Guia de Autodefesa Digital

Versão 1.0.0

Autodefesa

17 jan, 2021

Sumário

1 Introdução 2

2 Conceitos Básicos 4

3 Conceitos Avançados 7

4 Limites da segurança 13

5 Checklist de Segurança 16

6 Comunicação Digital 21

7 Criptografia Básica 28

8 Autenticação com Senhas 36

9 Computadores 43

10 Telefones celulares 59

11 A Internet e a Web 64

12 Mensageria 68

13 Backups Criptografados 71

14 Rastros Digitais 74

15 Roteiros de Oficinas 76

16 Referências 83

17 Meta 98

Tor Onion Service | PDF | EPUB

Este é um guia para **qualquer pessoa e grupo** que tenha interesse em saber por conta própria como se defender de ameaças do uso de dispositivos de comunicação na era da vigilância automática.

Não importa quem você seja. Não importa o que você pensa. Não importa o que você faz. Não importa o quanto você tem. Não importa se você governa ou é governado. A vigilância digital te afeta.

A vigilância digital pode ser realizada por qualquer ator hostil. Ele pode ocupar um cargo público, pode estar infiltrado numa empresa ou ser uma «pessoa comum». Ele pode até ser um agente duplo que te vende segurança mas que você não percebe por não ter senso crítico e autoconsciência.

Saiba aqui como se defender sem cair na paranóia.

CAPÍTULO 1

Introdução

Este não é um guia sobre guarda-costas digitais. Não vamos ensinar sobre como buscar ajuda para se defender. Aqui não temos interesse em alguém fazendo nossa segurança.

Pelo contrário, queremos que você aprenda a se defender.

Autodefesa é a capacidade de uma pessoa ou grupo se proteger por contra própria. Autodefesa digital é aplicação desse conceito no uso de tecnologia de comunicação.

O caminho da autodefesa é mais difícil. Requer que você estude e pratique. Mas também é o caminho mais rico. Nele, você aprende mais e se torna uma pessoa mais completa e capacitada para passar o conhecimento adiante.

Este guia está dividido em capítulos, cada um deles com um tema específico. Falaremos sobre segurança em computadores, em dispositivos móveis e também na web.

Cada tema sempre será apresentado de acordo com a seguinte sequência:

1. Funcionamento de uma dada tecnologia.
2. Ameaças dessa tecnologia.
3. Defesas viáveis.

Você pode seguir os capítulos de forma independente. Você pode inclusive já pular diretamente para algum assunto que seja do seu interesse ou necessidade imediata.

Mas caso você queira entender a lógica e os princípios básicos da segurança, recomenda-se que você comece pelo material introdutório.

Assistir o guia todo também é uma boa ideia, pois a bagagem teórica de um capítulo às vezes toma emprestado conhecimentos dos capítulos anteriores.

O guia é acompanhado de algumas atividades propostas para que você se exercite e tenha um incentivo para aplicar os paradigmas de segurança da informação na sua vida cotidiana.

Mais importante do que você adotar todos os procedimentos de segurança sugeridos ao longo do guia, é você entender os esquemas mentais de quem pensa em segurança, aquilo que chamanos de «mindset». Tendo isso, você poderá fazer **escolhas conscientes** sobre a sua segurança digital.

Por que este guia é importante?

Antigamente, para vigiar uma pessoa e obter informações sigilosas, era necessário manter uma pessoa dedicada a esta tarefa. A espionagem era limitada principalmente pelo fator humano. Espionar era um privilégio de poucos governos, empresas e instituições. Ser espionado era um sinal de estar realizando alguma atividade de importância que despertou o interesse de algum poder.

Aos poucos as instituições humanas vão mudando e surgem diversas formas de vigilância. Em particular, com a difusão da informática os custos da comunicação vão diminuindo.

Com isso, os custos da espionagem na comunicação digital também vão caindo, porque um mesmo aparato de vigilância pode coletar, processar e analisar milhões de comunicações de milhões de pessoas a um custo baixíssimo.

Nós **vivemos na era da vigilância de massa**. Pode ser que você não seja uma pessoa de interesse muito grande para algum poder, mas mesmo assim a sua comunicação pode estar sendo automaticamente interceptada ou armazenada sem o seu consentimento.

Simplesmente porque é barato. E porque mesmo a informação de pessoas consideradas comuns hoje tem valor estratégico. Para decisões políticas. Econômicas. Sociais.

