefois pour l'instant les ambitions de ce guide.

Ensuite, dans le cas particulier où l'anonymat (ou le pseudonymat) est prioritaire sur d'autres contraintes, par exemple si l'on souhaite discuter dans un salon public, d'autres limites s'ajoutent à celles évoquées ci-dessus. Ainsi, une identité contextuelle risque toujours de finir reliée à une identité civile, comme nous l'avons vu dans la page 244 partie sur les pseudonymes. En effet, même sous un pseudonyme, le fond et la forme de nos conversations peuvent en dire très long sur la personne se trouvant derrière le clavier.

Il est bon de garder en mémoire le fait que quand on essaye de définir une politique de sécurité lors d'une relation entre plusieurs personnes, que ce soit au téléphone, dans le page 289 cas d'échanges d'emails ou encore ici pour la messagerie instantanée, le niveau global de sécurité sera nivelé par le niveau de sécurité de la protagoniste la moins précautionneuse. En effet, si l'on prend par exemple soin d'utiliser Tails afin de ne laisser aucune trace de notre conversation sur l'ordinateur, alors que notre interlocutrice utilise son système d'exploitation habituel sans protection particulière, alors cette dernière sera sans doute le point le plus faible de la politique de sécurité de notre communication.

Enfin, comme cela a déjà été dit, le chiffrement OTR ne permet pas à l'heure actuelle de converser à plus de deux à la fois. Des recherches avancent cependant dans ce sens [5].



Pour aller plus loin…

En attendant, et à condition d'aimer bidouiller, il est d'ores et déjà possible de mettre en place son propre serveur de messagerie instantanée (par exemple XMPP) sur un service onion (voir page 266).

4. Wikipédia, 2014, *Proxy* [https://fr.wikipedia.org/wiki/Proxy].

5. Ian Goldberg *et al.*, 2009 *Multi-party Off-the-Record Messaging*, CACR Tech Report 2009-27 [http://www.cacr.math.uwaterloo.ca/techreports/2009/cacr2009-27.pdf] (en anglais) ; Jacob Appelbaum *et al.*, 2013, *mpOTR* [https://libraries.io/github/ioerror/mpOTR] (en anglais).

Chapitre 37

Cas d'usage : partager des documents sensibles

37.1 Contexte

Nous avons vu comment publier des documents que l'on veut rendre publics. Mais il est aussi parfois nécessaire de partager avec un groupe restreint de personnes des documents sensibles comme des documents de travail confidentiels, des photos de vacances ou encore le contact d'une source prête à divulguer des documents internes de son entreprise.

page 285
page 79

Dans ce cas d'usage, on va se concentrer sur la partage de documents sensibles *via* Internet, qui fait partie de l'objet de ce deuxième tome du *guide*. Selon notre situation, il peut être aussi possible d'envisager de s'échanger des clés USB chiffrées, des documents papier, *etc.*

37.2 Évaluer les risques

37.2.1 Que veut-on protéger ?

Le contenu du document

Le contenu des fichiers partagés est ici confidentiel. Seules les destinataires doivent donc pouvoir y accéder, de la même manière que lors de l'envoi d'un message électronique. Par exemple, si l'on veut partager des photos de vacances avec sa famille, ce qui est à cacher ce sont les photos elles-mêmes. Le fait que les destinataires soient les membres de la famille n'est pas une information sensible, *a priori*. Il s'agit donc de la partie *protéger ce que l'on partage*.

page 289

La source et la destination

L'identité des personnes source et destinataire peut aussi faire partie des informations que l'on désire protéger. Dans une situation de fuite de documents d'entreprise, qui a transmis les documents, à qui, sont deux informations particulièrement sensibles (la protection des sources d'information des journalistes est d'ailleurs la base de la déontologie du journalisme). Il s'agit là de la partie *protéger qui partage avec qui*.

Alors, on peut séparer cette problématique en trois parties : la première aborde la protection de la source, la seconde la protection des destinataires et la troisième aborde spécifiquement la confidentialité des documents à partager.

37.2.2 Contre qui veut-on se protéger ?

On cherche à se protéger des regards indiscrets qui chercheraient à savoir *qui* fait *quoi* sur le web, comme dans le cas d'usage consulter des sites web. Mais aussi des regards indiscrets qui pourraient tomber *par hasard* sur ces fichiers.

page 277

37.3 Protéger la source

Comme pour les premiers secours : *Se protéger soi-même pour pouvoir soigner les autres.*

Nos fichiers étant confidentiels, leur contenu n'est normalement pas censé être rendu public. Cela dit, rien ne nous garantit qu'ils ne finiront pas par l'être, que ce soit par erreur de notre part, de la part des personnes qui y auront également accès, ou encore car des adversaires mettraient à mal notre stratégie ou sa réalisation.

page 285

La démarche sera très similaire à celle de la publication d'un document que l'on pourra donc lire ou relire. Cependant, quelques réflexions spécifiques à cette situation sont nécessaires.

37.3.1 Première étape : traces dans le document

Lorsque nous voulons partager des documents confidentiels, d'autant plus si nous les avons produits, rien n'indique *a priori* que nous pouvons avoir confiance dans les personnes avec qui ces documents seront partagés.

Imaginons par exemple que nous voulions donner des documents attestant de la comptabilité extravagante de notre parti politique à une journaliste afin qu'elle puisse écrire un article à ce sujet sans les publier. Nous n'avons *a priori* aucune confiance en cette journaliste et préférerons donc qu'elle ne puisse pas savoir de qui ces documents proviennent.

page 30

Il faudra donc éviter d'y laisser des traces menant jusqu'à nous. Qu'elles soient évidentes, comme une identité civile, ou bien plus discrètes, comme les métadonnées :

- tout ce travail de production de documents devra donc être réalisé dans un environnement adapté (voir page 79) ;
- on prendra soin d'effacer les métadonnées (voir page 185).

37.3.2 Deuxième étape : se protéger des intermédiaires

En reprenant notre exemple précédent, c'est-à-dire dans le cas où les personnes avec qui nous partageons des fichiers ne sont pas de confiance, elles pourraient, de leur plein gré ou de force, révéler le site sur lequel elles les ont trouvés.

page 225

page 228

Si l'adversaire a le pouvoir d'accéder aux journaux de connexion [1], grâce à des pressions ou des réquisitions, elle pourrait arriver à savoir d'où vient la connexion qui a permis de mettre ces fichiers en ligne. En conséquence, et si l'on n'a pas mis en place quelques protections sur notre ordinateur, l'adversaire pourrait remonter jusqu'à l'adresse IP publique que l'on a utilisée, voire jusqu'à l'adresse MAC de notre ordinateur.

Pour éviter que les différents intermédiaires entre notre ordinateur et le serveur sur lequel nos fichiers seront hébergés ne fassent preuve d'indiscrétion, nous veillerons à utiliser le réseau Tor, via le Navigateur Tor.

page 261

page 315

page 266

page 359

On peut aller plus loin et éviter d'utiliser un serveur tiers : en partageant nos fichiers directement depuis notre ordinateur avec un service onion (grâce à l'outil OnionShare). Dans ce cas, même si l'adresse web permettant de récupérer les documents est révélée, cela n'aide pas à savoir où l'ordinateur se trouve et ne permet donc pas de remonter jusqu'à nous.

page 279

Il faut cependant garder en tête la possibilité pour l'adversaire d'attaquer Tor.

1. Il peut y avoir des journaux de connexion dans la « box », chez le Fournisseur d'Accès à Internet et chez les hébergeurs.

37.3.3 Troisième étape : regarder sur l'ordinateur source

Les documents confidentiels ou bien des traces de ceux-ci peuvent rester, à dessein on non, sur notre ordinateur.

Les solutions sont soit d'avoir chiffré son disque dur, soit d'éviter dès le départ de laisser des traces en utilisant un système *live* amnésique.

page 119
page 113

37.4 Protéger les destinataires

Après avoir pris les précautions nécessaire pour se protéger, on doit également penser aux destinataires de nos fichiers. Même si on ne peut pas toujours connaître la liste complète des personnes qui auront accès à ces documents, ni les protéger à leur place, on peut toujours faire en sorte qu'un minimum de protection leur soit nécessaire pour y accéder.

Le plus simple, efficace et réalisable est d'utiliser un service onion, ce qui forcera les destinataires à utiliser également le réseau Tor. Pour cela il faudra suivre l'outil OnionShare.

page 266
page 359

37.5 Protéger les fichiers confidentiels

Après avoir pensé à protéger les personnes qui se partagent les documents, reste à protéger les fichiers eux-mêmes.

La démarche ici est similaire à celle de l'échange d'emails confidentiels. Mais nous n'utiliserons pas le courrier éléctronique, soit parce que nos fichiers sont trop volumineux, soit parce qu'on a pas de liste précise de personnes destinataires, donc pas de liste d'adresses mail à qui envoyer ces fichiers. Nous préférerons mettre nos fichiers à partager en ligne sur un serveur, comme dans le cas d'une publication qui serait cette fois-ci privée.

Les solutions employées vont toutes parler de chiffrement, sous différents aspects, en fonction de notre politique de sécurité et de notre optique de partage.

page 295
page 285
page 47

37.5.1 Choisir parmi les outils disponibles

Il existe plusieurs outils pour chiffrer nos fichiers avant de les mettre en partage. Le choix entre l'un de ceux-ci dépend notamment du niveau de partage ainsi que de la qualité du chiffrement souhaité.

37.5.2 Chiffrement proposé par l'hébergeur

Tout d'abord, la solution qui semble demander le moins d'efforts est de mettre nos documents sur un service d'hébergement de fichiers qui propose de les chiffrer directement sur le serveur qui les accueille.

page 319

Généralement, ces services chiffrent les fichiers dans le navigateur de l'utilisatrice avant de les envoyer sur le serveur. Le site crée alors un lien de téléchargement avec la clé de déchiffrement incluse dans ce lien[2]. L'un des avantages est que cette clé n'est pas détenue par l'hébergeur du service : celui-ci n'a donc pas accès aux fichiers des utilisatrices et, même en cas de pressions ou de réquisitions des flics, il n'est pas en mesure de les fournir en clair. L'inconvénient principal de cette méthode est que la clé de déchiffrement est contenue dans le lien de téléchargement. C'est-à-dire que quiconque a accès à ce lien a aussi accès aux fichiers.

page 228

2. Différents logiciels peuvent être utilisés par les serveurs qui hébergent ces services. Lufi et Upl en sont deux exemples. On peut *a priori* leur accorder notre confiance, et les personnes qui écrivent ces lignes ne connaissent pas d'autres logiciels de ce type.

L'utilisation de ces services pour partager des fichiers confidentiels dépend donc de la confiance que l'on peut avoir dans le logiciel qui fournit ce service et dans l'hébergeur qui l'a configuré, ainsi que de la confidentialité mise en place pour transmettre le lien de téléchargement.

Pour limiter les risques, il est toutefois possible de cocher l'option qui active l'effacement des fichiers tout de suite après le premier téléchargement. Cela garantit que ces fichiers ne seront téléchargés qu'une seule fois ; cela permet aussi de savoir si les fichiers ont déjà été téléchargés, et de se rendre compte que la méthode de communication utilisée pour transmettre le lien n'était pas confidentielle.

Si l'on souhaite toutefois choisir de chiffrer en utilisant le service d'hébergement de fichiers, il faudra :

- utiliser le Navigateur Tor (voir page 315) pour accéder au web ;
- consulter la section partager un fichier (voir page 321) de l'outil *Trouver un hébergement web* ;
- avoir un moyen de transmettre le lien de téléchargement de manière confidentielle, par exemple en l'envoyant dans un mail chiffré (voir page 333).

37.5.3 Chiffrement avant le partage

Une autre possibilité est de chiffrer les fichiers avant de les mettre en ligne. Cette solution est un peu plus complexe à mettre en œuvre, mais elle a l'avantage de ne pas nécessiter de faire confiance à l'hébergeur. On choisit nous-même comment sont chiffrés les fichiers, voire qui peut les déchiffrer.

Encore une fois, plusieurs options sont disponibles, en fonction du nombre de destinataires, on pourra chiffrer nos fichiers avec phrase de passe ou avec une ou plusieurs clés publiques.

page 103
page 249

Dans les deux cas, faire attention au nom du fichier contenant le ou les documents chiffrés : si ce nom est explicite, il peut révéler des informations sur le contenu des documents. Renommer alors les fichiers avec un nom neutre, comme « document » ou « archive ».

Chiffrer avec une phrase de passe

page 103

Chiffrer nos fichiers à partager avec une phrase de passe permet à quiconque la possède de pouvoir déchiffrer et avoir accès à nos documents. Il faudra toutefois connaître leur localisation, donc l'adresse web permettant de les télécharger ou bien avoir accès à un des ordinateurs sur lequel ils sont stockés.

Un détail non négligeable est que chaque personne ayant accès aux fichiers doit connaître la phrase de passe qui a permis de les chiffrer pour les rendre lisibles. Il faudra donc utiliser un moyen de communication confidentiel pour partager ce secret entre toutes les personnes destinataires, ce qui peut parfois s'avérer compliqué.

Enfin on se confrontera aux mêmes limites que celles évoquées dans le chapitre sur la cryptographie symétrique.

page 249

Chiffrer avec une ou plusieurs clés publiques

Dans le cas où nous avons une liste définie de personnes avec qui partager nos documents et que chacune d'entre elles possède une paire de clé OpenPGP, il est possible de chiffrer ces fichiers avec leurs clés, afin qu'elles seules puissent les déchiffrer au final.

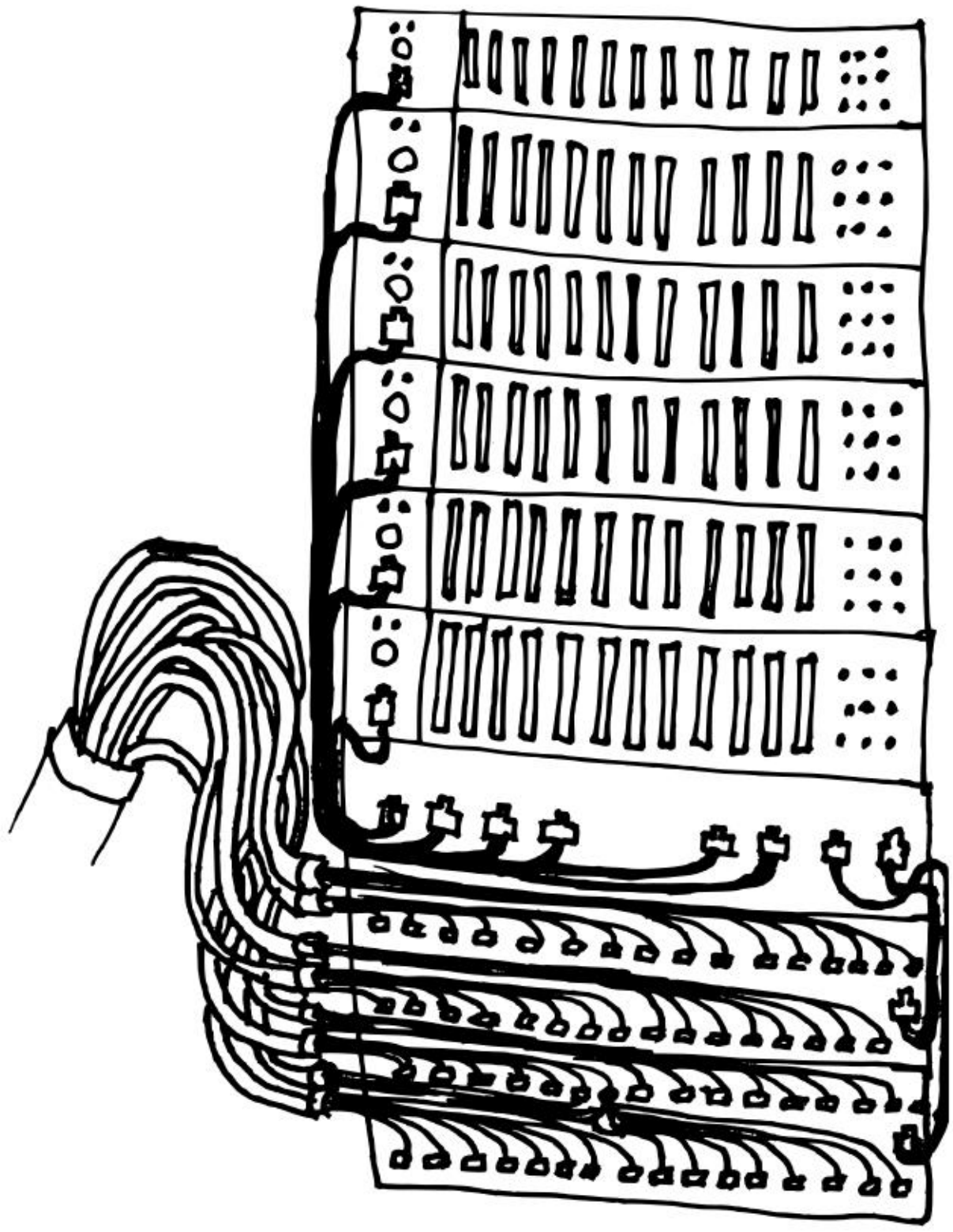
Allons-y

Il faudra d'abord suivre l'outil chiffrer des données (voir page 347), puis choisir une des deux solutions évoquées précédemment pour héberger ces fichiers :

- soit utiliser un service d'hébergement web (voir page 319)
- soit héberger soi-même ces fichiers avec OnionShare (voir page 359).

Déchiffrer les fichiers

Les destinaires des documents devront les déchiffrer en suivant la recette adaptée (voir page 348).



Sixième partie

Outils

Introduction

Dans cette troisième partie, nous expliquerons comment appliquer concrètement quelques-unes des pistes évoquées précédemment.

Cette partie est une annexe technique aux précédentes. Une fois comprises les problématiques liées à l'intimité dans le monde numérique, et une fois choisies les réponses adaptées, reste la question du « Comment faire ? » à laquelle cette annexe apporte certaines réponses.

page 275

Pour la plupart des recettes présentées dans ce guide, nous partons du principe que l'on utilise GNU/Linux avec le bureau GNOME ; ces recettes ont été écrites et testées sous Debian GNU/Linux version 11 (surnommée Bullseye) [1] et Tails version 5 [2] (*The Amnesic Incognito Live System*).

Pour autant, celles-ci sont généralement adaptables à d'autres distributions basées sur Debian, telles qu'Ubuntu [3] ou LinuxMint [4].

Si l'on n'utilise pas encore GNU/Linux, on pourra consulter les cas d'usage du premier tome, au chapitre un nouveau départ, ou utiliser un système *live*.

page 71

Les procédures sont présentées pas à pas et expliquent, chaque fois que c'est possible, le sens des actions proposées.

page 113

L'ordre dans lequel chaque recette est détaillée est important. Sauf mention contraire, il est recommandé de ne pas sauter une étape puis de revenir en arrière. Le résultat obtenu pourrait être très différent de celui attendu.

Enfin, il est important d'utiliser la version la plus à jour de ce guide, car les logiciels évoluent. On pourra la trouver sur le site web https://guide.boum.org/.

1. https://www.debian.org/releases/bullseye/index.fr.html
2. https://tails.boum.org/index.fr.html
3. https://www.ubuntu-fr.org/
4. https://linuxmint.com/

Chapitre 38

Installer et configurer le Navigateur Tor

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Un quart d'heure.

Nous avons vu que, lors de nos navigations sur le web, les sites visités peuvent enregistrer notre adresse IP et donc que des adversaires peuvent facilement remonter à nous par ce biais. D'où, parfois, la nécessité de dissimuler cette adresse IP. Tor est un logiciel permettant de faire transiter notre connexion au sein d'un réseau de « nœuds », masquant ainsi notre adresse IP réelle. C'est le routage en oignon.

page 202

page 261

Pour pouvoir utiliser le *réseau d'anonymisation Tor*, il faut paramétrer le logiciel Tor lui-même, mais également les logiciels qui vont l'utiliser, comme le navigateur web par exemple. Ces paramétrages sont souvent complexes, à tel point qu'il est difficile d'être sûre de l'anonymat qui en résulte.