A Educação, pelo menos em teoria, é a forma de preparar pessoas livres. Hoje, um conhecimento mínimo de tecnologia e autodefesa digital é parte importante para que uma pessoa possa exercer suas escolhas, sua profissão ou toda a sua vida com liberdade.

Não vivemos em um mundo onde podemos ignorar completamente o seu funcionamento e especialmente o funcionamento básico da tecnologia. Nem vivemos em um mundo onde as tecnologias de comunicação são seguras por padrão. Vivemos numa situação em que as tecnologias são mal feitas no que diz respeito à segurança e seus problemas técnicos são usados contra nós.

Este guia foi feito para todos os níveis de entendimento. Ele serve para você mesmo que você seja iniciante ou expert em segurança. Porque ele é um guia completo. Ele contém o **mindset**, ou forma de pensar a segurança digital.

Também é um guia modular e cheio de conceitos. Se você quiser pode pular direto para temas mais práticos e do seu interesse.

Se você aproveitar todo o guia, terá uma boa base para começar a se capacitar para ser um profissional em segurança da informação realizando outros guias e obtendo certificações se achar necessário.

CAPÍTULO 2

Conceitos Básicos

2.1 O que é segurança?

Para os fins deste guia, vamos considerar que **segurança é a proteção** a determinadas ameaças – ou **riscos de falha** – em nossas atividades.

Por exemplo, alpinistas usam uma série de equipamentos que possuem funções de proteção contra quedas. Da mesma forma, o cinto de segurança é um equipamento feito basicamente para proteção contra acelerações bruscas.

Tanto escalar montanhas quanto viajar em aviões são atividades que envolvem riscos de falha. Muita gente não deixa de viajar de avião por conta dos riscos de queda justamente pelos procedimentos e equipamentos de segurança envolvidos.

Outro aspecto da segurança, portanto, é sua capacidade de nos **encorajar** a desempenhar uma atividade ao minimizar riscos e também por nos tornar conscientes sobre quais riscos estamos submetidos/as e do quanto estamos protegidos/as.

2.2 Segurança versus paranóia

Isso coloca a segurança no campo oposto da **paranóia** – já que a paranóia é justamente o conjunto de procedimentos contra ameaças reais ou imaginárias que faz com que uma pessoa não tome iniciativa.

O Guia de Autodefesa Digital foi feito para que você tenha consciência das ameaças e proteções no universo da comunicação eletrônica de forma que você continue realizando suas atividades mas de forma consciente e segura, ao invés de se isolar num universo próprio de paranóia ou simplesmente ignorar qualquer medida de segurança e agir como quem diz «está tudo dominado mesmo, né?».

2.3 Praticidade e eficácia: segurança versus conforto

Nem sempre os procedimentos de segurança são os mais confortáveis. A experiência nos mostra que os procedimentos que são ao mesmo tempo práticos e eficazes são aqueles que acabam sendo adotados pelas pessoas.

Considere a seguinte recomendação de segurança: caso queira despistar quaisquer possíveis espiões de te seguirem a uma reunião importante, saia 5 horas antes da sua casa, tome 4 ônibus com destinos aleatórios e só então siga para o ponto de encontro.

Sem questionar a eficácia de tal procedimento, podemos ver logo de cara que ele é muito custoso.

Um grupo até pode adotar alguma coisa complicada assim em momentos extremos caso considere que isso seja eficaz. Mas, se usar isso no dia-a-dia, a tendência natural é que essa convenção não seja respeitada. E isso pode ser danoso ao grupo, pois ele passa a não seguir um acordo mas ao mesmo tempo contar com ele para a sua segurança.

Isso pode acontecer não só num grupo, mas em algum procedimento de segurança que você escolher adotar: ele pode ser tão difícil e complicado que depois de um tempo você larga mão.

2.4 Viabilidade: Redução de danos

É muito comum pessoas quererem adotar um montão de práticas de segurança de uma vez só, da mesma forma como alguém pode tentar largar um vício de uma vez – como por exemplo parar de fumar ou adotar a dieta vegetariana.

Mas mudanças radicais de hábito nem sempre resistem ao tempo: até a curto prazo elas podem ser abandonadas. A experiência mostra que é muito mais viável ir aos poucos, adotando mudanças incrementais na sua vida.

2.5 Segurança: dado cultural

Aqueles procedimentos que são práticos, eficazes e viáveis podem acabar sendo incorporados à própria cultura de um grupo. Exemplos mais simples disso são as práticas de higiene, como lavar as mãos ou escovar os dentes: são medidas preventivas práticas, baratas e eficazes contra doenças.

2.6 Economia da segurança

Em resumo, existe uma economia da segurança: uma prática de segurança é dada por alguns fatores básicos:

1. Custo de implementação e manutenção, ou seja, não só custo econômico mas também a quantidade de trabalho que dá para manter a prática.
2. Eficácia da medida, ou seja, o quanto determinada prática de segurança tem um efeito de eliminar a ameaça ou reduzi-la, por exemplo ao fazer com que o custo do ataque aumente.
3. Probabilidade de ataque, que é uma estimativa, muitas vezes bem aproximada ou feita de pura intuição, sobre o quanto uma ameaça é provável de acontecer.

Idealmente, queremos adotar as práticas que sejam mais eficazes e menos custosas aos eventos de ataque que sejam mais prováveis! Esse é o resumão básico sobre segurança!

2.7 Resumo

Vamos fazer um resumo rápido dos conceitos apresentados até o momento?

1. Segurança é a **proteção** a determinadas ameaças – ou **riscos de falha** – em nossas atividades.
2. Paranóia, ao contrário, é o mecanismo usado para não agir por conta de riscos reais ou imaginários.
3. Existe uma relação entre conforto e segurança que deve ser balanceada.

4, Adote procedimentos de segurança aos poucos, reduzindo os danos de forma sustentável ao invés de tentar mudanças radicais que não sejam duradouras.

5. Relação econômica na segurança: custo, eficácia e probabilidade de ataque.
6. Procedimentos práticos e eficazes tem mais chance de se tornarem culturais.

2.8 Atividades

1. Liste os procedimentos de segurança que você já utiliza ou atividades que você realiza, mesmo que de forma cotidiana e automática, que podem ser consideradas como procedimentos de segurança. Exemplo: andar olhando discretamente para trás de vez em quando para checar se há alguém te seguindo.
2. Liste quais você acha que são os riscos mais prováveis à sua segurança. Quais seriam aqueles que você acha que deve combater primeiro?

CAPÍTULO 3

Conceitos Avançados

3.1 Introdução

Até aqui tratamos do comportamento de práticas de segurança de forma bem genérica: elas são defesas viáveis, práticas e eficazes contra ameaças prováveis.

Tudo bem, mas quais são essas práticas? Como devemos adotá-las? Por onde começar?

Trataremos agora de mais alguns conceitos importantes que vão nos ajudar a entender como priorizar as defesas consideradas mais importantes.

Estes são tópicos avançados e, se preferir, você pode pulá-los!

3.2 Segurança se dá por níveis (camadas)

Em certo sentido podemos pensar em segurança como a estabilidade de um edifício: quanto mais molenga for o terreno onde ele está construído, mais chances de queda de todos os seus andares. Da mesma forma, se suas fundações forem fracas, todos os andares estarão comprometidos. Imagine agora um prédio onde apenas o último andar é muito fraco, e que seu desmoronamento não implique no abalo dos andares inferiores, ou que esse abalo não seja significativo.

Diríamos então que, neste prédio hipotético, a solidez dos andares superiores dependem não só da sua própria solidez mas também da solidez dos andares inferiores. Mesmo que um andar seja bem feito ele sofrerá de problemas estruturais se os andares inferiores foram mal feitos.

A segurança, e especialmente a segurança digital, funciona de modo muito parecido: se as bases da segurança não são sólidas, então as proteções oferecidas por um procedimento que se encontra no meio do seu «edifício da segurança» não será muito eficaz.

Por exemplo, não adianta muito você ter uma senha de acesso muito poderosa se você a utiliza num computador que já estiver invadido, por exemplo, por softwares que registram e extraem o que é digitado, os chamados «keyloggers».

Em outras palavras, a segurança se dá por níveis, ou camadas: defesas que se referem a um determinado nível do edifício – ou pilha – da segurança não protegem de ameaças que operam nos níveis inferiores.

Isso acontece quando há uma hierarquia de dependências entre coisas: se uma dependência falha, então aquilo que depende também tende a falhar.

Ou seja, em muitas situações o mais importante é melhorar a segurança a partir das camadas, ou níveis, mais baixos, numa abordagem infraestrutural.