C'est pourquoi pour utiliser Tor il est conseillé de se servir, soit d'un système *live* dédié à cet usage, soit d'utiliser un « kit prêt à l'emploi » : le Navigateur Tor. C'est un outil qui permet d'installer et d'utiliser très facilement Tor sur un système « classique ». Aucun paramétrage n'est nécessaire et tous les logiciels indispensables à une navigation *via* Tor y sont inclus.

page 113

Le Navigateur Tor rassemble :

- le navigateur web Firefox, paramétré pour utiliser Tor ;
- le logiciel Tor ;
- un lanceur, pour démarrer le tout en un simple double-clic.

Attention : il faut bien garder à l'esprit que le Navigateur Tor ne procure pas un anonymat pour l'ensemble de l'ordinateur : seules les connexions vers les sites web initiées dans ce navigateur passent par Tor. **Toutes les autres connexions (client mail, agrégateurs de flux RSS, Torrent, autres navigateurs web, *etc.*) ne sont pas anonymisées**. De plus, et quand bien même le Navigateur Tor tente de minimiser les traces laissées, des données de navigation telles que des cookies ou un historique peuvent toujours se retrouver enregistrées sur le disque dur, de même que les fichiers téléchargés ou les marque-pages du navigateur. Aussi, au cours de notre navigation, il arrive parfois que l'on clique sur un lien qui ouvre un autre logiciel (lecteur de musique par exemple), qui lui, ne passe pas par Tor. Ces avertissements ne sont pas à prendre à la légère, car des indices sur la nature de notre navigation pourraient alors fuiter.

On va voir ici comment installer le Navigateur Tor sur une Debian chiffrée.

page 119

Cependant, pour pouvoir utiliser un système se connectant à Internet uniquement *via* Tor et pouvoir utiliser Tor avec d'autres logiciels qu'un navigateur web, le plus simple est de se tourner vers un système *live* comme Tails.

page 113

38.1 Installer le Navigateur Tor

Pour installer le Navigateur Tor dans Debian :

- Ajouter le dépôt `contrib` (voir page 136).
- Installer le logiciel *Tor Browser Launcher* (voir page 134) en cherchant *torbrowser* dans la liste des logiciels.
- Lancer *Tor Browser Launcher* en appuyant sur la touche ⊞ (⌘ sur un Mac), taper `torb` puis cliquer sur *Tor Browser Launcher*.

Une fenêtre de configuration de *Tor Browser Launcher* s'ouvre. Il est possible de laisser les options par défaut et de cliquer sur *Installer le Navigateur Tor*.

La première fois qu'il est exécuté, le *Tor Browser Launcher* télécharge le Navigateur Tor depuis le site offciel de Tor [https://www.torproject.org/fr/] et vérifie automatiquement la signature de l'archive, pour finir par l'extraire et l'exécuter.

Au moment de l'écriture de ces lignes, le nom du navigateur n'est pas traduit et est nommé *Tor Browser* en anglais. Après son installation, un raccourci apparaît sur l'ordinateur, pour le trouver afficher la vue d'ensemble des Activités en appuyant sur la touche ⊞ (⌘ sur un Mac), puis taper `tor`.

Si Tor est bloqué (par notre fournisseur d'accès à Internet par exemple), ou si utiliser Tor peut sembler suspect à qui surveillerait notre connexion Internet, on peut configurer le Navigateur Tor pour utiliser des bridges Tor pour dissimuler notre utilisation de Tor.

page 267

On peut pour cela consulter la documentation du Navigateur Tor en cliquant sur ☰ → *Aide* → *Guide d'utilisation du Navigateur Tor* puis en allant sur la page *Ponts*.

38.2 Mise à jour du Navigateur Tor

Le Navigateur Tor télécharge automatiquement les mises à jour à faire, puis propose de les appliquer. Pour cela cliquer sur le menu ☰ puis sur *Redémarrer pour mettre à jour le Navigateur Tor*.

Chapitre 39

Naviguer sur le web avec Tor

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Cinq à dix minutes.

L'objectif de cet outil est de naviguer sur le web de façon confidentielle en utilisant le Navigateur Tor. Il n'y a pas beaucoup de différence avec l'utilisation d'un navigateur web « classique », qu'on considèrera comme un prérequis.

page 261

Si l'on n'utilise pas le système live Tails (voir page 113), il faudra installer le Navigateur Tor (voir page 313).

Une fois le Navigateur Tor lancé, on peut s'en servir presque comme d'un navigateur web ordinaire. Cependant, certains détails sont à noter.

Tout d'abord, il faut avoir bien compris contre quoi Tor protège, mais surtout contre quoi il ne protège pas, afin de ne pas faire n'importe quoi en se croyant protégée.

page 267

Attention : sauf si on utilise Tails, seule la navigation depuis le Navigateur Tor bénéficie de la confidentialité procurée par Tor.

En plus de ces limites, il faut savoir que les sites web consultés peuvent savoir que l'on se connecte *via* le réseau Tor. Certains, comme Wikipédia, utilisent cela pour bloquer l'édition anonyme. D'autres, comme Google, demanderont de résoudre des défis appelés « captcha » [1] pour montrer qu'on est bien une personne (et non pas un robot) avant d'accéder à leurs services. Résoudre ces défis, c'est produire du travail non rémunéré, le plus souvent pour les GAFAM [2]...

Certaines fonctionnalités sont désactivées pour éviter de laisser des traces, comme par exemple le stockage des cookies sur le disque ou l'enregistrement des mots de passe.

39.1 Accéder au dossier Téléchargement du Navigateur Tor

Tous les fichiers téléchargés depuis le Navigateur Tor sont enregistrés dans un dossier spécifique, ce dossier est bien caché [3]. Le plus simple pour trouver ce dossier de téléchargement est de télécharger un document depuis le Navigateur Tor et d'*Ouvrir le dossier contenant le fichier*.

Par exemple, sur une page web avec des images, on peut faire un clic-droit pour *Enregistrer l'image sous...*. Une fois le téléchargement terminé, un nouveau symbole

1. Wikipédia, 2017, *CAPTCHA* [https://fr.wikipedia.org/wiki/CAPTCHA].
2. Xavier de La Porte, 2016, *Le « captcha » ou l'art de faire travailler sans rémunérer*, L'Obs [https://www.nouvelobs.com/rue89/rue89-ce-qui-nous-arrive-sur-la-toile/20140217.RUE2129/le-captcha-ou-l-art-de-faire-travailler-sans-remunerer.html].
3. Dans le cas où le Navigateur Tor est installé depuis Tor Browser Launcher et que la langue du système d'exploitation est le français, le dossier de téléchargement peut être trouvé à partir du dossier personnel : `.local/share/torbrowser/tbb/x86_64/tor-browser_fr/Browser/Téléchargements`.

(ou ⊙) apparaît à coté de la barre d'adresse. Cette flèche affiche la liste de téléchargements et le symbole 🗀 nous invite à *Ouvrir le dossier contenant le fichier*. Une nouvelle fenêtre s'ouvre, c'est le dossier de téléchargement de Tor, et le chemin pour arriver à ce dossier s'affiche dans la barre de menu. On pourra maintenant déplacer les fichiers téléchargés là où on le souhaite.

Si l'on souhaite pouvoir accéder plus facilement à ce dossier par la suite, il est aussi possible de créer un raccourci du dossier *Téléchargements* de Tor :

- Dans le Navigateur Tor, après avoir fait un téléchargement, à droite de la barre d'adresse, cliquer sur 🡻 (ou ⊙).
- Dans le menu déroulant, cliquer sur l'icône 🗀 pour ouvrir le dossier contenant le fichier téléchargé.
- En haut de la fenêtre qui s'ouvre, dans la barre d'adresse, cliquer sur *Téléchargements* ▾.
- Dans le menu déroulant, choisir *Ajouter aux signets*.
- Le signet apparaît dans la colonne de gauche.
- Faire un clic droit dessus et choisir *Renommer…*.
- Lui donner un nom clair, comme *Téléchargements Tor Browser*.

39.2 Limites concernant la géolocalisation

Lorsqu'on utilise Tor, pour le site web que l'on consulte, notre connexion semble provenir de l'endroit où est hébergé le nœud de sortie utilisé. Quelques sites utilisent l'adresse IP de leurs visiteuses pour choisir la langue d'affichage. Ces sites pourront donc s'afficher dans des langues inattendues.

De plus, certaines administrations localisent leurs utilisatrices en fonction de leurs adresses IP, aussi l'utilisation de Tor peut poser des problèmes pour réaliser des démarches administratives [4].



Pour aller plus loin…

Il semblerait que les administrations françaises qui surveillent les adresses IP de leurs utilisatrices ne surveillent que le pays d'origine de la connexion, et pas (encore ?) les adresses des nœuds de sortie Tor.

C'est possible de configurer temporairement le Navigateur Tor pour qu'il n'utilise que des nœuds de sortie en France, ce qui donnera toujours une IP française lors de la navigation.

Attention, utiliser cette option diminue la confidentialité.

Pour faire ça quand on utilise un Navigateur Tor installé avec `torbrowser-launcher` :

1. Fermer le Navigateur Tor.
2. À partir du dossier personnel, trouver le fichier de configuration de Tor qui s'appelle *torrc* :
   - Aller dans *Dossier personnel*.
   - Faire la combinaison de touches Ctrl + H pour afficher les fichiers cachés.
   - Cliquer sur le symbole de la loupe dans la barre de menu et taper `torrc` dans la barre de recherche [5].
3. Ouvrir ce fichier *torrc* avec un éditeur de texte (clic droit → *Ouvrir avec Éditeur de texte*),
4. Ajouter une ligne contenant `ExitNodes {FR}`, puis enregistrer et fermer le fichier.

4. Anonyme, 2019, *Récit d'un controle CAF* [https://web.archive.org/web/20200927180556/https://nantes.indymedia.org/articles/45908].

5. Démarrer le Navigateur Tor, naviguer sur quelques sites et cliquer chaque fois sur le cadenas dans la barre d'adresse pour vérifier que le dernier nœud est toujours bien en France.

Dès les activités administratives finies, ne pas oublier d'éteindre aussitôt le Navigateur Tor, et rééditer le fichier *torrc* pour enlever la ligne qu'on y a ajoutée.

Pour faire ça dans Tails :

1. Au démarrage, configurer un *Mot de passe d'administration*[6] puis *Démarrer Tails*.
2. Se connecter à Tor, puis ouvrir un terminal (*Applications* → *Outils système* → *Terminal*).
3. Taper dans le terminal `sudo gedit /etc/tor/torrc`, appuyer sur la touche *Entrée* (↵ ou return), puis saisir le mot de passe d'administration que l'on a configuré au démarrage. Le fichier de configuration de Tor s'ouvre.
4. Ajouter dans ce fichier la ligne `ExitNodes {FR}`, puis enregistrer et quitter l'éditeur.
5. Dans le terminal, taper la commande `sudo service tor reload` pour relancer Tor avec la nouvelle configuration. Saisir à nouveau le mot de passe d'administration configuré au démarrage.
6. Redémarrer le Navigateur Tor, naviguer sur quelques sites et cliquer chaque fois sur le cadenas dans la barre d'adresse pour vérifier que le dernier nœud est toujours bien en France.

Dès les activités administratives terminées, redémarrer Tails.

---

5. Dans le cas où le Navigateur Tor est installé depuis Tor Browser Launcher et que la langue du système d'exploitation est le français, le chemin devrait ressembler à ça : `.local/share/torbrowser/tbb/x86_64/tor-browser_fr/Browser/TorBrowser/Data/Tor/torrc`.

6. https://tails.boum.org/doc/first_steps/welcome_screen/administration_password/index.fr.html

Chapitre 40

Choisir un hébergement web

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Une demi-heure à une heure.

L'objectif de cette partie est de trouver où héberger un document sur le web. Les possibilités sont trop nombreuses pour pouvoir apporter une réponse « clé en main » à cette question. De plus, conseiller une petite liste d'hébergeurs, sur lesquels seraient centralisés beaucoup de contenus « à risque », ne semble pas une bonne idée. Cette recette donnera donc plutôt quelques pistes pour choisir au mieux un hébergement.

Il est aussi possible d'héberger nous-même notre document de façon anonyme en utilisant les services onion de Tor. Pour cela, il faudra aller voir la recette sur l'utilisation d'OnionShare.

page 242
page 266
page 359

40.1 Quelques critères de choix

Il existe de très nombreux hébergeurs possibles, à tel point que l'on peut vite se sentir perdues dans la jungle des possibilités. Voici donc quelques critères pour se poser les bonnes questions. On parlera ci-dessous de document, mais ces critères valent aussi pour un projet plus ambitieux, tel qu'un blog ou un documentaire vidéo.

- **Type d'organisation :** beaucoup de sites proposent d'héberger des documents « gratuitement ». Nombre d'entre eux sont des services commerciaux qui trouvent un intérêt à publier du contenu créé par leurs utilisatrices. Mais il existe aussi des associations ou des collectifs qui hébergent des projets, sous certaines conditions.

page 240

- **Conditions d'hébergement :** si le document ne plaît pas à l'hébergeur, rien ne l'empêche de le supprimer sans même nous avertir. Sa charte (que l'on doit accepter lors de l'hébergement de notre document) peut souvent nous donner une idée de ce que l'hébergeur tolère ou non.
- **Conditions d'identification :** dans quelle mesure l'hébergeur demande des précisions et des garanties sur nos données personnelles à fournir pour pouvoir utiliser ses services.
- **Résistance aux pressions :** l'État peut, lui aussi, vouloir empêcher que notre document reste en ligne. Il lui suffit, dans bien des cas, d'intimider l'hébergeur pour que ce dernier supprime notre document. En effet, selon l'hébergeur choisi, celui-ci peut supporter plus ou moins la pression : certains attendront qu'un recours à la justice soit effectué, tandis que d'autres supprimeront notre document dès le premier email un peu menaçant.
- **Suppression du document :** inversement, on peut vouloir à un moment supprimer notre document. Or, l'hébergement de documents étant un service que l'on remet dans les mains d'autres personnes plus ou moins de confiance, on ne

peut pas avoir la garantie que nos fichiers seront réellement effacés à notre demande. Mieux connaître l'hébergeur peut dans certains cas nous donner plus de garanties.

- **Risques pour l'hébergeur :** selon le contenu de notre document, il peut faire courir un risque à l'hébergeur, en particulier s'il s'agit d'un hébergeur qui ne souhaite pas collaborer avec les flics. Il est alors nécessaire de se demander si l'on accepte de faire courir un risque à un hébergeur, qui pourrait être amené à disparaître en cas de répression.
- **Taille du document :** si notre document est « trop gros », certains hébergeurs refuseront de le prendre. Cela peut également être le cas si notre document est « trop petit ». La taille autorisée est spécifiée dans certaines offres, mais attention : certains hébergeurs rendent payantes des fonctionnalités comme l'hébergement de très gros fichiers.
- **Durée d'hébergement :** selon les hébergeurs, de nombreuses offres existent quant à la durée de l'hébergement. Par exemple, certains suppriment automatiquement le document au bout d'un délai donné, d'autres s'il n'a pas été téléchargé pendant un certain temps, *etc.*
- **Conditions d'identification pour la consultation :** afin de réduire le plus possible la possibilité que l'hébergeur ou les flics parviennent à identifier les personnes qui viendraient consulter notre document, il est important de ne pas utiliser un hébergement sur lequel elles pourraient déjà être identifiées. Ainsi, par exemple, les réseaux sociaux et autres plateformes du même genre (Facebook, Twitter, YouTube, *etc.*) sont à proscrire.
- **Utilisation via Tor :** pour les mêmes raisons, mieux vaut nous assurer que le document pourra être déposé et/ou accessible depuis le Navigateur Tor, voire depuis un service onion.

page 261

- **Rétention des journaux de connexion :** l'envoi, comme la consultation du document, peut laisser des traces compromettantes dans les journaux de connexion de l'hébergeur. Choisir un hébergeur qui ne conserve pas ces journaux ou bien les efface régulièrement permet de réduire ce risque.

page 266

- **Confidentialité du document :** suivant nos besoins, on peut souhaiter que l'hébergeur propose un système de chiffrement afin que le contenu du document ne puisse pas être lisible sur le serveur, ou au contraire ne pas s'en préoccupper puisque le document sera accessible publiquement.

page 225

40.2 Type de contenu

Maintenant que l'on a quelques critères de choix en tête, essayons de rendre cela plus concret. L'hébergement adapté à notre projet dépend du type de contenu que l'on souhaite publier : texte, image, vidéo, son, *etc.*

40.2.1 Publier du texte

Publier du texte est souvent ce qu'il y a de plus simple.

Si le texte à publier est en rapport avec un autre texte déjà publié, il est souvent possible de poster un commentaire, que ce soit sur un blog, un forum ou un site participatif. Pour ce genre de publication, l'inscription n'est pas forcément obligatoire. Cela ne veut en aucun cas dire que la publication est anonyme si l'on ne prend pas de précautions particulières, comme par exemple utiliser le routage en oignon. De plus, notre texte étant un commentaire et non un sujet principal, il n'est pas forcément mis en avant sur le site.

page 261

Il est aussi possible de publier un texte sur un site ou un blog existant. Il faudra alors l'envoyer au site en question *via* un formulaire ou par mail et la publication dépendra alors des administratrices. Certains sites [1] proposent la publication libre d'articles sur un thème donné.

1. Par exemple les sites du réseau Indymedia [https://fr.wikipedia.org/wiki/Indymedia] et ceux du réseau Mutu [https://reseaumutu.info].

40.2.2 Avoir un blog ou un autre site

Si l'on souhaite publier régulièrement des textes, on peut aussi choisir d'administrer un blog : de nombreuses organisations proposent des blogs déjà configurés et faciles à utiliser. On pourrait également administrer un site web, mais cette méthode demande un peu d'apprentissage.

Dans de nombreuses villes, des groupes de personnes s'intéressant aux logiciels libres ou à la liberté d'expression sur Internet peuvent être de bon conseil. Quelques listes sont aussi disponibles sur le web :

- une liste de grosses plateformes de blogs sur Wikipédia [https://fr.wikipedia.org/wiki/Cat%C3%A9gorie:H%C3%A9bergeur_de_blogs] ;
- une liste de services web libres sur le wiki de la communauté francophone d'Ubuntu [https://doc.ubuntu-fr.org/liste_de_services_web_libres] ;
- il existe aussi l'hébergeur noblogs.org [https://noblogs.org/].

40.2.3 Publier des fichiers audiovisuels

Afin de publier des images, vidéos ou sons, pour accompagner le texte d'un article par exemple, il existe plusieurs solutions. Tout d'abord, la plupart des sites où l'on peut publier du texte proposent l'inclusion de documents audiovisuels. Ces sites proposent alors, soit de prendre des fichiers depuis notre ordinateur (qui seront donc ensuite hébergés sur leur serveur), soit d'indiquer l'adresse des fichiers déjà hébergés sur un autre serveur.

Il existe aussi des sites dédiés au partage de fichiers audiovisuels. En voici quelques-uns :

- L'organisme à but non-lucratif *Internet Archive* se veut être une bibliothèque numérique libre [https://archive.org/].
- Le collectif CHATONS[2] maintient une liste de nombreux outils et services libres [https://entraide.chatons.org/], dont notamment des services de partage de vidéos [https://www.chatons.org/search/by-service?service_type_target_id=152] ou d'hébergement d'album photo [https://www.chatons.org/search/by-service?service_type_target_id=150]. Certains services permettent par ailleurs de stocker les fichiers de manière chiffrée sur leurs serveurs (dans le cas de l'hébergement d'images, cependant, selon les serveurs, cela n'est pas toujours automatique : il faut parfois demander explicitement le chiffrement du fichier lors de l'envoi).
- Enfin, on peut utiliser les outils cités dans la partie suivante sur le partage de fichiers.

40.2.4 Partager un fichier téléchargeable

Pour publier des documents que l'on souhaite rendre téléchargeables, on va aller voir du côté des services de téléchargement direct de fichiers (ou *DDL* pour *Direct Download Link*).

En français, cela signifie « lien de téléchargement direct » : on « poste » notre fichier sur un serveur de téléchargement direct, et on obtient alors un lien (une adresse web) qui, lorsqu'on le tape dans un navigateur web, permet de lancer le téléchargement du fichier.

Il existe aussi des sites de partage ou d'hébergement de fichiers. En voici quelques-uns :

- Le projet Riseup, collectif fournissant des outils de communication sécurisée, propose aussi un outil de partage de fichiers légers [https://share.riseup.net/].

2. CHATONS [https://chatons.org/], pour Collectif d'Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires, est une initiative qui a vu le jour en 2016. Ce collectif a pour objectif de rassembler les organisations souhaitant proposer des services respectueux de la vie privée des personnes qui les utilisent.

- Certaines structures du collectif CHATONS[3] fournissent un service de partage de fichiers [https://www.chatons.org/search/by-service?service_type_target_id=148].

Certains services permettent de stocker les fichiers de manière chiffrée sur leurs serveurs, comme ceux basés sur le logiciel *Lufi*.

40.3 En pratique

De façon plus concrète, il faut en premier lieu choisir l'hébergeur du fichier. Les critères présentés auparavant aident à effectuer ce choix. Il est très important de choisir un hébergeur en bonne connaissance de cause car notre anonymat peut dépendre en partie de ce choix.

page 305
page 347
Il est également possible de chiffrer le fichier à héberger. Pour cela, deux possibilités : soit l'on chiffre le fichier avant de le faire héberger en ligne ; soit l'on choisit un hébergeur qui chiffre le fichier dans notre navigateur web avant de le stocker sur ses serveurs, comme chez les CHATONS par exemple.

page 277
Afin de faire héberger notre fichier à proprement parler, la méthode exacte est différente selon l'hébergeur, mais le principe reste le même. On va tout d'abord ouvrir notre navigateur web et l'utiliser de façon, discrète. Ensuite, on va se rendre sur le site de l'hébergeur et trouver la page où « déposer » notre fichier (*upload* en anglais). Là, il faudra suivre la méthode spécifique à l'hébergeur afin de lui transmettre notre fichier. En général, cette méthode est facile à suivre et, même si elle varie, reste relativement similaire d'un hébergeur à l'autre. Une fois l'*upload* terminé, l'adresse web à laquelle se trouve le fichier est affichée.

page 293
page 243
Il est parfois nécessaire d'entrer une adresse mail afin de recevoir cette adresse web : le cas d'usage sur les échanges par mail et le chapitre sur les identités contextuelles vont nous permettre de décider quelle adresse mail fournir dans ce cas.

Une fois le lien obtenu, on peut le diffuser de la manière qui nous convient le mieux. Les personnes qui disposeront du lien pourront télécharger le fichier en le saisissant dans la barre d'adresse d'un navigateur web.

3. CHATONS [https://chatons.org/], pour Collectif d'Hébergeurs Alternatifs, Transparents, Ouverts, Neutres et Solidaires, est une initiative qui a vu le jour en 2016. Ce collectif a pour objectif de rassembler les organisations souhaitant proposer des services respectueux de la vie privée des personnes qui les utilisent.

Chapitre 41

Vérifier un certificat électronique

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quinze à trente minutes.

Nous avons vu précédemment qu'afin d'établir une connexion chiffrée, il fallait souvent faire confiance à une autorité de certification (AC). La plupart du temps, les AC sont déjà enregistrées sur l'ordinateur, dans le navigateur web par exemple. Mais ce n'est pas toujours le cas : notre navigateur web ou autre logiciel nous présentera alors un message nous expliquant qu'il n'a pas pu authentifier le certificat du service.

page 255

Il arrive également que le service visité, par manque de confiance, n'utilise pas d'autorité de certification. Il faut alors vérifier nous-même son certificat.

41.1 Vérifier un certificat ou une autorité de certification

Pour voir le certificat d'un site web, dans un navigateur web, on peut cliquer sur le cadenas dans la barre d'adresse, puis sur *Connexion sécurisée*, puis sur *Plus d'informations*. Une nouvelle fenêtre s'ouvre et indique plein d'informations sur la page web.

En cliquant sur le bouton *Afficher le certificat*, on peut regarder plus en détail le certificat, et savoir par exemple qui l'a émis, pour combien de temps, *etc.* Dans cette fenêtre, il y a généralement plusieurs onglets, correspondant chacun à un certificat. Le premier onglet correspond au certificat du site proprement dit ; les suivants correspondent aux autorités de certification qui authentifient le certificat du site (par le biais d'une signature numérique).

page 252

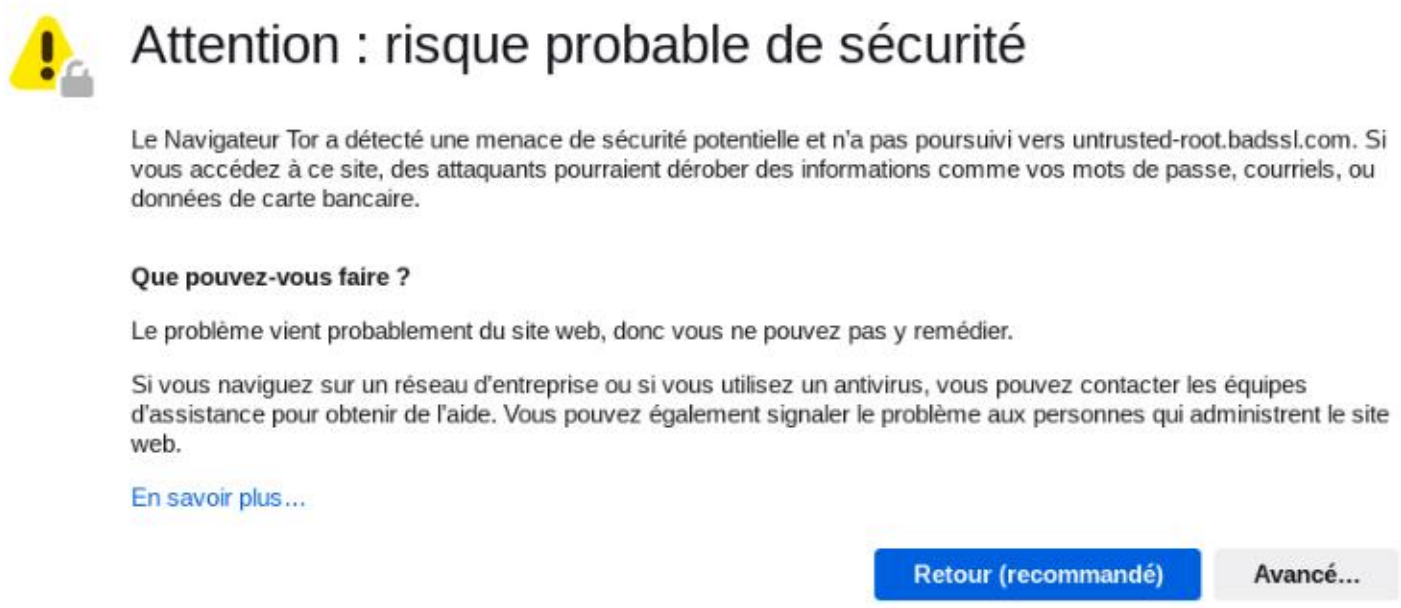
Nous nous intéresserons en particulier au certificat présenté par le site à notre navigateur web. On trouvera son empreinte SHA-256 dans la section *Empreintes numériques* du premier onglet.

Pour le certificat du site https://guide.boum.org/ utilisé en date du 13 décembre 2021 [1], par exemple, on obtiendra la chaîne de caractères suivante :

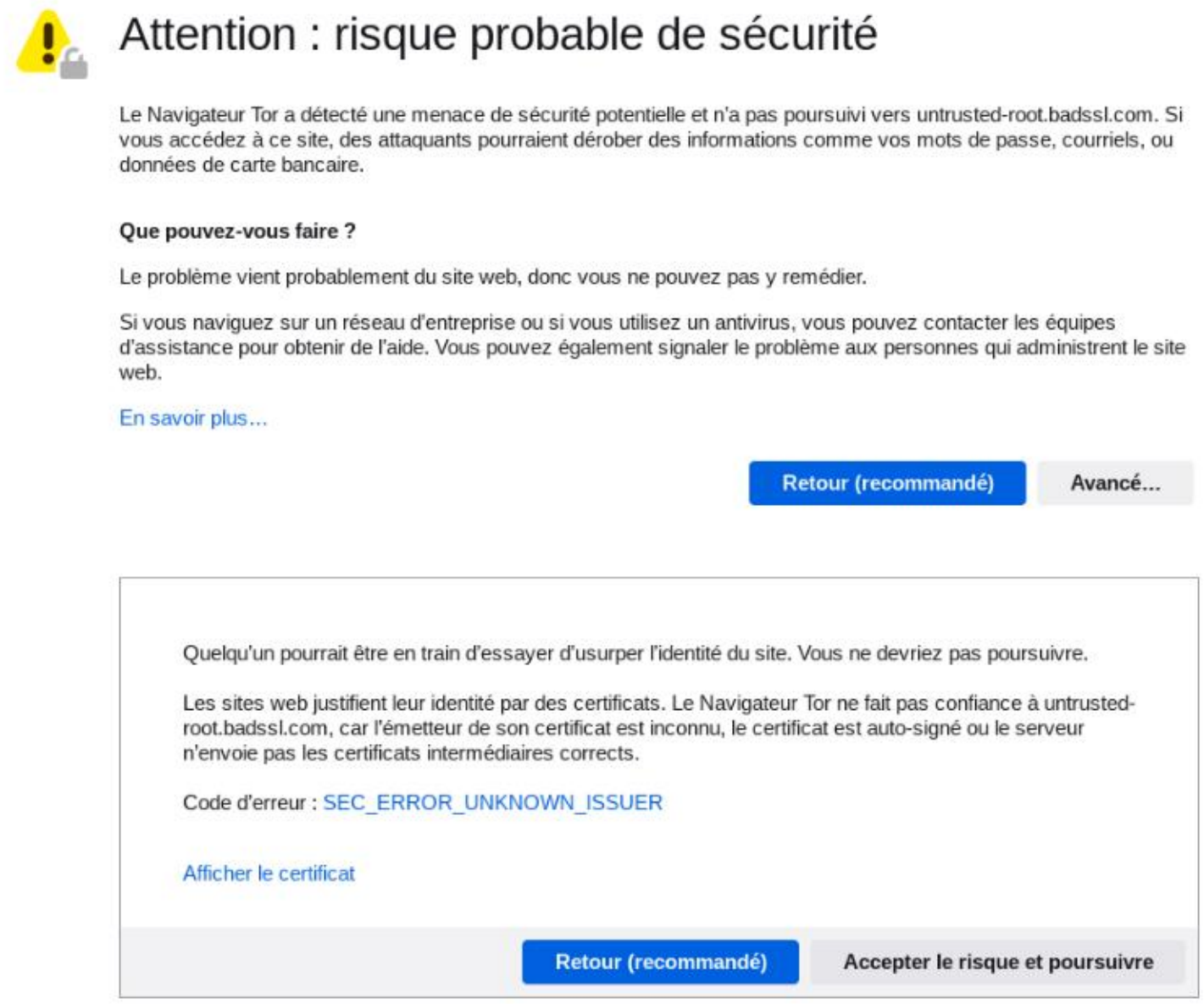
```
72:7E:9E:A3:1E:2E:B9:E1:5B:D5:88:93:01:38:7A:70:
8B:C6:81:E2:F3:D0:5F:CC:63:40:51:CF:22:EC:28:41
```

1. Ce certificat est disponible à l'adresse https://crt.sh/?id=5796332967.

Il arrive parfois que le navigateur affiche un avertissement de sécurité.



page 254 La notion « d'informations dérobées » évoquée dans le message précédent fait référence à l'attaque du monstre du milieu. Une fois cet avertissement parcouru, on peut cliquer sur *Avancé…*, ce qui fera apparaître la raison pour laquelle le navigateur web n'a pas voulu accepter le certificat, comme dans la capture d'écran suivante.



En cas de certificat auto-signé, on pourra lire par exemple la phrase *Le certificat n'est pas sûr car il est auto-signé.* Il se peut aussi que la date de validité du certificat soit dépassée, ce qui n'en empêche pas forcément l'usage. Il est en tout cas toujours utile de lire cette partie et de se demander si l'on souhaite continuer au regard de ces informations. Il est alors nécessaire de vérifier les certificats du site et des autorités de certification le cas échéant. Sans cela, la connexion sera bien chiffrée, mais pas *authentifiée*. Autrement dit, on chiffrera bien la communication, mais sans savoir vraiment avec qui on communique — ce qui est loin d'être idéal.

page 254

page 53 Vérifier un certificat signifie, la plupart du temps, visualiser son empreinte numérique et la comparer avec une autre source afin de s'assurer qu'elle est correcte. Nous

utiliserons de préférence l'empreinte numérique de type SHA-256, et non celle de type MD5 [2] ou SHA-1 [3], ces dernières n'étant plus considérées comme sûres.

Reste à trouver d'autres sources permettant d'obtenir cette empreinte. Il existe quelques techniques pour essayer de s'assurer de l'authenticité d'un certificat :

- Si une personne de confiance à proximité de nous utilise déjà le site ou l'AC en question et a déjà vérifié son certificat, on peut comparer l'empreinte du certificat qu'elle connaît avec celle qui nous est présentée. On peut également la demander par email à des personnes qui nous l'enverront de façon chiffrée *et* signée pour plus de sécurité. C'est encore mieux si l'on est en contact avec plusieurs de ces personnes, qui auraient vérifié ce certificat en utilisant chacune différentes connexions à Internet. Il faut alors suivre la démarche expliquée plus loin pour retrouver l'empreinte d'un certificat déjà installé dans le navigateur web de ces personnes. page 297
- Si l'on a accès à plusieurs connexions Internet depuis l'endroit où nous sommes, par exemple en zone urbaine où l'on trouve beaucoup d'accès Wi-Fi, on peut visiter le site web ou télécharger le certificat de l'AC en utilisant plusieurs de ces connexions et comparer l'empreinte du certificat qui nous sera présentée à chaque fois.
- Si l'on utilise le Navigateur Tor, on peut profiter du changement de circuit, et donc de nœud de sortie sur Internet, pour vérifier à plusieurs reprises l'empreinte du certificat. Cela évitera qu'une personne malveillante ayant la main sur le nœud de sortie ou étant placée entre le nœud de sortie et le site consulté puisse usurper son identité. page 261 page 254
  Pour connaître l'adresse IP du nœud de sortie par lequel on passe pour consulter un site dans le Navigateur Tor, il faut cliquer sur le cadenas 🔒 sur la gauche de la barre d'adresse, juste avant l'adresse du site. Un encart *Informations pour le site [...]* apparaît alors, détaillant, entre autres, le *Circuit Tor* emprunté pour ce site. Le nœud de sortie est l'avant-dernier nœud de la liste, juste avant le nœud correspondant au site visité. Sa géolocalisation (son pays) et son adresse IP sont indiquées. (Attention : il n'y a pas de nœud de sortie lorsque l'on consulte un service onion, c'est-à-dire un site dont le nom de domaine est en *.onion*.)
  Dans le même encart, il est possible de changer le circuit Tor emprunté pour accéder à ce site en cliquant sur le bouton *Nouveau circuit pour ce site*, situé juste en dessous de la représentation du circuit actuel. On peut alors s'assurer que l'IP du nœud de sortie change bien à chaque renouvellement du circuit.
  À chaque fois que le nœud de sortie change, on peut recharger le site visité ou le certificat de l'AC, et comparer son empreinte avec celles collectées les fois précédentes. Au bout de quelques essais réussis, la probabilité qu'il s'agisse du bon certificat devient suffisamment grande pour l'accepter. Enfin, c'est à nous d'en juger en fonction de notre politique de sécurité ! page 65

Ces techniques utilisées isolément ne sont pas forcément très robustes, mais leur utilisation conjointe procurera une crédibilité suffisante dans le fait que le certificat que l'on va utiliser est le bon. Et que personne n'aura réussi à nous tromper.

Gardons à l'esprit toutefois que ceci ne nous protège pas contre toutes les attaques visant le chiffrement de la connexion. page 255

Une fois que l'on aura pu établir avec un degré de confiance suffisant que le certificat présenté correspond bien au site que l'on souhaite consulter, on pourra cliquer sur le bouton *Accepter le risque et poursuivre* sur la page d'avertissement. Le certificat sera alors accepté par le navigateur web, et le site s'affichera.

---

2. Chad R Dougherty, 2008, *MD5 vulnerable to collision attacks* [https://www.kb.cert.org/vuls/id/836068] (en anglais).
3. Julien Cadot, 2017, *SHAttered : Google a cassé la fonction de hachage SHA-1* [https://web.archive.org/web/20211122073218/https://www.numerama.com/tech/235436-shattered-google-a-casse-la-methode-de-chiffrement-sha-1.html].

41.1.1 Le cas particulier des services onion

Il est à l'heure actuelle très difficile d'obtenir des certificats valides pour les services onion (les sites dont le nom de domaine se termine par *.onion*), ce qui fait que l'on aura toujours un message d'avertissement du Navigateur Tor lorsqu'on voudra se connecter à un tel site en *https*.

La plupart du temps, le certificat utilisé par le service onion est auto-signé : cela signifie que le site a lui-même signé son propre certificat. On pourra alors vérifier la validité de celui-ci par d'autres moyens, comme décrit dans la partie précédente.

page 323

Dans le cas de services onion qui sont aussi accessibles avec un nom de domaine « classique », le certificat présenté est généralement un certificat valide pour ce nom de domaine, mais pas pour le nom en *.onion*. Il suffit alors de vérifier que le nom de domaine pour lequel le certificat est valide correspond bien au site auquel on souhaite se connecter.

Quoi qu'il en soit, la confidentialité et l'authenticité de la connexion à un service onion sont assurées par le protocole de routage en oignon et par le système de « point de rendez-vous » : si l'on est sûre que l'adresse *.onion* à laquelle on se connecte est correcte, alors on peut être convaincue avec une confiance plutôt élevée que l'on accède bien au service onion correspondant.

page 261

page 266

41.2 Trouver l'empreinte d'un certificat déjà installé

Cette empreinte peut être visualisée en cliquant sur ☰ dans notre navigateur pour afficher le menu de Firefox ou du Navigateur Tor et en allant ensuite dans *Paramètres*. Choisir la page *Vie privée et sécurité*, puis descendre jusqu'à la section *Certificats*. Ici, cliquer sur *Afficher les certificats…*. On trouvera les certificats des sites déjà installés en choisissant l'onglet *Serveurs* dans la fenêtre qui s'ouvre. Enfin, en sélectionnant le site souhaité dans la liste et en cliquant sur le bouton *Voir…*, on pourra visualiser l'empreinte numérique du certificat. La même opération est possible pour les autorités de certification en choisissant plutôt l'onglet *Autorités*.

Chapitre 42

Utiliser un clavier visuel dans Tails

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quelques minutes.

Nous avons vu dans le premier tome qu'un ordinateur peut être compromis matériellement. Il peut notamment contenir des keyloggers matériels qui pourraient enregistrer tout ce qui est tapé sur le clavier. Les textes que l'on écrit, des actions que l'on exécute, mais surtout les mots de passe que l'on saisit.

page 35

Lorsqu'on a un doute quant à la confiance à accorder à un ordinateur sur lequel on va utiliser Tails, il est possible d'utiliser un clavier visuel (anciennement appelé « clavier virtuel ») afin de rendre inefficace la récupération des frappes sur le clavier. Attention cependant, cette méthode ne protège pas d'un mouchard qui enregistrerait l'affichage de l'écran.

page 31

Un clavier visuel est un logiciel ayant l'apparence d'un clavier et qui nous permet de saisir des caractères sans utiliser le clavier matériel de l'ordinateur. Il peut être utilisé avec plusieurs dispositifs de pointage comme une souris, un écran tactile ou un pavé tactile, par exemple.