É claro que em algumas ocasiões existe uma mútua dependência. Nesse caso, dizemos que as medidas de segurança mutuamente dependentes se encontram no mesmo nível.

3.3 Simplexidade: a Complexidade Necessária

É válido observar que sistemas, procedimentos ou vidas mais complexas e interdependentes podem ter mais vulnerabilidades do que situações mais simples e independentes.

Um dos **princípios** que vão nos guiar daqui em diante é o da **complexidade necessária**, ou seja, tentaremos sempre buscar o caminho mais simples, porque:

1. O mais simples é o mais simples de entender.
2. Sendo mais simples de entender, é mais simples de conhecer suas fraquezas e defesas.
3. Mais simples pode ser mais robusto por ser mais simples de adotar e manter.
4. Simplicidade pode ter relação direta com economia e custos: mais simples, mais barato, não só financeiramente.

Aqui, **simples será usado como um sinônimo para complexidade necessária**, já que mesmo as coisas mais simples possuem sua complexidade. Estamos falando de **simplexo**, a noção complexa do simples que não é simplória.

Recomenda-se, então, que medidas de segurança sejam avaliadas também no quanto de complexidade necessária elas possuem: naquilo que elas são mais complicadas, são mais complicadas por um motivo importante e necessário?

Assim, se duas medidas de segurança que possuem a mesma capacidade de defesa, tenderemos a escolher a mais simples, pois ela não acarreta em complexidades desnecessárias.

Esta é basicamente a versão, no campo da segurança, do princípio da **Navalha de Occam**, onde uma hipótese é escolhida entre diversas concorrentes e equivalentes pela sua simplicidade. Ou seja, o princípio do universo econômico. Mas é bom lembrar que este é um princípio guia e não necessariamente uma verdade absoluta.

3.4 Interdependência: Compartimentalização e Pontos de Falha

A partir do que discutimos até o momento fica como consequência o fato de que a interdependência entre sistemas e pessoas pode acarretar em falhas em cascata quando existe alguma violação de segurança: a invasão num ponto pode comprometer todos os outros pontos dele dependentes.

Aplicando o princípio da complexidade necessária, podemos pensar também no conceito de **dependência necessária**, sendo a adoção de procedimentos de segurança que sejam dependentes ou interdependentes apenas o quanto for preciso.

Os termos usados para **dependência necessária** são **compartimentalização** ou **desacoplamento**, isto é, isolar partes, pessoas ou procedimentos de segurança de um sistema para que falhas numa parte não impliquem na falha de outras ou mesmo do todo.

A cada sistema que for crucial para o funcionamento de outro, ou seja, a cada sistema do qual outros dependam, daremos o nome de **ponto de falha**. O ideal é sempre minimizarmos os pontos de falha. O pior caso é aquele conhecido como **Ponto Singular de Falha** ou **Singular Point of Failure (SPF ou SPOF)**: aquele cuja falha implica na falha de todo o sistema.

O corpo humano é um exemplo de sistema que possui diversos pontos singulares de falha, os chamados órgãos vitais: enquanto o corpo ainda permanece vivo sem membros como braços e pernas, ele falhará se perder um coração, pulmão ou cérebro.

Resiliência é a propridade de um sistema de minimizar pontos de falha e resistir, ou seja, permanecer funcionando e se restaurar após falhas.

3.5 Tipos de ameaças

Existem várias formas de classificar as falhas de segurança. Adotaremos a seguinte:

1. Negação de Serviço é a mais simples de entender. Consiste em bloquear o funcionamento de um sistema de modo que, na prática, ele não consiga operar normalmente.

   A negação de serviço por si só não toma o controle de todo o computador nem obtém dados sensíveis. Apenas deixa um sistema temporariamente inutilizado.

   Uma forma simples de negação de serviços é um programa que trave ou que pare de rodar por conta de algum problema. Programas que travam sozinhos são bem suspeitos como portas de entrada para esse tipo de ataque.

   A negação de servido é uma falha na segurança da informação pois ataca diretamente a propriedade da **disponibilidade**.

2. Execução arbitrária de código: nesta falha, um atacante consegue realizar operações no sistema para as quais ele não deveria ter autorização.

   Ele pode, por exemplo, invadir um computador e fazer com que ele execute programas diversos.