L'environnement de bureau GNOME fourni par Tails permet d'utiliser un clavier visuel parmi les différentes options d'accessibilité proposées. Il faut pour cela cliquer sur l'icône d'*Accès universel* dans la barre tout en haut, puis activer l'option *Clavier visuel*. Une autre possibilité est d'appuyer sur la touche [⊞] ([⌘] sur un Mac), de taper `param`, puis de cliquer sur *Paramètres* : on peut alors activer l'option *Clavier visuel* dans la section *Saisie* de la page *Accessibilité*.

Une fois activé, le clavier visuel s'affiche dès qu'on a la possibilité de saisir du texte. Il suffit alors de taper ses mots de passe en utilisant sa souris, son touchpad ou tout autre dispositif de pointage.

Il est à noter qu'il est possible d'activer ce clavier visuel dès l'écran de bienvenue de Tails, ce qui permet de l'utiliser aussi pour saisir la phrase de passe afin de déverrouiller le volume persistant.

Chapitre 43

Configurer et utiliser le client mail Thunderbird

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quinze à trente minutes.

Cette partie va décrire la méthode à adopter pour configurer et utiliser le client de messagerie Thunderbird de manière à l'utiliser pour toutes les tâches ayant trait à ses emails. Elle a été testée avec la version 91 de Thunderbird. L'interface pourrait être légèrement différente avec des versions plus récentes.

Sous Debian, si Thunderbird n'est pas encore installé, il faut installer le paquet `thunderbird-l10n-fr`[1] en suivant la recette installer un logiciel. page 135

43.1 Lancer Thunderbird

Lancer Thunderbird en appuyant sur la touche ⊞ (⌘ sur un Mac), taper `thu` puis cliquer sur *Messagerie Thunderbird*.

Lorsqu'on lance Thunderbird et qu'aucun compte mail n'y est configuré, un onglet de configuration intitulé *Configurez votre adresse électronique existante* apparaît afin de nous assister dans l'ajout d'un premier compte à partir d'une adresse mail déjà existante.

Néanmoins, il vaut généralement mieux prendre un peu de temps pour paramétrer certaines options de confidentialité de Thunderbird avant de configurer ce premier compte mail : on peut donc fermer cet onglet en cliquant sur *Annuler* afin de pouvoir réaliser les opérations décrites ci-dessous. Cependant, si l'on souhaite configurer dès maintenant un compte mail, on peut directement passer à la partie correspondante. page suiv.

43.2 Configurer le routage en oignon pour Thunderbird

Si l'on utilise Tails, Thunderbird est déjà configurer pour fonctionner avec Tor. On peut directement passer à l'étape suivante page suiv.

Si l'on utilise Thunderbird dans un système Debian et que l'on souhaite qu'il utilise le réseau Tor pour se connecter à notre serveur de messagerie, une configuration spécifique est nécessaire. page 261

Premièrement, installer le Navigateur Tor s'il n'est pas déjà installé. page 313

Ensuite :

- ouvrir l'onglet *Préférences* en allant dans ☰ pour afficher le menu de Thunderbird.

1. Le protocole OpenPGP, servant au chiffrement [page 295] des emails, est intégré et activé par défaut depuis la version 78.2.1 de Thunderbird. Nous n'avons donc plus besoin d'installer le module complémentaire Enigmail, qui était nécessaire avec les versions précédentes.

- S'assurer qu'on est bien dans la rubrique *Général* dans la colonne de gauche.
- Descendre jusqu'à la section *Connexion*.
- Cliquer sur *Paramètres...* au niveau de *Configurer la façon dont Thunderbird se connecte à Internet*.
- Cocher *Configuration manuelle du proxy*.
- Remplir le champ *Hôte SOCKS* avec `127.0.0.1` et *Port* avec `9150`.
- Cocher *SOCKS v5*.
- Cocher *Utiliser un DNS distant lorsque SOCKS v5 est actif*.
- Cliquer sur le bouton *OK*.
- Fermer l'onglet des préférences en cliquant sur le bouton ✖ correspondant.

Désormais, avec cette nouvelle configuration, pour pouvoir recevoir et envoyer des emails, il faudra toujours ouvrir le Navigateur Tor et se connecter à Tor. Si, pour une raison ou pour une autre, le Navigateur Tor ne fonctionne pas, l'envoi et la réception d'emails ne marcheront pas non plus.

43.3 Définir un mot de passe principal dans Thunderbird

page 249
page 252
Par défaut, Thunderbird propose de retenir les mots de passe d'accès aux comptes mail configurés. De plus, si l'on souhaite utiliser les fonctionnalités de chiffrement ou de signature numérique des emails avec OpenPGP décrites au chapitre suivant, Thunderbird aura besoin de stocker notre *clé privée* dans sa configuration.

page 333
page 249
Afin de restreindre l'accès à ces mots de passe et clés privées enregistrées par Thunderbird, il faut définir au préalable un *mot de passe principal*. Cette phrase de passe va être demandée à chaque ouverture du Thunderbird.

Pour cela, dans Thunderbird, cliquer sur ☰ pour afficher le menu, puis sur *Préférences*. Dans la liste de gauche, choisir *Vie privée et sécurité* et descendre jusqu'au titre *Mots de passe*. Cocher la case *Utiliser un mot de passe principal*. Une nouvelle fenêtre s'ouvre, demandant un mot de passe pour protéger la clé. C'est le moment de choisir page 103 une bonne phrase de passe puis de la taper deux fois, avant de cliquer sur *OK*. Un message de confirmation du changement de mot de passe principal apparaît. On peut alors le valider avec *OK* puis fermer l'onglet des préférences en cliquant sur le bouton ✖ correspondant.

43.4 Configurer un compte mail

Pour ajouter un nouveau compte mail existant à Thunderbird, cliquer sur ☰ pour afficher le menu de Thunderbird et aller dans ✚ *Nouveau* → *Compte courrier existant...*. Un onglet intitulé *Configurez votre adresse électronique existante* s'ouvre alors.

Il faut alors renseigner les deux premiers champs demandés : *Votre nom complet* et *Adresse électronique*. Le nom qu'on mettra dans le champ *Votre nom complet* apparaîtra dans les emails envoyés, et sera donc lisible par nos correspondantes *et par les intermédiaires* faisant transiter nos messages. Il est donc suggéré de remplir page 218 ce champ avec le pseudonyme qu'on voudra voir apparaître dans les en-têtes de nos emails.

Il n'est par contre pas nécessaire de remplir le champ *Mot de passe*, à moins que l'on souhaite que Thunderbird mémorise notre mot de passe de connexion à ce compte mail (auquel cas il est vivement conseillé d'avoir au préalable défini un *mot de passe principal* en suivant la procédure décrite cette page précedemment).

Une fois les informations saisies, cliquer sur *Continuer*.

Si *Configuration trouvée chez le fournisseur de messagerie* s'affiche, la configuration automatique a fonctionné. Si Thunderbird est incapable de trouver la configuration automatiquement, il est possible de chercher la documentation officielle de notre hébergeur mail pour vérifier les paramètres spécifiques pour IMAP, POP et SMTP. Si

cette information est introuvable sur le site web du hébergeur mail, il est possible de trouver le contact mail des admins et de la leur demander.

L'assistant nous propose alors de choisir entre deux protocoles, IMAP ou POP. Sélectionner celui qui nous convient le mieux et cliquer sur *Terminé*, puis fermer l'onglet de configuration du compte en cliquant sur le bouton ✖ correspondant.

page 292

Thunderbird est désormais prêt à réceptionner les messages. On peut répéter la procédure si l'on souhaite ajouter des comptes mail supplémentaires. Sinon, on peut passer directement à la partie suivante, consacrée à la configuration avancée de Thunderbird.

43.5 Configuration avancée de Thunderbird

Une fois Thunderbird configuré pour un compte mail, on peut vouloir optimiser sa configuration, pour qu'elle nous soit plus agréable ou pour qu'elle réduise les risques en termes de sécurité informatique.

Pour cela, cliquer sur ☰ pour afficher le menu de Thunderbird puis choisir *Paramètres des comptes*. Nous n'allons pas faire un tour exhaustif des options de configuration, mais de quelques-unes qui nous semblent utiles.

43.5.1 Durée de conservation des messages

Tout d'abord, si l'on a choisi d'utiliser le protocole POP, dans la partie *Paramètres serveur*, on peut décider de la durée après laquelle les messages seront supprimés des serveurs après rapatriement. Cela est bien sûr sans grande garantie et dépend notamment de notre hébergeur mail : nous ne pouvons qu'espérer qu'il efface véritablement nos données.

page 42

43.5.2 Ports utilisés

Enfin, si l'on rencontre des problèmes pour l'envoi ou la réception des emails il est possible que les ports des protocoles utilisés ne soient pas les bons avec les réglages par défaut. Si c'est le cas, il faudra faire des modifications en fonction des informations de configuration disponibles chez notre hébergeur mail.

On accède à ces paramètres en cliquant sur l'adresse mail dans la colonne de gauche, puis sur *Paramètres du compte* en haut à droite. Un nouvel onglet s'ouvre où on peut modifier le port SMTP dans la section *Serveur sortant (SMTP)* tout en bas. Cliquer alors sur *Modifier le serveur SMTP...* et enfin modifier le numéro du *Port* et mettre celui fourni par notre hébergeur. Pour modifier le serveur entrant, retourner dans la colonne de gauche, sélectionner les *Paramètres serveur* et modifier le *Port* correspondant au *Type de serveur* choisi auparavant (IMAP ou POP3).

43.5.3 Utiliser un service onion

Si notre hébergeur mail a mis en place des services onion, on peut alors configurer Thunderbird pour qu'il utilise les adresses onion correspondantes.

page 266

Pour les trouver, il faut chercher les informations qui ont été publiées par notre hébergeur mail : les adresses onion et leurs ports pour les services SMTP, IMAP et/ou POP. Cette information n'est pas toujours facilement accessible. Il est possible de faire une recherche sur Internet avec les mots-clés suivants : « *configuration smtp onion service [et le nom de l'hébergeur mail]* ». Si on ne trouve pas, on peut aussi demander directement aux personnes qui administrent cet hébergement mail.

Une fois les adresses onion trouvées :

- il faut configurer le routage en oignon dans Thunderbird comme vu précédemment.

page 329

- Pour le serveur POP ou IMAP : dans la colonne de gauche en dessous du compte mail concerné, il faut aller dans la section *Paramètres serveur* puis remplacer l'adresse indiquée dans *Nom du serveur* par l'adresse du service onion POP ou IMAP.
- Pour modifier l'adresse du serveur SMTP, il faut aller dans la section *Serveur sortant (SMTP)* tout à la fin de la colonne de gauche, sélectionner le compte mail concerné, cliquer sur *Modifier…* et enfin remplacer l'adresse du serveur SMTP dans *Nom du serveur* par l'adresse du service onion SMTP.

Chapitre 44

Utiliser le chiffrement OpenPGP dans Thunderbird

Le standard Internet [1] OpenPGP est un format de cryptographie qui permet notamment d'effectuer et de vérifier des signatures numériques ainsi que de chiffrer et de déchiffrer des messages ou des fichiers.

Nous allons ici détailler l'usage d'OpenPGP dans Thunderbird pour gérer des clés et chiffrer ou signer des messages. Cependant, certains usages d'OpenPGP qui ne sont pas possibles dans Thunderbird sont traités dans le chapitre suivant. page 343

44.1 Créer une paire de clés

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quinze minutes à une heure.

Cet outil détaille la création et une partie de la gestion d'une paire de clés de chiffrement. page 249 Il est bon de rappeler quelques notions de base à toujours avoir à l'esprit :

- Les clés de chiffrement n'utilisent pas toutes le même algorithme. Nous avons parlé du chiffrement RSA mais il en existe plusieurs autres. page 251
- L'algorithme ne définit pas strictement la taille de la clé, on peut choisir de faire varier cette dernière afin de jouer sur les niveaux de sécurité.
- Certaines clés ont des dates d'expiration à laquelle elles périment, d'autres n'en ont pas.

44.1.1 Générer la paire de clés

Tout d'abord, avant de générer une paire de clés OpenPGP, il faut avoir défini un *mot de passe principal*, comme détaillé dans le chapitre précédent. page 330 Cette phrase de passe est demandée à chaque ouverture de Thunderbird. Elle sert à restreindre l'accès aux mots de passe enregistrés, mais aussi à la clé privée qu'on va créer.

Afin de créer notre nouvelle paire de clés, dans Thunderbird, cliquer sur ≡ → *Outils* → *Gestionnaire de clés OpenPGP*. Choisir *Génération* → *Nouvelle paire de clés*. Une fenêtre *Ajouter une clé OpenPGP personnelle pour […]* s'ouvre. Vérifier que l'*Identité* sélectionnée correspond à l'identité contextuelle utilisée, ainsi que l'adresse électronique qui lui est associée. page 243

Il est conseillé de choisir une date d'*Expiration de la clé*. Si c'est la première fois que l'on crée une paire de clés, on choisira une date d'expiration comprise entre un an et

1. Wikipédia, 2014, *Standard Internet* [https://fr.wikipedia.org/wiki/Standard_Internet].

deux ans par exemple. Afin de ne pas oublier de renouveler sa clé à temps, il peut être de bon goût de noter quelque part cette date d'expiration.

Dans les *Paramètres avancés*, le *Type de clé* par défaut est *RSA*. Il est conseillé de sélectionner *ECC (courbe elliptique)* à cet endroit, car les algorithmes cryptographiques correspondants offrent une sécurité équivalente aux clés de type RSA tout en étant plus efficaces. Néanmoins, il reste tout à fait possible d'utiliser une clé de type RSA.

Si l'on choisit l'option *RSA* comme *Type de clé*, la *Taille de la clé* proposée par défaut, 3072 bits, est considérée comme sûre jusqu'au-delà de 2030[2] ; mais si l'on souhaite protéger ses communications plus fortement ou plus longtemps, il est conseillé de choisir la taille de clé la plus élevée disponible, à savoir 4096 bits. Dans le cas d'une clé de type ECC, par contre, il n'est pour l'instant pas possible de choisir la taille de la clé.

Une fois les paramètres de la clé sélectionnés, cliquer sur *Générer la clé* puis sur *Confirmer*.

Cela peut être presque instantané ou prendre plusieurs minutes. C'est le moment de faire bouger sa souris, d'utiliser son clavier ou encore d'utiliser le disque dur si cela est possible, afin d'aider son ordinateur à générer des données aléatoires. Celles-ci sont nécessaires au processus de génération de la clé[3].

Une fois cette opération terminée, notre clé apparaîtra en gras dans le *Gestionnaire de clés OpenPGP*. Il peut arriver que la clé ne soit pas visible. Dans ce cas, monter ou descendre dans la liste de clés.

44.1.2 Sauvegarder sa clé privée

Cette étape de création de clés effectuée, il est bon de penser à la manière de sauvegarder notre paire de clés, et en particulier notre clé privée : celle-ci étant secrète, il s'agit de ne pas la laisser traîner n'importe où. La clé privée doit être uniquement accessible à la personne supposée y avoir accès. Le mieux est de conserver cette paire de clés sur un volume chiffré, que celui-ci soit une clé USB, un disque dur interne ou externe, ou la persistance de Tails.

page 145

page 116

Si la sauvergarde se fait sur la persitance de Tails, c'est bien de prévoir une sauvegarde de son système live :

page 151

- Depuis le *Gestionnaire de clés OpenPGP*, sélectionner la clé et choisir *Fichier* → *Sauvegarder une ou des clés secrètes dans un fichier*.
- Choisir où placer le fichier et son nom, puis cliquer sur *Enregistrer*.
- Choisir alors une phrase de passe pour protéger la sauvegarde de la clé secrète. Ça peut être la même phrase de passe que celle choisie précédemment comme mot de passe principal de Thunderbird, car c'est pratiquement la même information qu'on protège : notre clé secrète. Cliquer alors sur *OK*.
- Une boîte de dialogue doit confirmer que *Les clés ont été correctement enregistrées*. On peut la *Fermer*.
- Vérifier alors que la sauvegarde est bien placée en lieu sûr.

page 330

44.1.3 Conserver un certificat de révocation à l'abri

Si des adversaires mettent la main sur notre clé privée, ou simplement si on la perd, il est nécessaire de la *révoquer*, afin que nos correspondantes soient au courant qu'il

2. Agence nationale de la sécurité des systèmes d'information, 2020, *Mécanismes cryptographiques – Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques* [https://www.ssi.gouv.fr/uploads/2021/03/anssi-guide-mecanismes_crypto-2.04.pdf], p. 20.

3. Zvi Gutterman, Benny Pinkas, Tzachy Reinman, 2006, *Analysis of the Linux Random Number Generator* [http://www.pinkas.net/PAPERS/gpr06.pdf] (en anglais).

ne faut plus utiliser la clé publique correspondante. On utilise pour cela un *certificat de révocation*.

Le certificat de révocation se présente sous la forme d'un fichier ou de quelques lignes de texte, qu'il nous faudra stocker dans un endroit sûr, par exemple sur une clé USB chiffrée, chez une personne de confiance ou sur un papier bien caché. En effet, toute personne qui a accès à ce fichier peut révoquer notre clé publique, et donc nous empêcher de communiquer de manière chiffrée.

Lorsque l'on crée une paire de clés OpenPGP, Thunderbird crée automatiquement un certificat de révocation, mais il le cache dans son dossier de configuration. Pour le trouver :

- lancer le logiciel Fichiers : appuyer sur la touche ⊞ (⌘ sur un Mac), taper `fich` puis cliquer sur *Fichiers* ;
- dans le panneau de gauche, aller dans *Dossier personnel* ;
- cliquer sur ☰ puis *Afficher les fichiers cachés* ;
- ouvrir le dossier `.thunderbird` ;
- trouver le dossier au nom bizarre qui finit par `.default` (par exemple `7u6xu6tq.default-default` ou `profile.default`) et l'ouvrir ;
- le certificat de révocation de notre clé privée se trouve dans un fichier dont le nom commence par l'identifiant [4] de la clé et finit par `_rev.asc` (par exemple `0xC7BF166A096820DA_rev.asc`) ;
- double-cliquer sur ce fichier pour l'ouvrir.

Selon notre choix, on pourra ensuite :

- le sauvegarder cliquant sur ☰ puis *Enregistrer sous…* et choisir un nom de fichier clair. Par exemple `Certificat de révocation pour la clé 0xC7BF166A096820DA.asc` ;
- l'imprimer en cliquant sur l'icône d'imprimante, à partir du menu ☰.

Si notre clé privée venait à être compromise, on utiliserait ce certificat pour révoquer la clé publique associée. page 340

44.1.4 Configurer le chiffrement pour un compte de messagerie

La cryptographie asymétrique permet de chiffrer des emails ou de les signer, ou les deux. Il faut donc configurer le compte de messagerie que l'on veut utiliser avec la paire de clés que l'on vient de générer.

Pour cela :

- cliquer sur ☰ pour afficher le menu de Thunderbird puis ouvrir *Paramètres des comptes* ;
- sélectionner d'un clic la section *Chiffrement de bout en bout* du compte mail à éditer ;
- choisir la clé correspondant à notre identité contextuelle à la place de *Aucune. Ne pas utiliser OpenPGP pour cette identité.*

Plus bas, dans les *Paramètres par défaut pour l'envoi de messages*, il est possible de choisir différentes options.

Par défaut, les emails ne sont pas chiffrés, et il faut activer manuellement le chiffrement pour chaque email. On peut *Activer le chiffrement pour les nouveaux messages* ; il faudra alors désactiver le chiffrement pour écrire à une personne qui n'utilise pas OpenPGP.

On peut aussi cocher la case *Signer les messages non chiffrés* afin de signer tous les emails que nous enverrons depuis ce compte (les messages chiffrés étant toujours

4. En cas de doute, on peut retrouver l'identifiant de notre clé (sans le `0x` initial) dans le *Gestionnaire de clés OpenPGP* de Thunderbird, en face de l'identité contextuelle correspondante.

signés par défaut). Cela permet aux destinataires d'authentifier tous les emails, y compris ceux qui ne sont pas chiffrés. Cela leur montre aussi qu'on utilise OpenPGP. Attention cependant, car cela prouve cryptographiquement que l'email a été envoyé par une personne détentrice de la clé secrète correspondante, ce qui n'est pas toujours souhaitable.