3. Escalada de Privilégios é uma falha onde um atacante ganha privilégios ou acesso a partes não autorizadas de um sistema.

Essas falhas podem ser exploradas simultaneamente!

3.5.1 Natureza das falhas

Qual é a natureza das ameaças à nosa segurança? Podemos pensar em:

1. Ameaças que existem naturalmente, isto é, que são consequências da natureza de operação de dispositivos, procedimentos, etc.

2. Ameaças que existem por conta da estupidez, ignorância ou falta de atenção de quem desenvolveu os dispositivos, procedimentos, etc.

3. Ameaças que foram colocadas intencionalmente, ou seja, por malícia de quem desenvolveu os dispositivos, procedimentos, etc, visando manter um canal aberto para possíveis invasões. Isso pode ser feito na surdina e até em colaboração com agências de vigilância de governos.

Como saber de que tipo de vulnerabilidade estamos falando? Essa distinção faz alguma diferença?

Pelo critério da Navalha de Occam, podemos dizer que não há diferença entre ameaças que foram colocadas por estupidez ou malícia, pois os danos que elas podem causar são os mesmos.

Essa versão específica de navalha é chamada de Navalha de Hanlon. O que é explicado por estupidez não precisa ser explicado em termos de malícia.

Podemos ainda dizer que o que é explicado pela natureza dos sistemas não precisa ser explicado nem pela estupidez, nem pela malícia.

De modo que nossa prioridade deve ser nos proteger de qualquer ameaça e só então tratar de entender a intencionalidade das vulnerabilidades: de onde elas vieram e porquê ainda estão lá. Este é um princípio importante para que não nos desesperemos ante a qualquer possibilidade de ameaça.

Afinal, viver é perigoso.

3.6 Qual a diferença entre segurança e privacidade?

Neste curso vamos considerar uma definição específica de privacidade.

Enquanto segurança é a preparação antecipada a ameaças diversas que podem nos causar danos, a privacidade é toda e qualquer informação que queremos proteger. É qualquer informação que não queremos que seja tornada pública ou que queiramos manter disponível apenas a um círculo restrito de pessoas.

3.6.1 Privacidade é algo coletivo

Ao contrário do que se imagina, a privacidade não se restringe apenas a uma pessoa. Isso valeria apenas num mundo de pessoas isoladas ou com informações que não são compartilhadas com ninguém.

Pelo fato de nos comunicarmos, – consequência da vida em sociedade – informações sobre nós e sobre outras pessoas trafegam de um lado para outro e de pessoa em pessoa, o que implica que a privacidade é, necessariamente, uma propriedade coletiva. Qualquer pessoa, mesmo que seja parte do seu círculo privado de comunicação, pode entregar a sua privacidade ao divulgar uma informação sua que ela possui.

3.6.2 Privacidade é algo político

No mundo contemporâneo, a existência da privacidade é uma consequência de uma vida em sociedade na qual dentro da própria sociedade existem ameaças a seus integrantes e principalmente a conjuntos inteiros de integrantes (classes, gêneros, raças, etc). A privacidade é, então, usada para que permita a articulação entre um mesmo grupo social para que possa se preparar para uma disputa aberta.

A privacidade, portanto, é algo inerentemente político, entendendo política como uma disputa entre antagonistas. De modo que podemos chamar de **sigilo** a defesa das informações privadas de um grupo.

Fica fácil assim pensar no sigilo como importante inclusive nas guerras.

3.7 Segurança por obscuridade

É muito, muito comum que se confunda segurança com privacidade. São coisas distintas.

Quando alguém tenta usar a privacidade como medida de segurança, estará adotando o que chamamos de **segurança por obscuridade**, o que de fato **não é segurança**.

Para nos guiar, vamos utilizar o **Princípio de Kerckhoffs**, que em resumo diz o seguinte:

```
Assuma que o inimigo conhece o sistema.
```

Em versão menos resumida, podemos dizer que, por tal princípio, devemos assumir por simplicidade, mesmo que não seja o caso, que o atacante de um sistema conhece todos os detalhes do funcionamento desse sistema.

O que não quer dizer que ele saiba ou tenha invadido o sistema, ou mesmo que possui as informações que estejam protegidas dentro do sistema.

Ou seja, a segurança de um dado sistema não pode ser baseada na suposição de que o oponente não conhece o funcionamento do sistema. Além de ser uma suposição que pode ser falsa, não podemos assumir que por mero desconhecimento um oponente não seja capaz de descobrir uma brecha no sistema.