44.2 Exporter et partager notre clé publique

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quelques minutes.

Pour nous envoyer des emails chiffrés et pour vérifier la signature de nos emails, nos correspondantes doivent disposer de notre clé publique. Mais avant de l'utiliser, il leur faudra avoir aussi vérifié l'empreinte de cette clé.

page 338

44.2.1 Envoyer notre clé publique par email

Il est possible de transmettre notre clé publique par email. Dans la fenêtre de rédaction d'un message, cliquer sur le bouton ⌄ juste à droite du bouton 📎 *Joindre* puis cocher *Ma clé publique OpenPGP*. Notre clé sera alors automatiquement ajoutée en pièce jointe au moment de l'envoi de l'email.

44.2.2 Publier sa clé publique sur les serveurs de clés

page 243

Si l'existence de l'identité contextuelle à laquelle correspond la clé n'est pas elle-même confidentielle, on pourra publier notre clé publique sur un serveur de clés, afin que quiconque désirant nous envoyer des emails chiffrés puisse la télécharger à cette fin.

Commencer par exporter sa clé publique dans un fichier, qui pourra ensuite tout autant être partagé sur un serveur ou via une clé USB chiffrée. La procédure est la même sous Tails ou avec une Debian chiffrée :

- Dans Thunderbird, cliquer sur ☰ → *Outils* → *Gestionnaire de clés OpenPGP*.
- Sélectionner la clé OpenPGP que l'on souhaite exporter ; dans le menu, cliquer sur *Fichier* → *Exporter une ou des clés publiques vers un fichier* ; choisir un emplacement d'exportation et un nom de fichier, puis cliquer sur *Enregistrer*.

Publier ensuite la clé sur un serveur de clé :

page 315

- Ouvrir le Navigateur Tor et saisir l'adresse https://keys.openpgp.org/.
- Cliquer sur *upload* (*téléverser* en français).
- Cliquer sur *Browse...* (*Parcourir...* en français) et choisir le fichier dans lequel on a exporté sa clé publique.
- Cliquer sur *Upload*. Une page confirme la bonne réception de la clé.
- Visiter le lien reçu dans l'email de confirmation (en le copiant-collant dans la barre d'adresse du Navigateur Tor) pour confirmer que c'est bien nous qui sommes derrière l'adresse mail associée à la clé publiée.

44.2.3 Obtenir l'empreinte d'une clé

Si l'on transmet notre clé publique par un moyen non authentifié, il est nécessaire de faire parvenir à notre correspondante l'empreinte (voir page 54) de notre clé par un moyen authentifié, afin qu'elle s'assure qu'il sagit bien de la bonne clé appartenant à la bonne personne.

Pour obtenir l'empreinte de notre clé :

- Dans Thunderbird, cliquer sur ☰ → *Outils* → *Gestionnaire de clés OpenPGP*.
- Double-cliquer sur notre clé OpenPGP pour afficher les *Propriétés de la clé*.

- Noter ou copier l'empreinte de la clé pour la partager de manière sécurisée.

Des méthodes pour partager l'empreinte par un canal sûr et vérifier l'authenticité de la clé (voir page suivante) sont expliquées plus loin.

44.3 Importer, vérifier et exporter des clés publiques

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : De quelques minutes à une demi-heure.

Les clés publiques d'autres personnes nous servent à chiffrer les emails que nous leur envoyons et à vérifier l'authenticité des messages qu'elles ont signés.

Pour obtenir ces clés publiques, il faut les importer. Avant de les utiliser, il faut vérifier leur authenticité afin de s'assurer que nous avons la bonne clé publique de la bonne personne. Il est aussi parfois utile d'exporter ces clés dans un fichier pour les utiliser dans d'autres logiciels.

cette page page suiv. page 339

44.3.1 Importer une clé publique

Le but de ce chapitre est d'importer une clé OpenPGP, que nous utiliserons pour vérifier des signatures numériques ou pour chiffrer des messages. La procédure est la même sous Tails ou avec une Debian chiffrée.

Importer une clé ne signifie pas avoir vérifié qu'elle appartient bien à la propriétaire supposée. Nous verrons dans la section suivante qu'il faut pour cela effectuer d'autres opérations, comme étudier ses signatures ou son empreinte numérique.

page suiv.

Dans Thunderbird, l'import de clé passe par le *Gestionnaire de clés OpenPGP*. Pour y accéder, cliquer sur ☰ → *Outils* → *Gestionnaire de clés OpenPGP*.

Si l'on dispose de la clé dans un fichier

Dans le *Gestionnaire de clés OpenPGP*, cliquer sur *Fichier* → *Importer une ou des clés publiques depuis un fichier*. Dans la fenêtre qui s'ouvre, sélectionner le fichier contenant la clé, puis cliquer sur *Ouvrir*.

On peut alors passer à l'étape de confirmation de l'import (voir page suivante).

Si l'on veut chercher la clé en ligne

Toujours dans le *Gestionnaire de clés OpenPGP*, cliquer sur *Serveur de clés* → *Rechercher des clés en ligne*.

Dans la fenêtre qui s'ouvre alors, taper l'adresse mail ou l'identifiant correspondant à la clé recherchée, par exemple `guide@boum.org`, `0x326F9F67250B0939`[5] ou encore `D4874FA4F6B688DC0913C9FD326F9F67250B0939`, et choisir *OK*. Il faudra bien vérifier l'empreinte par la suite, comme on verra un peu plus tard.

Il est à noter que si l'on a précédemment configuré Thunderbird pour utiliser le routage en oignon, il faut aussi que le Navigateur Tor soit lancé pour que la recherche de clés en ligne puisse fonctionner.

page 329

5. Il s'agit de l'identifiant court d'une clé, qui n'est pas suffisant pour sélectionner de manière unique une clé. Riseup, 2017, *Bonnes pratiques pour l'utilisation d'OpenPGP* [https://help.riseup.net/fr/security/message-security/openpgp/best-practices#ne-vous-fiez-pas-%C3%A0-lidentifiant-de-cl%C3%A9].

Confirmation de l'import

Une fois que Thunderbird a trouvé la clé (dans le fichier indiqué ou bien en ligne, selon la procédure utilisée juste avant), une fenêtre de résultats s'ouvre, qui affiche l'identifiant complet de la clé et les adresses mail associées. Si c'est bien la clé qu'on souhaite importer, choisir *Acceptée (non vérifiée)* et cliquer sur *OK*.

Si l'importation se passe bien, une fenêtre *Clés correctement importées* s'ouvre, avec un résumé des information sur la clé. La fermer avec *OK*.

La clé importée devrait maintenant être visible dans le *Gestionnaire de clés OpenPGP*. **Il reste nécessaire de vérifier son authenticité**.

44.3.2 Vérifier l'authenticité d'une clé publique

page 253 Lors de l'utilisation de la cryptographie asymétrique, il est crucial de s'assurer que l'on dispose de la véritable clé publique de notre correspondante. Sinon, on s'expose

page 254 à une attaque du monstre du milieu.

On devra tout d'abord choisir une méthode pour s'assurer que l'on dispose de la bonne clé publique. On indiquera ensuite à Thunderbird notre confiance en cette clé.

page 63 En fonction des exigences de notre modèle de menace et de nos possibilités, on pourra choisir différentes façons pour vérifier l'authenticité d'une clé publique. Admettons qu'on doive vérifier l'authenticité de la clé publique d'Ana.

Se transmettre la clé par un canal sûr...

Lorsque c'est possible, le plus simple est de se passer en main propre, à l'aide d'une clé USB par exemple, le fichier contenant la clé publique. Ana exporte (voir page ci-contre) alors sa clé publique vers un fichier, qu'elle stocke sur une clé USB éventuellement chiffrée (voir page 145) qu'elle nous donne ensuite. On importera (voir page précédente) ensuite directement la clé publique d'Ana à partir de ce fichier.

...ou se transmettre l'empreinte par un canal sûr.

page 53 L'un des inconvénients de la méthode précédente est qu'elle nécessite de se passer un fichier informatique par un moyen sûr. Cela n'est pas toujours possible. Heureusement, ce n'est en fait pas nécessaire : il suffit d'obtenir, par un moyen sûr, une somme de contrôle de la clé publique, qu'on appelle « empreinte » (ou « fingerprint » en anglais).

Ana peut ainsi publier sa clé publique sur Internet, par exemple sur son blog ou sur un serveur de clés. De notre côté, nous téléchargeons cette clé de façon non authentifiée, puis on vérifie que l'empreinte de la clé correspond à celle qu'Ana nous a fait parvenir de façon *authentifiée*. Pour voir l'empreinte de la clé d'Ana obtenue depuis Internet, il faudra l'importer (voir page précédente) dans le *Gestionnaire de clés OpenPGP*, puis double-cliquer sur sa clé.

Que gagnons-nous à utiliser cette méthode ? Au lieu de devoir se faire passer un fichier, il est suffisant de se transmettre une ligne de caractères comme celle-ci :

```
A490 D0F4 D311 A415 3E2B B7CA DBB8 02B2 58AC D84F
```

Par exemple, Ana, qui est une personne bien organisée, peut avoir en permanence sur elle un exemplaire de l'empreinte de sa clé publique écrite sur un bout de papier. Il nous suffit alors de la croiser pour qu'elle nous la passe : pas besoin d'ordinateur ni de clé USB.

Si l'on ne peut pas rencontrer Ana, elle pourra aussi nous envoyer cette empreinte par courrier postal, et on pourra l'appeler pour qu'elle nous la lise par téléphone. La vérification sera moins bonne qu'en se voyant directement, mais il reste plus difficile

pour des adversaires de nous envoyer un courrier postal avec sa clé et de répondre au numéro de téléphone d'Ana en nous lisant son empreinte, tout en imitant sa voix.

Ça se complique encore si on ne connaît pas Ana. Dans ce cas, il nous faudra faire confiance à des personnes qui prétendent la connaître. Encore une fois, il n'y a pas de recette magique, mais combiner différents moyens de vérification permet de compliquer la tâche de possibles adversaires souhaitant monter une « attaque du monstre du milieu » : il nous est possible de demander à plusieurs personnes qui prétendent connaître Ana plutôt qu'à une seule, d'utiliser plusieurs moyens de communication différents, *etc.*

page 254

Enregistrer la confiance dans une clé

Une fois qu'on a établi une confiance en la clé d'Ana, il est utile d'informer Thunderbird qu'il peut faire confiance à cette clé.

Pour cela, ouvrir le *Gestionnaire de clés OpenPGP* de Thunderbird en cliquant sur ☰ → *Outils* → *Gestionnaire de clés OpenPGP*.

Une fois la clé d'Ana repérée dans la fenêtre principale, double-cliquer dessus pour afficher les détails de la clé. Vérifier que c'est la bonne clé, par exemple en vérifiant son empreinte. Dans l'onglet *Votre acceptation*, choisir alors *Oui, j'ai vérifié en personne que l'empreinte de cette clé est correcte*, puis valider en cliquant sur *OK*.

Thunderbird sait maintenant qu'on a confiance en la clé d'Ana.



Pour aller plus loin…

Dans Thunderbird, quand on fait confiance à une clé, notre choix reste sur notre ordinateur seulement. Pour faire fonctionner la toile de confiance (voir page 257), le protocole OpenPGP permet de signer une clé et de rendre cette signature publique, ce qui permet à n'importe quelle utilisatrice de la toile de confiance de profiter des vérifications qu'on a faites.

Pour l'instant, il n'est pas possible de faire de signature publique avec l'interface de Thunderbird. C'est possible uniquement dans le trousseau OpenPGP du système, auquel on peut accéder avec l'application *Kleopatra* par exemple.

44.3.3 Exporter une clé publique dans un fichier

Le but de cet outil est d'exporter une clé OpenPGP, par exemple pour pouvoir l'utiliser avec un autre logiciel.

Le fichier créé lors de cette opération contiendra la clé publique nécessaire pour chiffrer des messages destinés à l'identité correspondante ou vérifier des signatures faites par cette identité.

Pour cela :

- Dans Thunderbird, cliquer sur ☰ → *Outils* → *Gestionnaire de clés OpenPGP*.
- Sélectionner la clé OpenPGP que l'on souhaite exporter ; dans le menu, cliquer sur *Fichier* → *Exporter une ou des clés publiques vers un fichier* ; choisir un emplacement d'exportation et un nom de fichier, puis cliquer sur *Enregistrer*.

44.4 Gestion de sa paire de clé : la prolonger, en changer, la révoquer

Lors de la création de notre paire de clés, nous avons pu choisir une date d'expiration. Avant que la paire de clés expire, il est possible de modifier la date d'expiration afin de prolonger sa validité. Cependant, les technologies évoluent et on peut vouloir changer de paire de clés et transitionner vers une nouvelle paire. Enfin, il arrive parfois qu'une clé privée soit compromise et que l'on doive donc la révoquer.

cette page
cette page
cette page

44.4.1 Prolonger sa paire de clés

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quelques minutes.

Dans le cas où notre paire de clés va expirer mais qu'il n'y a pas de raison de transitionner vers une nouvelle paire, on peut prolonger sa validité.

Pour cela :

- dans Thunderbird, cliquer sur ☰ → *Outils* → *Gestionnaire de clés OpenPGP* ;
- double-cliquer sur notre paire de clés ;
- cliquer sur *Modifier la date d'expiration* ;
- sélectionner *La clé expirera dans* et choisir un nombre de mois, par exemple douze ou vingt-quatre mois (un ou deux ans) ;
- cliquer sur *OK* pour valider.

Nous voilà reparties pour une autre saison en compagnie de notre paire de clés !

44.4.2 Effectuer la transition vers une nouvelle paire de clés

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quinze minutes à une heure.

Avant que notre paire de clés expire, ou lorsque des avancées dans le domaine de la cryptographie nous obligent à utiliser des clés plus sûres, il nous faudra créer une nouvelle paire de clés.

On suivra pour cela l'outil créer une paire de clés (voir page 333).

On exportera alors notre nouvelle clé publique (voir page précédente) et on la fera parvenir aux personnes avec lesquelles on communique.

Quelque temps plus tard, on pourra révoquer notre ancienne clé (voir cette page).

Cependant, nous conserverons bien notre ancienne clé privée, afin de pouvoir déchiffrer les messages reçus précédemment, chiffrés avec l'ancienne clé publique.

44.4.3 Révoquer une paire de clés

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quinze à trente minutes.

Dans le cas où notre propre paire de clés est compromise, par exemple si on a perdu notre système ou qu'on soupçonne qu'il a été piraté, l'enjeu est d'arriver à le faire savoir à nos correspondantes. Ainsi elles seront au courant que la clé n'est plus de confiance et pourront arrêter de l'utiliser.

Pour cela, nous utiliserons le certificat de révocation créé précédemment (voir page 334) avec notre paire de clé.

⚠ **Attention** : les instructions qui suivent révoqueront de manière irréversible notre clé. À utiliser seulement en cas de besoin !

Préparer le certificat de révocation

Il faut tout d'abord retrouver le certificat de révocation sauvegardé lors de la création de notre paire de clés. On l'avait alors stocké dans un endroit sûr, par exemple sur une clé USB chiffrée, chez une personne de confiance ou sur un papier bien caché. page 334

Si il était sur un bout de papier, il faut créer un fichier contenant les informations du certificat de révocation :

- lancer l'Éditeur de texte : appuyer sur la touche ⊞ (⌘ sur un Mac), taper `gedi` puis cliquer sur *Éditeur de texte* ;
- dans le document, taper précisément la partie qui commence par `-----BEGIN PGP PUBLIC KEY BLOCK-----` et finit par `-----END PGP PUBLIC KEY BLOCK-----` ;
- Enregistrer le fichier au format `.asc`, par exemple `revocation.asc`.

Sinon, si on avait sauvegardé le fichier contenant le certificat de révocation sur un autre support (clé USB chiffrée ou autre), il faut tout d'abord :

- ouvrir ce fichier en faisant un clic droit dessus, puis *Ouvrir avec une autre application* ;
- dans *Choisir une application*, choisir *Éditeur de texte* et cliquer sur *Sélectionner* ;
- enlever le caractère : qui se situe au tout début de la ligne `-----BEGIN PGP PUBLIC KEY BLOCK-----` ;
- cliquer sur *Enregistrer* et fermer l'éditeur de texte.

Le certificat de révocation est maintenant prêt. Nous pouvons alors l'utiliser pour révoquer notre clé.

Révoquer notre clé OpenPGP

Pour pouvoir révoquer une clé OpenPGP, il faut avoir la clé publique correspondante. Si notre clé privée a été compromise, il est possible qu'on n'ait plus accès au système sur lequel elle était. Par conséquent, si l'on ne dispose pas de la clé publique que l'on veut révoquer, on va commencer par l'importer (voir page 337).

Il faut ensuite importer le certificat de révocation.

Dans Thunderbird, ouvrir le *Gestionnaire de clés OpenPGP* en cliquant sur ☰ → *Outils* → *Gestionnaire de clés OpenPGP*. Puis :

- choisir *Fichier* → *Importer une ou des révocations depuis un fichier* ;
- séléctionner le fichier contenant le certificat de révocation, puis cliquer sur *Ouvrir* ;
- la clé révoquée apparaît alors grisée.

Si l'on avait publié notre clé publique sur un serveur de clés, il faut maintenant y publier la clé révoquée, en suivant la recette ci-dessous.

Publier la clé publique révoquée

Si notre clé publique avait au préalable été publiée sur un serveur de clés, le mieux est de publier à nouveau notre clé révoquée, pour que notre clé publique y soit désormais également révoquée, permettant ainsi à toutes nos correspondantes d'en être averties en la mettant à jour depuis le serveur de clés.

Pour cela, que ce soit sous Tails ou dans une Debian, suivre la recette pour publier sa clé publique sur les serveurs de clés. page 336

Une fois cette synchronisation effectuée, il reste à le faire savoir à nos correspondantes.

Prévenir nos correspondantes de la révocation de notre clé

L'étape la plus importante de la révocation de notre clé est de prévenir nos correspondantes afin qu'elles n'utilisent plus cette clé.

Pour cela, on peut, au choix :

- leur envoyer par email le certificat de révocation, qu'elles pourront alors importer afin de révoquer notre clé publique dans leur trousseau de clés ;
- exporter notre clé publique révoquée (voir page 339) puis la leur envoyer par email, afin qu'elles puissent l'importer à nouveau ;
- leur demander de mettre à jour notre clé révoquée depuis le serveur de clés sur lequel on l'aura publiée ; pas de recette toute faite pour ça, entre leur envoyer un email chiffré, le leur faire savoir de vive voix, *etc.*

44.4.4 Révoquer la clé publique d'une correspondante

Si l'une de nos correspondantes nous a fait savoir que sa paire de clés était compromise et qu'elle l'a révoquée, il nous faut mettre à jour sa clé sur notre ordinateur afin que Thunderbird prenne cette révocation en compte.

Pour cela :

- si notre correspondante nous a envoyé le certificat de révocation de sa clé, suivre la recette ci-dessus afin d'importer ce certificat ;
- si elle nous a envoyé sa clé publique révoquée, il faut alors l'importer à nouveau (voir page 337) ;
- si elle a publié sa clé publique révoquée sur un serveur de clés, il nous faut alors mettre à jour notre copie de la clé en l'important à nouveau depuis le serveur de clés (voir page 337).

44.5 Chiffrer et/ou signer ses emails dans Thunderbird

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quelques minutes.

page 329 Une fois Thunderbird démarré et configuré :

- cliquer sur le bouton *Écrire* afin de débuter la rédaction d'un nouveau message ;
- une fenêtre *Rédaction* s'ouvre, dans laquelle on va rédiger notre email ;
- si l'on souhaite chiffrer l'email, cliquer sur le bouton *Chiffrer*, s'il n'est pas déjà sélectionné (le cadenas est barré lorsque le chiffrement est désactivé) ; on peut aussi activer le chiffrement de l'email en cliquant dans le menu *Sécurité* → *Chiffrer* ;

page 252

- si l'on souhaite signer numériquement l'email, cliquer sur *OpenPGP* → *Signer numériquement* ou dans le menu *Sécurité* → *Signer numériquement* ;
- si notre correspondante ne dispose pas déjà de notre clé publique, il est possible de la joindre à l'email automatiquement en cliquant sur le bouton juste à droite du bouton *Joindre* puis en cochant *Ma clé publique OpenPGP* ;
- une fois notre email terminé, cliquer sur *Envoyer*.