Por exemplo, você pode deixar a porta da sua casa fechada mas destrancada se quiser, mas não pode assumir que ninguém vai tentar abri-la, independentemente de alguém saber ou não que a porta está destrancada.

Se ninguém estiver de olho na sua casa, o fato da porta estar destrancada pode ser considerado como um risco baixo, mas se você for um alvo específico de alguém então o risco é mais alto. Mas você nunca sabe efetivamente o tamanho desse risco e não deve contar com a suposição de que ninguém sabe que você não tranca a porta. Considerando que é muito rápido e fácil você sempre trancar a porta, o melhor a fazer é trancá-la e assumir que todo mundo sabe como uma porta funciona, como se todo mundo fosse um bom chaveiro que soubesse inclusive arrombar a porta.

Assim você passará a se preocupar com a resistência da sua porta e com a qualidade da sua fechadura e no tempo que demora para que alguém consiga arrombá-la.

Em segurança, não podemos assumir a obscuridade como proteção. Podemos até tornar nossos procedimentos secretos, mas não podemos assumir que pelo fato de serem secretos eles são desconhecidos.

3.8 Segurança da informação

Para concluir este capítulo e considerando que este não é um guia de segurança geral, mas de segurança em comunicação digital, enunciaremos os princípios básicos da segurança da informação.

Grosso modo, podemos dividir a segurança da informação em algumas propriedades. As consideradas mais importantes são as seguintes:

1. Confidencialidade: é a garantia de que comunicação apenas poderá ser interpretada pelas partes envolvidas, isto é, mesmo havendo interceptação por terceiros o conteúdo da comunicação estará protegido.

   Isso significa que, numa comunicação entre você e outra pessoa, haverá confidencialidade se apenas vocês tiverem acesso ao conteúdo da comunicação.

2. Integridade: é a garantia de que o conteúdo da comunicação não foi adulterado por terceiros.

   Ou seja, na comunicação entre você e outra pessoa, vocês conseguem identificar se alguém alterou o conteúdo das mensagens.

3. Disponibilidade: é garantia de que o sistema de comunicação estará acessível sempre que necessário. Este é um requisito de segurança porque a falta de comunicação pode ser muito prejudicial.

4. Autenticidade: garante que cada uma das partes possa verificar se está de fato se comunicando com quem pensa estar se comunicando, isto é, a garantia de que não há um impostor do outro lado da comunicação.

Opcionalmente também podemos falar de:

5. Não-repúdio: garantir que as partes envolvidas na comunicação não possam negar ter participado da comunicação. Esta propriedade é desejada em sistemas nos quais haja um controle sobre quem realizou determinados tipos de operações.

   O oposto do não-repúdio é a negação plausível, no caso onde não é possível determinar com certeza se determinada pessoa participou da comunicação.

   Alguns sistemas foram criados para possuir a propriedade do não-repúdio, enquanto outros são baseados na negação plausível.

6. Anonimato: é garantia de que as partes envolvidas na comunicação não possam ser identificadas.

7. Auditabilidade: o sistema de comunicação tem seu funcionamento conhecido e pode ser auditável por qualquer pessoa que tenha acesso e conhecimento.

Nem sempre os sistemas satisfazem todas essas propriedades, seja intencionalmente ou não. É importante observar o que cada sistema oferece em termos dessas propriedades.

Em muitas situações, é possível combinar diversos sistemas que ofereçam propriedades distintas de segurança da informação para obter o máximo de propriedades possíveis.

3.9 Resumo

Hora do resumo dos conceitos apresentados:

1. Segurança se dá por níveis/camadas: o comprometimento da segurança numa camada afeta a segurança de todas as camadas superiores e/ou dependentes.
2. Em segurança, damos preferência a procedimentos e ferramentas que obedeçam o princípio da simplicidade, isto é, da complexidade necessária.
3. A interdependência entre sistemas e procedimentos pode acarretar em pontos de falha. Contra isso, utilizamos compartimentalização.
4. A privacidade é toda e qualquer informação que queremos proteger. Ela é algo coletivo e político.
5. Segurança por obscuridade, de fato, não é segurança. Assuma que o inimigo conhece todas as suas defesas.
6. Os princípios mais importantes da segurança da informação são: confidencialidade, integridade, disponibilidade e autenticidade.