Si la personne qui reçoit l'email utilise aussi Thunderbird, elle verra dans la barre d'en-tête de l'email un bouton *OpenPGP* avec :

- un cadenas fermé si l'email est chiffré ;
- un cachet si l'email est signé.

En cliquant sur ce bouton, des détails sur le chiffrement et la signature s'affichent.

Si la personne ne possède pas la clé privée pour laquelle le message a été chiffré, un message *La clé secrète nécessaire pour déchiffrer ce message n'est pas disponible* apparaîtra en lieu et place du corps de l'email.

Chapitre 45

Utiliser le chiffrement OpenPGP dans le bureau

Le standard Internet [1] OpenPGP est un format de cryptographie qui permet notamment d'effectuer et de vérifier des signatures numériques ainsi que de chiffrer et de déchiffrer des messages ou des fichiers.

La plupart des outils de ce guide utilisent OpenPGP en utilisant autant que possible Thunderbird pour gérer les clés OpenPGP, car son interface est plus ergonomique et que c'est comme ça que ça fonctionne dans Tails. Cependant, certains usages d'OpenPGP qui ne sont pas possibles dans Thunderbird restent regroupés dans ce chapitre.

page 333

Thunderbird et le reste de notre environnement de bureau (que l'on utilise Debian ou Tails) utilisent deux trousseaux de clés OpenPGP différents. Les clés que l'on voudrait avoir dans les deux trousseaux doivent être manuellement exportées de l'un puis importées dans l'autre.

45.1 Importer une clé dans le trousseau du bureau

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quelques minutes.

L'objectif de cet outil est d'importer une clé OpenPGP dans le trousseau OpenPGP du bureau. Il est à noter que ce trousseau n'est pas le même que celui de Thunderbird.

Si l'on utilise une Debian chiffrée, il faut tout d'abord installer le logiciel *Kleopatra*, qui contient l'outil de gestion de clés que l'on va utiliser. Si l'on utilise Tails, ce paquet est déjà installé.

page 119

page 134

Au lancement de Kleopatra, il se peut que celui-ci affiche un message d'avertissement intitulé *Résultats des tests automatiques de Kleopatra* et dans lequel la *Vérification de la configuration de scdaemon* apparaît comme ayant échoué. Ce n'est pas grave, mais ça peut vite devenir perturbant. Afin que ce message ne s'affiche pas à chaque démarrage de Kleopatra, on peut décocher la case *Lancer ces tests au démarrage* puis cliquer sur *Continuer*. Une autre possibilité est d'installer le paquet `scdaemon`, quand bien même il ne nous sera pas utile.

page 135

45.1.1 Importer une clé secrète

Il peut être nécessaire d'importer sa clé secrète (appelée aussi clé privée) dans le trousseau du bureau, par exemple pour signer ou déchiffrer des fichiers, ou encore pour signer des clés publiques.

1. Wikipédia, 2014, *Standard Internet* [https://fr.wikipedia.org/wiki/Standard_Internet].

page 334 Si elle se trouve dans le trousseau de Thunderbird, commencer par sauvegarder sa clé secrète, sous la forme d'un fichier avec l'extension `.asc`.

Il faut ensuite l'importer dans le trousseau du bureau en double-cliquant dessus.

Une fenêtre *Vous avez importé une clé privée* apparaît. Le logiciel demande *Est-ce bien votre propre clé ?*. Répondre *Oui*.

Une nouvelle fenêtre *Résultat de l'importation du certificat* apparaît. Valider avec *OK*.

45.1.2 Importer une clé publique

Importer une clé publique dans le trousseau OpenPGP du bureau permet de vérifier des signatures numériques ou de chiffrer des fichiers.

Si on a reçu ou téléchargé un fichier contenant la clé (avec l'extension `.asc` ou `.pub`, généralement), il suffit de double-cliquer sur le fichier pour l'importer dans le trousseau du bureau.

page 339 Si on veut récupérer une clé qu'on a déjà dans le trousseau de Thunderbird, on aura besoin de l'exporter pour obtenir le fichier contenant la clé à importer. On pourra ensuite importer cette clé en double-cliquant sur le fichier.

Une boîte de dialogue *Vous avez importé un nouveau certificat (clé publique)* apparaît. Le logiciel propose de nous guider pour certifier son authenticité. C'est une bonne idée de choisir *Oui* si l'on dispose d'une clé secrète (car celle-ci est nécessaire afin de signer la clé que l'on vient d'importer).

45.2 Signer une clé

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quelques minutes.

L'objectif de cet outil est de signer une clé OpenPGP dans le trousseau OpenPGP du bureau. Il est à noter que ce trousseau n'est pas le même que celui de Thunderbird.

page 119 Si l'on utilise une Debian chiffrée, il faut tout d'abord installer le logiciel *Kleopatra*, qui contient l'outil de gestion de clés que l'on va utiliser. Si l'on utilise Tails, ce paquet est déjà installé.

page 134

Au lancement de Kleopatra, il se peut que celui-ci affiche un message d'avertissement intitulé *Résultats des tests automatiques de Kleopatra* et dans lequel la *Vérification de la configuration de scdaemon* apparaît comme ayant échoué. Ce n'est pas grave, mais ça peut vite devenir perturbant. Afin que ce message ne s'affiche pas à chaque démarrage de Kleopatra, on peut décocher la case *Lancer ces tests au démarrage* puis cliquer sur *Continuer*. Une autre possibilité est d'installer le paquet `scdaemon`, quand bien même il ne nous sera pas utile.

page 135

page 338 Mais pourquoi signer une clé ? Mettons que l'on ait au préalable vérifié l'authenticité de la clé d'Ana en suivant la recette décrite au chapitre précédent. Il est alors utile d'informer OpenPGP qu'il peut faire confiance à cette clé. Cette opération s'appelle *signer* la clé. Kleopatra parle aussi de *certifier* la clé. La procédure est la même sous Tails ou avec une Debian chiffrée.

page préc. Pour pouvoir signer une clé, il faut tout d'abord avoir importé notre clé secrète dans Kleopatra.

Ensuite :

- Aller dans *Kleopatra*, en appuyant sur la touche ⊞ (⌘ sur un Mac) pour ouvrir la vue d'ensemble des activités, puis en tapant `kleo` et enfin en cliquant sur le logiciel correspondant.

- Si la clé que l'on souhaite signer n'est pas présente, l'importer. page ci-contre
- Une fois la clé d'Ana repérée dans la fenêtre principale, double-cliquer dessus pour afficher les détails de la clé. Vérifier que c'est la bonne clé, par exemple en vérifiant son empreinte (qui se trouve en bas de la fenêtre).
- Cliquer ensuite sur *Certifier*.
- Saisir la phrase de passe de notre clé secrète dans la boîte de dialogue qui s'affiche le cas échéant [2].
- Une fenêtre *La certification a réussi* doit s'afficher. Cliquer sur *OK*.

OpenPGP sait maintenant qu'on a confiance en la clé d'Ana.

45.3 Vérifier une signature numérique

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quelques minutes.

L'objectif de cet outil est de vérifier l'authenticité d'un fichier disposant d'une signature numérique OpenPGP. page 252

Si l'on utilise une Debian chiffrée, il faut tout d'abord installer le logiciel *Kleopatra*, qui contient l'outil de gestion de clés que l'on va utiliser. Si l'on utilise Tails, ce paquet est déjà installé. page 119 page 134

Au lancement de Kleopatra, il se peut que celui-ci affiche un message d'avertissement intitulé *Résultats des tests automatiques de Kleopatra* et dans lequel la *Vérification de la configuration de scdaemon* apparaît comme ayant échoué. Ce n'est pas grave, mais ça peut vite devenir perturbant. Afin que ce message ne s'affiche pas à chaque démarrage de Kleopatra, on peut décocher la case *Lancer ces tests au démarrage* puis cliquer sur *Continuer*. Une autre possibilité est d'installer le paquet `scdaemon`, quand bien même il ne nous sera pas utile. page 135

Afin de pouvoir vérifier la signature numérique d'un fichier, il faut au préalable avoir trouvé la clé publique de la personne ou du groupe qui a produit cette signature, puis avoir importé cette clé dans le trousseau du bureau. En général, la clé publique nécessaire à la vérification de la signature est téléchargeable depuis le site web où l'on a récupéré le fichier et sa signature. Si la signature a été réalisée par une de nos correspondantes, c'est sa clé publique qu'il faudra utiliser pour vérifier la signature. page 343

Cette signature se présente sous la forme d'un petit fichier, portant généralement le même nom que le fichier contenant les données signées, avec une extension `.sign`, `.sig` ou `.asc` en plus.

45.3.1 Effectuer la vérification de signature

- Si le fichier de signature finit avec l'extension `.sign`, faire un clic-droit dessus et choisir *Renommer…*. Enlever le `n` de la fin pour qu'il finisse en `.sig`.
- Aller dans *Kleopatra*, en appuyant sur la touche ⊞ (⌘ sur un Mac) pour ouvrir la vue d'ensemble des activités, puis en tapant `kleo` et enfin en cliquant sur le logiciel correspondant.
- Dans la barre d'outils en haut de la fenêtre, cliquer sur *Déchiffrer/vérifier…*.
- Dans la fenêtre qui s'ouvre alors, choisir le fichier de signature.

Une fenêtre *Vérifier les fichiers* s'affiche. Elle contient la progression, puis le résultat de la vérification.

2. Si on a déjà tapé notre phrase de passe peu de temps avant, elle n'est pas redemandée. OpenPGP la garde en mémoire pendant dix à trente minutes.

45.3.2 Interpréter le résultat de la vérification

- *Signature valable* signifie que le fichier est bien signé par la clé précisée sous *Avec le certificat*.
- *Impossible de vérifier la donnée* peut signifier deux choses :
  - Si la boîte de résultat indique *Avec le certificat* suivi du nom d'une clé de notre trousseau, cela signifie que le fichier est bien signé par la clé précisée, mais qu'on n'a pas confirmé l'authenticité de cette clé. Si on souhaite la vérifier, suivre l'outil correspondant (voir page 338), puis signer la clé (voir page 344).
  - Si la boîte de résultat indique *Avec le certificat indisponible* suivi de l'identifiant d'une clé, cela signifie que le fichier est bien signé mais que la clé publique nécessaire pour vérifier la signature n'est pas dans le trousseau OpenPGP du bureau. Dans ce cas, trouver la clé et l'importer dans le trousseau du bureau (voir page 343) avec le bouton *Importer*.
- *Signature non valable* signifie que le fichier vérifié ne correspond pas à celui qui a été signé. On peut avoir téléchargé le mauvais fichier, le mauvais fichier de signature, ou être victime d'une attaque. Dans tous les cas, on ne peut pas considérer le fichier téléchargé comme étant authentique.

45.4 Signer des données

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quelques minutes.

page 252 L'objectif de cet outil est de signer numériquement des données. Cela peut notamment permettre à d'autres personnes d'authentifier un message, un document, un logiciel, *etc.*, comme provenant bien de nous. Cet outil nécessite d'avoir préalablement créé une paire de clés et d'en avoir importé la clé secrète dans le trousseau OpenPGP du bureau.

page 333

page 343

45.4.1 Signer du texte

Cette méthode ne fonctionne que pour signer du texte. Pour signer un autre type de fichier suivre la section suivante.

Pour signer du texte :

- Aller dans *Kleopatra*, en appuyant sur la touche ⊞ (⌘ sur un Mac) pour ouvrir la vue d'ensemble des activités, puis en tapant `kleo` et enfin en cliquant sur le logiciel correspondant.
- Dans la barre d'outils en haut de la fenêtre, cliquer sur *Bloc-notes*.
- Dans l'onglet *Bloc-notes*, taper ou coller le texte à signer.
- Aller dans l'onglet *Destinataires*.
- Cocher *Signer en tant que* (en choisissant la bonne identité contextuelle si on en a plusieurs).
- Décocher *Chiffrer pour moi* et *Chiffrer pour d'autres*.
- Cliquer sur *Bloc-notes Signer*.
- Saisir la phrase de passe de notre clé secrète dans la boîte de dialogue qui s'affiche le cas échéant [3].

Le texte signé se trouve dans l'onglet *Bloc-notes*. On peut le copier-coller vers un fichier.

3. Si on a déjà tapé notre phrase de passe peu de temps avant, elle n'est pas redemandée. OpenPGP la garde en mémoire pendant dix à trente minutes.

45.4.2 Signer un fichier

Pour pouvoir signer un ficher, il faut d'abord importer notre clé secrète dans le trousseau du bureau. page 343

Pour signer le fichier :

- Aller dans *Kleopatra*, en appuyant sur la touche ⊞ (⌘ sur un Mac) pour ouvrir la vue d'ensemble des activités, puis en tapant `kleo` et enfin en cliquant sur le logiciel correspondant.
- Dans la barre d'outils en haut de la fenêtre, cliquer sur *Signer/chiffrer…*.
- Choisir le fichier à signer et cliquer sur *Ouvrir*.
- Cocher *Signer en tant que* (en choisissant la bonne identité contextuelle si on en a plusieurs).
- Décocher *Chiffrer pour moi* et *Chiffrer pour d'autres*.
- Cliquer sur *Signer*.
- Saisir la phrase de passe de notre clé secrète dans la boîte de dialogue qui s'affiche le cas échéant[4].
- Un message *Succès de la signature* doit s'afficher.

Le processus de signature peut prendre jusqu'à plusieurs minutes en fonction de la taille du fichier et de la puissance de l'ordinateur qu'on utilise. Une fois la signature terminée, elle se présente sous la forme d'un petit fichier ayant le même nom que le fichier original, mais se terminant par l'extension `.sig`, situé au même endroit que le fichier original. À chaque fois l'on transmettra le fichier original, il faudra lui joindre ce fichier de signature afin que les destinataires puissent en vérifier l'authenticité. De plus, afin que les destinataires puissent vérifier notre signature, elles auront besoin d'avoir importé au préalable notre clé publique.

45.5 Chiffrer des données

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quelques minutes.

L'objectif de cet outil est de chiffrer numériquement des données. Cela peut servir notamment à transmettre un ou plusieurs documents confidentiels sur un support non chiffré qui contient déjà des données, ou bien encore à mettre en ligne ces mêmes documents. page 249

Si l'on utilise une Debian chiffrée, il faut tout d'abord installer le logiciel *Kleopatra*, qui contient l'outil de gestion de clés que l'on va utiliser. Si l'on utilise Tails, ce paquet est déjà installé. page 119 page 134

Au lancement de Kleopatra, il se peut que celui-ci affiche un message d'avertissement intitulé *Résultats des tests automatiques de Kleopatra* et dans lequel la *Vérification de la configuration de scdaemon* apparaît comme ayant échoué. Ce n'est pas grave, mais ça peut vite devenir perturbant. Afin que ce message ne s'affiche pas à chaque démarrage de Kleopatra, on peut décocher la case *Lancer ces tests au démarrage* puis cliquer sur *Continuer*. Une autre possibilité est d'installer le paquet `scdaemon`, quand bien même il ne nous sera pas utile. page 135

Pour commencer :

- Aller dans *Kleopatra*, en appuyant sur la touche ⊞ (⌘ sur un Mac) pour ouvrir la vue d'ensemble des activités, puis en tapant `kleo` et enfin en cliquant sur le logiciel correspondant.
- Dans la barre d'outils en haut de la fenêtre, cliquer sur *Signer/chiffrer…*.

4. Si on a déjà tapé notre phrase de passe peu de temps avant, elle n'est pas redemandée. OpenPGP la garde en mémoire pendant dix à trente minutes.

- Choisir le fichier à chiffrer et cliquer sur *Ouvrir*.

On peut choisir de chiffrer le fichier pour une ou plusieurs clés publiques, ou d'utiliser une phrase de passe.

45.5.1 Chiffrer des données avec une phrase de passe

Si on utilise une phrase de passe, il faudra la partager avec les personnes qui devront déchiffrer les données.

- Décocher *Signer en tant que*.
- Décocher aussi *Chiffrer pour moi* et *Chiffrer pour d'autres*.
- Cocher *Chiffrer avec un mot de passe*.
- Cliquer sur *Chiffrer*.
- Entrer la *Phrase secrète* deux fois puis cliquer sur *OK*.
- Un message *Succès du chiffrement* doit s'afficher.

Le processus de chiffrement peut prendre jusqu'à plusieurs minutes en fonction de la taille du fichier et de la puissance de l'ordinateur qu'on utilise. Une fois l'opération de chiffrement terminée, le fichier chiffré apparaît à côté du fichier original non chiffré, avec l'extension `.gpg` à la fin de son nom.

45.5.2 Chiffrer des données avec une ou plusieurs clés publiques

Si l'on chiffre avec des clés publiques, il est nécessaire d'avoir dans son trousseau les clés publiques de *toutes* les personnes avec qui l'on souhaite partager le fichier. Si ce n'est pas déjà fait, il faudra les importer.

page 343

- Décocher *Signer en tant que*, à moins que l'on ne souhaite aussi signer le fichier numériquement. Il faudra alors choisir la bonne identité contextuelle (si on en a plusieurs).
- Si l'on souhaite aussi chiffrer le fichier pour notre propre clé cocher aussi *Chiffrer pour moi*.
- Cocher *Chiffrer pour d'autres* et choisir les clés des personnes avec qui on souhaite partager le fichier.
- Cliquer sur *Chiffrer* (ou *Signer/chiffrer*).
- Un message *Succès du chiffrement* (ou *Succès de la signature et du chiffrement*) doit s'afficher.

Le processus de chiffrement peut prendre jusqu'à plusieurs minutes en fonction de la taille du fichier et de la puissance de l'ordinateur qu'on utilise. Une fois l'opération de chiffrement terminée, le fichier chiffré apparaît à côté du fichier original non chiffré, avec l'extension `.gpg` à la fin de son nom.

45.6 Déchiffrer des fichiers

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quelques minutes.

L'objectif de cet outil est de déchiffrer un fichier chiffré numériquement. Cela peut servir notamment à lire des documents confidentiels transmis de façon chiffrée.

page 249

Si l'on utilise une Debian chiffrée, il faut tout d'abord installer le logiciel *Kleopatra*. Si l'on utilise Tails, ce paquet est déjà installé.

page 119
page 134

⚠ Au lancement de Kleopatra, il se peut que celui-ci affiche un message d'avertissement intitulé *Résultats des tests automatiques de Kleopatra* et dans lequel la *Vérification de la configuration de scdaemon* apparaît comme ayant échoué. Ce n'est pas grave, mais ça peut vite devenir perturbant. Afin que ce message ne s'affiche pas à chaque démarrage de Kleopatra, on peut décocher la case *Lancer ces tests au démarrage* puis cliquer sur *Continuer*. Une autre possibilité est d'installer le paquet `scdaemon`, quand bien même il ne nous sera pas utile.

page 135

⚠ **Attention** : toujours déplacer le fichier à déchiffrer jusqu'à l'emplacement où l'on souhaite le stocker sous sa forme déchiffrée. Par exemple, si le fichier chiffré est stocké sur une clé USB non chiffrée, il sera très important de le déplacer avant de le déchiffrer, sinon le fichier déchiffré se retrouvera en clair sur la clé USB.

Pour déchiffrer le fichier :

- Aller dans *Kleopatra*, en appuyant sur la touche ⊞ (⌘ sur un Mac) pour ouvrir la vue d'ensemble des activités, puis en tapant `kleo` et enfin en cliquant sur le logiciel correspondant.
- Dans la barre d'outils en haut de la fenêtre, cliquer sur *Déchiffrer/vérifier…*.
- Choisir le fichier à déchiffrer et cliquer sur *Ouvrir*.
- Saisir la phrase de passe partagée ou la phrase de passe de notre clé secrète dans la boîte de dialogue qui s'affiche le cas échéant [5].
- Si le fichier est non seulement chiffré mais aussi signé, le résultat de la vérification de la signature s'affiche de la même façon que lorsqu'on vérifie une simple signature. Sinon, un message indique le *Succès du déchiffrement.*

page 346

- Cliquer sur *Tout enregistrer* pour enregistrer le fichier déchiffré.

5. Si on a déjà tapé notre phrase de passe peu de temps avant, elle n'est pas redemandée. OpenPGP la garde en mémoire pendant dix à trente minutes.

Chapitre 46

Utiliser la messagerie instantanée avec OTR

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Une demi-heure à une heure.

L'objectif de cet outil est de dialoguer avec une personne en utilisant la messagerie instantanée avec chiffrement et authentification. On va pour cela utiliser le protocole OTR [1], qui permet d'ajouter chiffrement, authentification et confidentialité persistante à nombre de protocoles de messagerie instantanée.

page 258

Afin de pouvoir utiliser OTR pour dialoguer avec notre correspondante, il faut qu'elle aussi active OTR dans son logiciel de messagerie instantanée. Pour cela, elle pourra donc aussi suivre les indications présentées dans ce chapitre.

46.1 Installer le client de messagerie instantanée Pidgin

On va utiliser pour cela le client de messagerie Pidgin. En effet, il dispose d'une bonne prise en charge du chiffrement OTR. De plus, il permet d'utiliser différents protocoles de messagerie instantanée, comme XMPP [2] ou IRC [3], parmi d'autres [4]. Ce logiciel est installé dans le système live Tails, mais seuls les protocoles XMPP et IRC y sont pris en charge, les autres étant difficiles à anonymiser. Sur une Debian chiffrée, il faudra commencer par installer les paquets `pidgin` ainsi que `pidgin-otr`.

page 119

page 135

46.2 Lancer Pidgin

Pour ouvrir le logiciel de messagerie instantanée, ouvrir la vue d'ensemble des activités en appuyant sur la touche ⊞ (⌘ sur un Mac), en tapant ensuite `pidgin`, enfin en cliquant sur *Messagerie internet Pidgin*.

1. Wikipédia, 2014, *Off-the-Record Messaging* [https://fr.wikipedia.org/wiki/Off-the-Record_Messaging].

2. Wikipédia, 2014, *Extensible Messaging and Presence Protocol* [https://fr.wikipedia.org/wiki/XMPP].

3. Wikipédia, 2014, *Internet Relay Chat* [https://fr.wikipedia.org/wiki/Internet_Relay_Chat]. IRC accepte normalement une utilisation sans création de compte préalable. Aujourd'hui la plupart des serveurs IRC refusent les connexions *via* Tor ; à l'exception de quelques serveurs, dont OFTC [https://www.oftc.net/Tor/] (en anglais). L'utilisation d'IRC n'est pas expliquée dans ce guide.

4. Pour une liste exhaustive des protocoles pris en charge par Pidgin, se référer à leur site web [https://www.pidgin.im/] (en anglais).

46.3 Configurer un compte de messagerie

Lorsqu'on ouvre Pidgin et qu'aucun compte de messagerie n'est configuré, une fenêtre propose d'ajouter un nouveau compte.

Pour configurer un nouveau compte, cliquer sur le bouton *Ajouter...*.

Une fenêtre *Ajouter un compte* s'ouvre. Si l'on dispose déjà d'un compte de messagerie instantanée, fournir les informations nécessaires concernant ce compte, en commençant par sélectionner le *Protocole* que l'on souhaite utiliser.

46.4 Créer un compte de messagerie instantanée XMPP

Tout comme pour un compte mail, un identifiant et une phrase de passe (voir page 103) seront nécessaires. Pour éviter d'utiliser tout le temps la même ou bien de risquer de l'oublier, il est possible d'utiliser un gestionnaire de mots de passe (voir page 355).

On peut utiliser des serveurs communautaires où l'inscription est libre. Par exemple, des listes de serveurs XMPP libres sont disponibles sur le site jabberfr.org[5].

Une fois le compte créé chez le serveur choisi et les informations nécessaires[6] entrées dans la fenêtre de Pidgin, cocher la case *Créer ce nouveau compte sur le serveur*.

46.5 Chiffrer la connexion au serveur

Par défaut, Pidgin configure le nouveau compte pour qu'il chiffre la communication avec le serveur.

page 255 Si le certificat est bien signé par une autorité de certification, la connexion se déroulera sans problème, et Pidgin enregistrera le certificat du serveur dans sa configuration.

Si le certificat du serveur n'est pas signé, ou que pour une raison ou une autre Pidgin n'arrive pas à vérifier son authenticité, il est alors nécessaire de mettre en place les

page 323 mêmes techniques que lors de la vérification d'un certificat dans son navigateur web,

page 254 sans quoi des adversaires pourraient usurper l'identité du serveur.

Dans ce cas, lors de notre première connexion, Pidgin affichera une fenêtre demandant si l'on veut *Accepter le certificat pour [exemple.org] ?* Il expliquera également la raison pour laquelle il n'a pas voulu accepter le certificat (*Le certificat est auto-signé. Il ne peut être vérifié automatiquement*, si par exemple le certificat n'est pas signé par une autorité de certification). En cliquant sur *Voir le certificat...*, Pidgin affichera

page 53 l'empreinte numérique de celui-ci, nous permettant de le vérifier.

46.6 Activer le plugin OTR (*Off-the-Record*)

page 251 Il faut maintenant activer le chiffrement de bout en bout avec OTR.

Dans le menu *Outils* de Pidgin, cliquer sur *Plugins*. Trouver la ligne « Messagerie confidentielle 'Off-the-Record' » et cocher la case correspondante pour activer le plugin. Il est possible en cliquant sur *Configurer le plugin* de choisir certaines options telles que *Ne pas archiver les conversations d'OTR*.

---

5. Une liste de serveurs XMPP communautaires [https://wiki.jabberfr.org/Serveurs#Serveurs_communautaires]. Si la création de compte échoue avec un serveur, ne pas hésiter à essayer avec un autre serveur.

6. Pour plus de détails sur les informations à renseigner sur Pidgin et créer donc le compte XMPP, voir le site de Linuxpedia [https://www.linuxpedia.fr/doku.php/internet/pidgin-jabber].

46.7 Mettre en place une conversation privée

46.7.1 Ajouter un contact ou rejoindre un salon de discussion

En fonction de notre situation, nous allons soit devoir ajouter le contact auquel nous souhaitons parler dans Pidgin, soit devoir rejoindre le salon dans lequel le trouver.

Ajouter un contact

Pour ajouter un contact dans Pidgin, cliquer sur *Contacts* dans la barre de menu du logiciel et aller à *Ajouter un contact...*. Remplir ensuite les informations correspondantes de notre contact et cliquer sur *Ajouter*.

Notre contact va alors recevoir une demande d'autorisation d'ajout à notre liste de contacts. Une fois que notre contact aura accepté la demande d'ajout, il sera possible de commencer à discuter.

Rejoindre un salon de discussion

Si au contraire l'on veut rejoindre un salon de discussion dans lequel se trouvera sans doute la personne avec qui l'on veut converser, cliquer sur *Contacts* dans la barre de menu du logiciel et aller à *Rejoindre une discussion...*. De la même manière, remplir les informations nécessaire et enfin cliquer sur *Discuter*.

Il ne sera malheuresement pas possible d'utiliser le chiffrement de bout en bout dans les salons avec Pidgin. En effet, le protocole OTR ne fonctionne pas pour les salons avec Pidgin.

46.7.2 Commencer une conversation privée

Pour commencer une conversation privée, double-cliquer sur un nom se trouvant dans la colonne de droite de la fenêtre d'un salon de discussion où l'on se trouve ou bien cliquer sur le nom de notre partenaire dans la fenêtre principale de Pidgin. Une fenêtre de conversation s'ouvre. Cliquer alors sur le menu *OTR* → *Commencer une conversation privée*.

Si c'est la première fois qu'on utilise OTR avec ce compte, Pidgin va alors générer une clé privée et afficher une fenêtre *Génération de la clé privée*. Cette clé est unique pour un compte donné. Si l'on possède plusieurs comptes de messagerie instantanée, on aura donc plusieurs clés. Lorsqu'elle affiche que la génération de cette clé est *effectuée*, on peut fermer cette fenêtre en cliquant sur *Valider*.

Pidgin affiche alors *Ana n'a pas encore été authentifiée. Vous devriez authentifier ce contact*. Cela signifie que notre conversation est chiffrée, mais que une adversaire pourrait se faire passer pour Ana. Pour être sûr de parler avec Ana, il faut authentifier la conversation.

page 254

46.7.3 Authentifier une correspondante

Pour authentifier une correspondante, il faut soit s'être mis d'accord au préalable sur un secret, soit disposer d'un moyen de communication autre que la messagerie instantanée, que l'on considère comme sûr. Ce moyen peut être une conversation de vive voix, un email chiffré, *etc.*

OTR propose trois façons d'authentifier un contact :

- par question-réponse : on définit une question et sa réponse. La question étant ensuite posée à notre correspondante ;
- avec un secret partagé : un secret connu uniquement des deux interlocutrices est demandé afin de vérifier qu'on dialogue bien avec la personne escomptée ;

- grâce à la vérification manuelle de l'empreinte : on vérifie que l'empreinte de la clé de la personne avec qui l'on s'apprête à avoir une conversation chiffrée est la même que celle qui nous a été fournie par un moyen *authentifié*.

Une fois les secrets, les questions-réponses ou les empreintes échangés, cliquer sur le menu *OTR* → *Authentifier contact*. Choisir la méthode d'authentification en-dessous de *Comment désirez-vous authentifier votre contact ?*, puis répondre aux questions. Enfin, cliquer sur *Authentifier*.

Si l'authentification est réussie, le statut de la conversation devient *Privé*, ce qui signifie qu'elle est non seulement chiffrée, mais aussi authentifiée.

page 116

Si l'on utilise un système non-live ou que l'on a activé la persistance de Pidgin dans Tails, cette étape d'authentification n'est à effectuer qu'une fois pour toutes pour un contact donné.

46.7.4 Terminer une conversation

Une fois notre dialogue terminé, cliquer sur le menu *OTR* → *Terminer la conversation privée*. Cela efface la clé de chiffrement temporaire générée pour cette conversation de la mémoire vive de l'ordinateur. Même si des adversaires obtenaient nos clés privées, elles n'auraient pas accès à la clé leur permettant de déchiffrer la conversation *a posteriori*.

Chapitre 47

Gérer des mots de passe

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Quinze à trente minutes.

Lorsqu'on crée une adresse mail, un compte sur un site web, *etc.*, ce compte est en général protégé par un mot de passe.

Il est important de ne pas utiliser le même mot de passe pour différents comptes ou différentes utilisations.

Il est important aussi de ne pas utiliser le même mot de passe pour des identités contextuelles différentes, afin que la compromission de l'une d'entre elles n'entraîne pas la compromission des autres.

page 243

Il existe deux bonnes écoles pour la gestion des mots de passe :

- choisir et retenir une phrase de passe différente pour chaque usage ;
- générer aléatoirement des mots de passe et les enregistrer dans un *gestionnaire de mots de passe* qui, lui, est protégé par une bonne phrase de passe que l'on retiendra.

47.1 Choisir une bonne phrase de passe

La première école a l'avantage de ne nécessiter aucun support de stockage : on a toujours ses phrases de passe avec soi. Pour l'appliquer, consulter choisir une bonne phrase de passe (voir page 103).

Toutefois, lorsqu'on multiplie les comptes ainsi que les identités contextuelles, cela peut faire beaucoup de phrases de passe à retenir.

47.2 Utiliser un gestionnaire de mots de passe

La seconde méthode peut alors nous être utile. Dans la pratique, on aura une phrase de passe à retenir par identité, notre gestionnaire de mots de passe se chargeant ensuite de conserver les différents mots de passe liés à cette identité. Cela peut se faire sur un système Debian chiffré comme sur un système *live* amnésique en utilisant la persistance.

page 119
page 113

47.2.1 Installer le gestionnaire de mots de passe

page 116

On va utiliser le gestionnaire de mots de passe KeePassXC. S'il n'est pas installé sur notre système, installer le logiciel (voir page 134) *KeePassXC*. Le logiciel KeePassXC est installé par défaut dans Tails.

47.2.2 Lancer KeePassXC

Appuyer sur la touche [⊞] ([⌘] sur un Mac) pour ouvrir la vue d'ensemble des activités puis taper `keepassxc` et cliquer sur l'icône *KeePassXC*.

47.2.3 Créer et enregistrer une base de données de mots de passe

Une base de données de mots de passe est un ensemble de mots de passe qui seront stockés dans une même base de données KeePassXC et chiffrés par la phrase de passe associée.

Si on choisit d'utiliser KeePassXC dans Tails, il faudra au préalable activer la persistance (voir page 116) et activer l'option *Données personnelles*.

Au lancement de KeePassXC, il faut tout d'abord créer une nouvelle base de données de mots de passe et l'enregistrer pour l'utiliser lors de futures sessions de travail. Pour créer une nouvelle base de données de mots de passe, choisir *Créer une nouvelle base de données*.

Pour stocker la base de données de mots de passe nouvellement créée afin de l'utiliser lors de prochaines sessions de travail, renseigner un nom et optionnellement une description. Cliquer ensuite sur *Continuer*.

On peut ensuite régler les *Paramètres de chiffrement* de la base de données, qui pourront aussi être modifiés ultérieurement. Cliquer ensuite sur *Continuer*.

Ensuite, il faut choisir une phrase de passe qui servira à déchiffrer la base de données de mots de passe. Étant donné que cette base de données va contenir certains de nos mots de passe, il est important de choisir une bonne phrase de passe (voir page 103). Spécifier deux fois cette phrase de passe dans la boîte de texte *Mot de passe*.



Pour aller plus loin…

On peut aussi décider d'*Ajouter une protection supplémentaire* en générant ou en indiquant un *Fichier clé* qui comprend des octets aléatoires ; par contre, il faudra garder ce fichier secret et ne pas le perdre : sans le fichier clé, il sera impossible d'accéder à notre base de données.

L'intérêt d'une telle protection est de pouvoir stocker ce fichier clé sur un autre support que notre base de données de mots de passe, comme par exemple sur une clé USB chiffrée que l'on garderait en sécurité. En plus de notre phrase de passe, il nous faudra donc avoir cette clé USB avec nous pour pouvoir accéder aux mots de passe contenus dans la base de données ; et une personne qui parviendrait à deviner notre phrase de passe ne pourra pas tout de même pas déchiffrer la base de données sans notre fichier clé.

Par contre, le risque de cette technique est celui d'égarer la clé USB contenant le fichier clé : si nous n'avions pas fait de copie de sauvegarde de notre fichier clé, nous serions alors dans l'impossibilité totale d'accéder à nos mots de passe.

Cliquer sur *Terminer* une fois terminé.

Il faut ensuite indiquer à KeePassXC l'emplacement où enregistrer cette base de données. Si l'on utilise Tails, l'emplacement par défaut est le dossier *Persistent* : laisser tel quel, afin que la base de données soit bien enregistrée dans le volume persistant de notre Tails. Sinon, choisir l'emplacement désiré pour sauvegarder la base de données. Cliquer sur *Enregistrer*.

Étant donné qu'elle va contenir certains de nos mots de passe, penser à régulièrement sauvegarder une copie (voir page 151) de cette base de données.

47.2.4 Générer et enregistrer un mot de passe aléatoire

KeePassXC permet également de générer des mots de passe aléatoires plus robustes que des mots de passe dont on pourrait se souvenir.

Dans KeePassXC, cliquer sur *Entrées* puis ⊕ *Nouvelle entrée…*. Remplir les champs utiles. Pour le champ *Mot de passe*, cliquer sur le bouton en forme de dé (⚄), situé sur la droite de la zone de saisie.

Une fenêtre contenant différentes options de génération de mot de passe s'ouvre.

Parmi les options disponibles, il est préférable d'utiliser des lettres minuscules, majuscules et des chiffres, puis d'augmenter le nombre de caractères du mot de passe (au minimum 32), puisqu'on n'aura pas à retenir ce dernier. Les caractères spéciaux sont, quant à eux, parfois sources de problèmes avec certains logiciels ou sites web.

Pour choisir les caractères souhaités, cliquer sur les boutons correspondants dans la section *Types de caractères*. Lorsqu'un bouton est surligné (en vert), le mot de passe va être généré avec ce type de caractères ; lorsque le bouton est désélectionné (c'est-à-dire lorsqu'il apparaît en gris clair), les caractères correspondants ne seront pas utilisés dans le mot de passe généré. Cliquer sur l'œil barré 👁 à droite du mot de passe généré permet de rendre visible le mot de passe et ainsi de pouvoir vérifier ce qui est généré.

L'indicateur d'*Entropie* permet de mesurer la robustesse du mot de passe généré. Elle est directement liée aux types de caractères sélectionnés et à la longueur du mot de passe. L'entropie minimale recommandée est de 128 bits.

Cliquer ensuite sur *Confirmer le mot de passe*, puis sur *OK*.

47.2.5 Restaurer et déverrouiller la base de données de mots de passe

Lorsqu'on veut utiliser une base de données de mots de passe préalablement enregistrée, il nous faut la déverrouiller. Pour cela, lancer KeePassXC. En général, s'il la trouve, KeePassXC nous propose automatiquement d'ouvrir la dernière base de données de mots de passe utilisée. Il indique alors *Déverrouiller la base de données KeePassXC*, suivi du nom du fichier correspondant. S'il s'agit bien de la base de données que l'on souhaite ouvrir, on peut sauter le paragraphe suivant.

Dans le cas contraire, s'il ne s'agit pas de la bonne base de données de mots de passe, ou si *KeePassXC* ne nous propose pas automatiquement de base de données à déverrouiller, aller dans le menu *Base de données*, cliquer sur *Ouvrir une base de données…*, puis naviguer à travers la liste des dossiers pour trouver le fichier *.kdbx* correspondant à la base de données que l'on souhaite ouvrir. Sélectionner ce fichier puis cliquer sur *Ouvrir*.

Que KeePassXC ait automatiquement trouvé la base de données à ouvrir ou qu'on la lui ait indiquée nous-même, il nous demande alors de la déverrouiller. Pour cela, dans le champ *Saisissez le mot de passe*, saisir la phrase de passe que l'on avait configurée à la création de la base de données. Si l'on avait défini des identifiants supplémentaires pour protéger la base de données (tels qu'un fichier clé, par exemple), il faut aussi les indiquer à cet endroit. Enfin, cliquer sur *OK*.

Si la phrase de passe est incorrecte, le message d'erreur suivant apparaît :



> Erreur de lecture de la base de données : Des identifiants invalides ont été fournis, veuillez ressayer.
>
> Si le problème se reproduit, le fichier de la base de données pourrait être corrompu.

47.2.6 Utiliser un mot de passe enregistré

Après avoir restauré et déverrouillé la base de données de mots de passe, on peut utiliser les mots de passe qui y sont enregistrés.

Il existe deux méthodes pour utiliser un mot de passe enregistré : de façon manuelle en copiant/collant l'identifiant et le mot de passe ou en utilisant la saisie automatique.

Saisie automatique

KeePassXC peut enregistrer des « associations de fenêtres », qui lient une entrée avec le nom d'une fenêtre et une séquence de saisie automatique, c'est-à-dire les informations de l'entrée à taper directement dans cette fenêtre.

Pour ce faire, la fenêtre où l'on souhaite faire une saisie automatique doit être ouverte, par exemple le navigateur web avec la page de connexion à notre boîte mail.

Ensuite, rechercher dans KeePassXC l'entrée que l'on souhaite utiliser pour cette fenêtre, puis double-cliquer dessus afin de pouvoir la modifier. Les champs *Nom d'utilisateur* et *Mot de passe* doivent être remplis. Dans la colonne de gauche, aller dans *Saisie automatique*. S'assurer que la case *Activer la saisie automatique pour cette entrée* est bien cochée. Cliquer alors sur le symbole ✚ en bas de la section *Associations de fenêtres* pour créer une nouvelle association. Il est alors possible de choisir la fenêtre à laquelle on veut associer l'entrée dans le menu déroulant *Titre de la fenêtre* à droite. Pour finir, cliquer sur *OK* : le paramétrage est terminé.