3.10 Atividades

1. Caso você já tenha feito uma lista dos procedimentos de segurança que você utiliza ou gostaria de utilizar, você conseguiria organizá-los numa hierarquia de dependências, isto é, qual depende de qual?

CAPÍTULO 4

Limites da segurança

4.1 Introdução

Já falamos sobre várias características da segurança e também sobre aspectos sobre a privacidade. Agora precisamos mostrar quais são os seus limites.

Queremos responder à seguintes perguntas:

1. É possível afirmar com certeza se estou ou não sendo invadido(a)?
2. Existe segurança totalmente eficaz, isto é, 100% infalível?

4.1.1 Ceticismo e ignorância

Digamos que a segurança pode ser o ramo da ciência que mais se beneficie com o **ceticismo**. Quanto mais duvidarmos da realidade e dos fatos, mais chances teremos de criar e usar procedimentos seguros.

Lembre-se que **ceticismo** é diferente de **paranóia**. No nosso caso, pensaremos no ceticismo como uma dúvida constante mas que não impede que sigamos em frente. Podemos até assumir algumas coisas como verdades práticas, mas sempre deixaremos espaço para a dúvida.

Pois bem, neste nosso ceticismo, diremos que é muito difícil provar que algo não existe. Podemos dizer que determinada coisa não existe por nunca termos nos encontrado com ela, mas nada garante que não possamos encontrá-la se nos dedicarmos por tempo suficiente.

Em outras palavras,

```
A ausência de evidência não é a evidência de ausência.
```

Assim, podemos descobrir se a nossa segurança está sendo violada. Mas nunca saberemos de antemão se ela está ou não sendo violada. E nem saberemos a quantidade de violações.

Em outras palavras, a procura por evidências de invasões será sempre incerta e incompleta. Podemos contudo, nos proteger das ameaças mais factíveis, baratas e prováveis.

Mas calma! A quantidade de invasões em curso pode sim ser zero! Estamos falando apenas da nossa **ignorância** quanto à existência e quantidade de invasões e não nas invasões que de fato possam estar acontecendo.

Da mesma forma que não podemos assumir que os possíveis oponentes desconhecem nossos procedimentos de segurança, não podemos assumir que conhecemos todas as ameaças que operam contra nós.

Podemos, através da investigação – as chamadas **auditorias de segurança** – descobrir várias invasões de segurança que podem estar ocorrendo contra nós. **Mas nunca conseguiremos saber se descobrimos todas!**

Assim, por simplicidade, podemos até assumir que todos os seus sistemas estão invadidos ou em vias de serem invadidos. E a partir dessa perspectiva desoladora começar a pensar em procedimentos de segurança. Esta é a abordagem **prática** que adotaremos, isto é, ela é **pragmática**.

É possível descobrir se você está sendo invadido(a). Mas nada garante que isso seja descoberto. E não é possível dizer se você não está sendo invadido(a).

Sim, viver é perigoso. Podemos diminuir nossa ignorância, mas nunca por completo.

```
O ceticismo pragmático é a nossa melhor defesa contra uma ignorância invencível.
```

4.1.2 Sistemas abertos

Além disso, o mundo é um sistema aberto. Nós e nossos sistemas são também abertos. Porque para interagir no mundo é necessário ter alguma abertura. Qualquer abertura afeta o funcionamento interno de um sistema e eventualmente pode ser usada para perverter o funcionamento do sistema.

Nesse sentido, toda interação é uma construção de interdependência e sujeita a riscos. Contra isso não há o que fazer além de ter consciência e levar esse fato em conta ao pensar sua segurança.

Ou seja, **não existe segurança completa** em sistemas que admitem graus de abertura.

E, na natureza, apenas sistemas fechados e isolados não trocam informação com o mundo exterior, o que não é o caso de sistemas vivos, sociais, informacionais.

Talvez o mais fundamental sobre segurança é o fato de que, até onde vai a nossa ignorância, qualquer sistema é incompleto e possui falhas.

Por isso, não existe sistema 100% seguro. Mas lembremos que **poder** não é o mesmo que **ser**. Um sistema **pode** ser invadido, mas não quer dizer que ele **esteja** sendo invadido.

4.2 Arquiteturas abertas e fechadas

Mesmo quando já conhecemos o funcionamento de algo ainda assim temos dúvidas se não nos debruçamos o suficiente sobre todas as possibilidades de mal funcionamento.