Dorénavant, il est possible d'utiliser la séquence de saisie automatique en positionnant le focus [1] dans la fenêtre où l'on souhaite saisir nos identifiants, par exemple le champs courriel dans le navigateur de notre boîte mail. Passer ensuite dans KeePassXC sur l'entrée correspondante et lancer la saisie automatique. Ça se fait avec la combinaison de touches Ctrl + Maj + V [2] ou en cliquant sur l'icône représentant un clavier ⌨ et intitulée *Saisir automatiquement* dans la barre d'outils en haut.



Attention : le remplissage automatique permet aussi de faire de belles boulettes, comme coller son mot de passe dans une fenêtre de messagerie instantanée… et envoyer le message automatiquement. Il faut donc faire très attention à l'endroit où on place le curseur avant d'exécuter le remplissage automatique.

Il est possible que cette méthode de saisie automatique ne fonctionne pas pour tous les types d'interfaces. Dans ce cas, il faut passer à la saisie manuelle.

Saisie manuelle

Dans KeePassXC, pour récupérer l'identifiant dans le presse-papier, aller sur l'entrée que l'on souhaite utiliser, puis faire clic-droit et choisir *Copier le nom d'utilisateur* ou effectuer la combinaison de touches Ctrl + B. Ensuite, coller le contenu du presse-papier dans le champ de la fenêtre où saisir l'identifiant. Procéder de la même manière pour copier le mot de passe en refaisant un clic-droit sur l'entrée et en choisissant *Copier le mot de passe*, ou bien en effectuant Ctrl + C, pour enfin le coller dans le champ d'entrée du mot de passe.

---

1. L'endroit où vont apparaître les prochains caractères lors de la frappe au clavier.
2. Maj est la notation pour la touche majuscule, également notée en anglais Shift. Cette touche peut être trouvée sous diverses notations selon les claviers : ⇧, ⇧ Shift, SHIFT ou encore ⇧ Maj.

Chapitre 48

Utiliser OnionShare

Les logiciels évoluent, c'est pourquoi il est vivement conseillé d'utiliser la version la plus à jour de cet outil, qui est disponible sur le site web https://guide.boum.org/.

Durée : Cinq à dix minutes.

Pour mettre à disposition d'autres personnes un ou plusieurs fichiers, il est possible de les faire héberger sur un serveur web. page 319

Cependant, on n'a aucune raison *a priori* de faire confiance aux personnes ou administrations qui s'occupent de ces serveurs.

Si l'on préfére ne pas nous en remettre à une tierce partie, il est donc possible d'héberger soi-même les documents à partager, qui plus est, *via* un service onion. page 266

Cela a entre autre l'avantage de fortement protéger la localisation du serveur d'hébergement, qui ici est notre propre ordinateur. Il ne faudra pour autant pas oublier que ce système d'anonymisation n'est pas infaillible. page 267

Pour faire cela, nous utiliserons le logiciel OnionShare qui permet en une poignée de clics de créer un service onion, et d'y héberger les fichiers de notre choix.

48.1 Utiliser OnionShare dans Tails

OnionShare est installé par défaut dans Tails. On peut suivre la documentation officielle de Tails, qui est disponible à partir de n'importe quel support de Tails, même sans connexion à Internet.

Commencer par démarrer Tails. Sur le bureau, double-cliquer sur l'icône *Documentation de Tails*. Dans l'index qui s'ouvre, chercher la section *Internet non censuré et anonyme* et cliquer sur la page *Partager des fichiers avec OnionShare* sous *Applications Internet*. C'est celle-ci qu'il s'agira de suivre. page 115

48.2 Utiliser OnionShare dans Debian

Commencer par installer le logiciel *OnionShare* si ce n'est déjà fait. Pour le lancer, ouvrir la vue d'ensemble des Activités en appuyant sur la touche (sur un Mac), puis taper `onion` et cliquer sur *OnionShare*. page 131

OnionShare fera une connexion *via* Tor. On pourra se laisser guider par le logiciel en choisissant le fichier que l'on souhaite partager.


BLEEDING
BLOODY
MURDER

Qui parle ?

Malheureusement, nous n'avons pas de réponse simple à offrir à cette question, mais nous souhaitons en dire quelques mots.

Tout d'abord, nous tenons à la possibilité de publier un livre de manière anonyme et ce, pour plusieurs raisons. L'une d'elles, que nous avons développée dans la préface, est qu'à la question « Rien à cacher ? », nous répondons à l'unisson « si ! ». L'anonymat est donc d'abord une manière de se protéger. De plus, nous choisissons de ne pas nous mettre en avant individuellement, afin d'écarter le *qui* du devant de la scène et de laisser le *quoi* sous les projecteurs.

Ensuite, depuis les premières parutions de ce *guide*, le nombre de personnes ayant participé, de près ou de loin, à sa rédaction, sa correction, son édition, rend à la fois large, évolutif et non clairement défini le collectif qui fait vivre ce projet.

Enfin, nous estimons avoir laissé suffisamment de traces au fil de ces pages pour permettre à toute personne nous lisant de nous situer, au moins partiellement, concernant notre rapport à l'informatique, qu'il soit technique, politique ou éthique.

*
* *

Deux caractéristiques de cet écrit nous obligent néanmoins à faire face, sous certains angles, aux interrogations relatives à sa provenance. Cet ouvrage prétend d'une part transmettre des savoirs et savoir-faire techniques, réservés d'ordinaire à des spécialistes. D'autre part, la justesse des indications fournies peut avoir des implications sur la sérénité des personnes qui les mettraient en œuvre. Les petites erreurs qui nous auront échappées peuvent donc avoir de graves conséquences.

Il importe donc de dire quelques mots sur les personnes qui ont contribué à ce guide. Mettre au clair l'étendue de nos savoirs et savoir-faire — et leurs limites — permet de trouver un rapport d'apprentissage plus adéquat à cet écrit, mais aussi de décider du niveau de confiance *technique* qu'il mérite. Disons donc que, au sein du collectif :

- les questions soulevées par ce guide nous importent, que ce soit techniquement ou politiquement, depuis plus d'une dizaine d'années ;
- nous animons des ateliers de transmission et conseillons des personnes qui ont besoin d'intimité numérique ;
- nous connaissons plutôt bien le fonctionnement de certains systèmes d'exploitation, et plus particulièrement celui de Debian GNU/Linux ;
- nous avons de bonnes bases en cryptographie, mais sommes très loin de pouvoir prétendre maîtriser le sujet.

Et pour finir, affirmons une dernière fois que la parole portée par cet ouvrage, comme toute parole de *guide*, se doit d'être prise avec des pincettes proportionnelles aux conséquences en jeu.

Index

AC, *voir* autorité de certification
administratrices, *voir* admins
admins, **206**
adminsys, *voir* admins
adresse
    adresse .onion, *voir* service onion
    adresse IP, **202**, 205, 217
    adresse MAC, *voir* adresse matérielle
    adresse matérielle, **198**, 215
    adresse privée, **205**
    adresse publique, **205**
ADSL, **199**
algorithme, **48**, 333
AMD Platform Security Processor, *voir* Intel Management Engine
AMD PSP, *voir* Intel Management Engine
anonymat, **243**
anonymity set, 268
application, **22**
architecture, **17**
archivage, **89**
argument, 98
ARPANET, **197**
AS, *voir* système autonome
authenticité, **53**
auto-hébergement, 242, 319
autorité de certification, **255**, 323

backbone, *voir* épine dorsale
backdoor, *voir* porte dérobée
bibliothèque, **23**
binaire, **17**
BIOS, **20**, 76, 107, 126
bit, **17**
BitTorrent, **200**
boot, *voir* démarrage
box Internet, **205**, 215
boîte noire, 269
bridge, *voir* switch
bridge Tor, **267**, 268, 314
bug, 29

cache, 43, **213**
carte mère, **16**
carte réseau, **198**
CD ou DVD, 171
censure administrative, 233, 234
certificat électronique, **255**, 323
chemin d'un fichier, **98**, 142
cheval de Troie, **32**
chiffrement, 47, **47**, 249, 347
    chiffrement de bout en bout, **251**, 333, 343, 352
    chiffrement répudiable, **52**
    chiffrer un disque dur, **145**
    chiffrer un système, **119**
    chiffrer une clé USB, **145**
chipset, **20**
clavier virtuel, *voir* clavier visuel
clavier visuel, **327**
client de messagerie, *voir* client mail
client mail, **292**, 333
clé de chiffrement, **48**, 50, 249, 333, 343
Code de la sécurité intérieure, 32, 224, 229, 237
Code de procédure pénale, 31, 52
Code pénal, 51
code source, **39**
cold boot attack, **27**, 50, 75
collision, **53**
commutateur, *voir* switch
confidentialité, **47**
cookie, **214**, 222
CPU, *voir* processeur
cryptanalyse, **47**
cryptographie, **47**
    cryptographie asymétrique, **55**, 249, 333
    cryptographie symétrique, **55**
cryptologie, 51

Debian, 22, 119

deep packet inspection, *voir* examen approfondi des paquets
Déjà Dup, **153**
démarrage, 107
dépôt de paquets, **136**
déréférencement, **234**
DHCP, **204**
disque dur, **18**, 42
disque SSD, *voir* mémoire *flash*, *voir aussi* disque dur
distribution, **23**, 40
DNS, **210**, 232
domaine de premier niveau, **232**
DPI, *voir* examen approfondi des paquets
déni plausible, *voir* chiffrement répudiable
dépôt de paquets, **23**

écrasement des données, **42**
effacement, **42**
électricité, 21
empreinte, *voir* somme de contrôle
en-tête, **202**, 217
encapsulation, **201**
enregistreur de frappe, **35**
épine dorsale, **208**
espace d'échange, *voir* mémoire virtuelle
Ethernet, **199**
examen approfondi des paquets, **217**, 230, 236
ext2, ext3 ou ext4, **24**

Facebook, 222
FAI, *voir* fournisseur d'accès à Internet
FAT32, **24**
fibre optique, **199**
filoutage, *voir* hameçonnage
filtrage, **236**
firewall, *voir* pare-feu
firmware, *voir* microprogramme
fonction de hachage, **53**, 161
force brute, **77**
format de fichiers, **24**
formatage, **24**, 44, 146
fournisseur d'accès à Internet, **205**, 224

GAFAM, **31**, 224
Gestionnaire de machines virtuelles, 84, **163**
gestionnaire de mots de passe, **355**
Gestionnaire de paquets Synaptic, **23**, 135
GNU/Linux, 22, 40
GnuPG, 49
Google, 221

hachage, *voir* fonction de hachage
hameçonnage, **234**
hibernation, **28**
historique, 29
homme du milieu, *voir* monstre du milieu
HTTP, **200**, 217, 291
HTTPS, **200**, 255, 291
hébergement, **211**, 233, 242, 285, 319, 359

identité contextuelle, **243**
image disque, **114**, 169
image ISO, 114, **123**, 169
IMAP, 200, **292**, 331
IMAPS, 200, 255, **292**
imprimante, 36
installeur, 119
Intel Management Engine, **20**, 33
Intel ME, *voir* Intel Management Engine
Internet, **205**, 209, 239
Internet Protocol, **202**
interopérabilité, **199**
intégrité, **53**
IP, *voir* Internet Protocol
IPv4, *voir* Internet Protocol
IPv6, *voir* Internet Protocol
IRC, **200**, 351

Java, **214**, 241
JavaScript, **214**, 241
journalisation, **43**
journaux, **29**, 215, 216, 218, 224

KeePassXC, **355**
keylogger, *voir* enregistreur de frappe

LAN, *voir* réseau local
library, *voir* bibliothèque
licence
  licence libre, **40**, 132
  licence propriétaire, **39**
ligne de commande, **97**
liste autorisée, **66**
liste bloquée, **66**
log, *voir* journaux
logiciel, **22**, 131
  installation d'un logiciel, **131**
  logiciel espion, **32**
  logiciel libre, **39**, 40, 132
  logiciel malveillant, **31**, 32, 76
  logiciel open source, **40**
  logiciel portable, **44**
  logiciel propriétaire, 39, **39**
lois, 31
  loi pour la confiance dans l'économie numérique, 225

loi relative au renseignement, 32
loi renforçant la lutte contre le crime organisé, le terrorisme [...], 31
loi renforçant les dispositions relatives à la lutte contre le terrorisme, 52
LOPPSI2, 231
requête légale, *voir* réquisition judiciaire
LUKS, **50**, 145

MAC, *voir* adresse matérielle
machine du milieu, *voir* monstre du milieu
machine-in-the-middle, *voir* monstre du milieu
malware, *voir* logiciel malveillant
man-in-the-middle, *voir* monstre du milieu
MAT2, **185**
mémoire
mémoire *flash*, **18**, 20, 42, 140
mémoire morte, *voir* mémoire persistante
mémoire persistante, **18**
mémoire virtuelle, **25**, 28, 44, 73
mémoire vive, **18**, 27
messagerie instantanée, 351
métadonnées, **30**, 218, 221
microcode, *voir* microprogramme
micrologiciel, *voir* microprogramme
microprogramme, **20**, 76, 107, 120
mise à jour, 175
modem, **199**, 205
modem-routeur, *voir* box Internet
modèle de menace, **63**
monster-in-the-middle, *voir* monstre du milieu
monstre du milieu, **254**
mot de passe, **41**, 355

NAT, **205**
neutralité du Net, **207**
nom de domaine, **210**, 232
noyau, **22**
NTFS, **24**
numérisation, 17

Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, 231, 233
oignon, **261**, 313
adresse .onion, *voir* service onion
OnionShare, **359**
service onion, **266**, 326, 331, 359
ondes, 21
open source, **40**
OpenPGP, **333**, **343**
option, 98
OS, *voir* système d'exploitation
OTR, **351**
Outlook, *voir* client mail

paire de clés, *voir* clé de chiffrement
paquet (logiciel), **23**, 135
paquet (réseau), **202**, 217
pare-feu, **203**
partition, **23**
peering, **207**
périphérique, **20**
phishing, *voir* hameçonnage
phrase de passe, 47, **103**
Pidgin, **351**
pilote, **22**
point d'accès, **204**
politique de sécurité, **65**
pont, *voir* switch
pont Tor, *voir* bridge Tor
POP, 200, **292**, 331
POPS, 200, 255, **292**
port, **203**
portail captif, **216**
porte dérobée, **39**, 216
pourriel, **31**, 32, 296
processeur, **16**
programme, **22**
protocole
protocole applicatif, **200**, 217
protocole de communication, **199**
protocole IP, *voir* Internet Protocol
protocole réseau, **202**, 217
pseudononymat, **243**

radio, *voir* Wi-Fi
RAM, *voir* mémoire vive
réquisition judiciaire, 51, **228**
requête légale, *voir* réquisition judiciaire
réseau local, **204**
risques
évaluation des risques, **63**
réduction des risques, **61**
RJ-45, *voir* Ethernet
robot, 296
rootkit, **32**
routage, **208**
routeur, 205, **207**, 208, 217
RPV, *voir* VPN
Réseau Privé Virtuel, *voir* VPN
rétention de données, **224**

sauvegarde, **151**

sauvegardes automatiques, **29**
secure-delete, 139
`shred`, **142**
Signal, **200**
signature numérique, **55**, 345
signature stéganographique, **36**
site miroir, 231
Skype, 201
SMTP, **200**, 291, 331
SMTPS, **200**, 255, 291
somme de contrôle, **53**, 161
spam, *voir* pourriel
spyware, *voir* logiciel espion
SSD, *voir* mémoire *flash*, *voir aussi* disque dur
SSL, *voir* TLS
stockage web local, **214**
stéganographie, **36**
surface d'attaque, **66**
swap, **25**, 28
switch, **204**
Synaptic, *voir* Gestionnaire de paquets Synaptic
syntaxe, 98
système autonome, **206**
système de fichiers, **24**, 43
système d'exploitation, **22**
  installation d'un système, **119**
  système hôte, 84
  système invité, 84
  système *live*, 22, 44, 82, 113, **113**

Tails, 44, 82, **113**, 175, 267, **280**, 295, 301, 327, 343, 359
  stockage persistent, 151, 356
TCP, **202**
terminal, **97**
Thunderbird, *voir* client mail
TLD, *voir* domaine de premier niveau
TLS, **255**, 258
top level domain, *voir* domaine de premier niveau
Tor, **261**, 313
traces, **27**, **213**
transistor, **17**
transit, **207**, 209
TrueCrypt, 40

UDP, **202**
UEFI, **20**, 76, 126, 128
upgrade, *voir* mise à jour
USB, **20**

veille, **28**
VeraCrypt, **52**
Virtual Private Network, *voir* VPN
virtualisation, 83, **163**
  machine virtuelle, 212
  virtualisation matérielle, **164**
virus, **32**
VPN, **227**

watermarking, *voir* signature stéganographique
webmail, **291**
WebRTC, **215**
Wi-Fi, **199**, 204
Windows, 82, 165
wipe, *voir* écrasement des données

XMPP, **200**, 351, 352

Crédits

Couverture, quatrième de couverture et dessins des pages i, xvi, 8, 188 et 360 de l'équipe du guide d'autodéfense numérique.

Photo page 16 de Darkone, licence CC BY-SA 2.5, trouvée sur :
https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:ASRock_K7VT4A_Pro_Mainboard.jpg.

Photo page 16, domaine public, trouvée sur :
https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:Pentium-60-back.jpg.

Photo page 18, de Topory, licence CC BY-SA 3.0, trouvée sur :
https://fr.wikipedia.org/wiki/M%C3%A9moire_vive#/media/Fichier:RAM_n.jpg.

Photo page 18, domaine public, trouvée sur :
https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:Hdd-wscsi.jpg.

Photo page 19, domaine public, trouvée sur :
https://commons.wikimedia.org/wiki/File:MSATA_SSD_16_GB_Sandisk_-_SDSA3DD-016G-2494.jpg.

Photo page 20 de Zac Luzader Codeczero, licence CC BY 3.0, trouvée sur :
https://secure.wikimedia.org/wikipedia/fr/wiki/Fichier:AT_Motherboard_RTC_and_BIOS.jpg.

Dessin page 77 de XKCD, licence CC BY-NC 2.5, trouvé sur :
https://xkcd.com/538/.

Photo page 199 de David Monniaux, licence CC BY-SA 3.0, trouvée sur :
https://commons.wikimedia.org/wiki/File:Ethernet_RJ45_connector_p1160054.jpg.

Photo page 207 de Geek2003, licence CC BY-SA 3.0, trouvée sur :
https://commons.wikimedia.org/wiki/File:Avaya_Secure_Router_2330.jpg.

Photo page 211 de Victor Grigas, licence CC BY-SA 3.0, trouvée sur :
https://commons.wikimedia.org/wiki/File:Wikimedia_Foundation_Servers-8055_08.jpg.

Schéma page 263 de HANtwister, licence CC BY-SA 3.0, trouvé sur :
https://en.wikipedia.org/wiki/Onion_routing#/media/File:Onion_diagram.svg.

Schémas pages 264, 265, 265 et 266 de Nos Oignons et Electronic Frontier Foundation, licence CC BY, trouvés sur :
https://nos-oignons.net/Diffusez/index.fr.html.

Icônes dans le corps du texte issues de la police de caractères Font Awesome 4 par Dave Gandy, licence SIL OFL 1.1 (https://fontawesome.com/v4/).

Icône « pour aller plus loin » de Mr Minuvi de The Noun Project ; icône « contenu de fenêtre » de Gregor Cresnar de The Noun Project ; icône « texte de loi » de Handicon de The Noun Project ; icône « précisions » de Colourcreatype de The Noun Project : licence CC BY 3.0 (https://thenounproject.com/).

Les autres schémas sont faits par l'équipe du guide et utilisent des icônes : de GNOME Project, licence CC BY-SA 3.0 ; de Silvestre Herrera, licence GPLv2, trouvées sur http://www.silvestre.com.ar/ ; du domaine public trouvées sur https://openclipart.org.