Assim, o mero fato de não conhecermos o funcionamento de algo já nos lança dúvidas se aquilo não possui uma falha que pode ser explorada por alguém.

Por isso, não podemos confiar em sistemas que não ofereçam meios para serem inspecionados.

No caso de hardware e softwares para comunicação digital, como veremos ao longo do curso, é importante que eles possuam arquitetura aberta e possam ser não apenas inspecionados mas também corrigidos caso sejam encontradas falhas.

Isso implica que precisamos dar preferência para os chamados **softwares livres e abertos** e também aos **hardwares livre ou aberto**. Eles não são necessariamente mais seguros – apesar de muitos serem – mas eles permitem que sejam investigagos com mais facilidade.

4.3 Resumo

1. Não existe segurança total ou sistema infalível.
2. Em segurança, recomenda-se adotar o ceticismo pragmático: é possível descobrir se você está sendo invadido(a), mas isso nem sempre acontece. Pior que isso, não é possível dizer que você não está sendo invadido(a).
3. Temos que evitar basear nossa segurança em sistemas fechados que não podem ser auditados.
4. Não assuma de antemão como sendo malícia uma vulnerabilidade encontrada que pode ser explicada por incompetência ou por fatos naturais.

4.4 Atividades

1. Pense, mas não escreva, nas situações nas quais você descobriu que estava sendo invadido/a. Como você reagiu? Sua segurança melhorou desde então?

CAPÍTULO 5

Checklist de Segurança

5.1 Introdução

Já falamos sobre o funcionamento ideal de práticas de segurança e sobre como elas podem ser priorizadas.

Só nos falta um conceito final para que possamos tratar dos ataques e defesas, que é o nosso Checklist de Segurança, também conhecido como modelo de ameaças. Ele nos ajudará a organizar a nossa estratégia de segurança.

Para cada tecnologia ou atividade, dividiremos nossa análise de segurança em três etapas:

1. Funcionamento: saber como algo funciona é o primeiro passo.
2. Ataques: entendendo, conseguimos avaliar as ameaças possíveis.
3. Defesas: conhecendo as ameaças, podemos pensar em defesas.

5.1.1 Ameaças: usos não convencionais

Qualquer objeto técnico tem inúmeros usos possíveis. Mesmo que eles tenham sido construídos para desempenhar determinadas funções, eles acabam por ter usos que não foram colocados intencionalmente pelas pessoas que os projetaram.

Nós podemos usar um martelo como peso de papéis. Podemos usar o forno de microondas para secar roupas. Podemos usar uma porta para quebrar nozes, uma furadeira para bater massa de bolo, e assim por diante.

Com um pouco de memória e criatividade, acho que você também pode se lembrar ou mesmo inventar usos alternativos para vários objetos.

Existem vários desvios de função malucos e criativos. Outros, nem tanto.

O desvio de função é parte essencial na evolução da tecnologia. Inclusive na tecnologia de causar danos a pessoas e sistemas.

Podemos então definir como **ameaça** qualquer desvio de função de um objeto técnico ou situação que possa ser usada para nos causar algum tipo de dano ou prejuízo.

O martelo do exemplo anterior pode ser usado para ferir uma pessoa. O automóvel para atropelar alguém. Aliás, você já notou que automóveis e martelos não se tornam proibidos mesmo sendo armas em potencial?

Quando pensamos em algum objeto ou atividade física – um patinete, uma melancia ou mesmo uma escada – temos grande facilidade em imaginar seu uso convencional.

Mas tempos um pouco de dificuldade para entender os riscos do uso desses objetos e atividades, como casas de madeira que podem entrar em combustão, árvores que podem cair sobre a gente, sequestros relâmpagos, etc.

Quando se trata de objetos ou atividades que são difíceis de visualizar, nós temos muito menos intuição ainda desses riscos, como é o caso do uso de dispositivos de comunicação digital.

Temos, por exemplo, dificuldade de entender que uma comunicação que trafega por fios elétricos pode ser interceptada por alguém.

Em parte porque automaticamente pensamos sempre no uso convencional.

Mas, também, porque não entendemos direito o funcionamento interno de diversas tecnologias, de tal modo que temos uma limitação em imaginar seus usos não convencionais.

5.2 Exemplo

Nada melhor do que um exemplo para ajudar a entender o que é o Checklist da Segurança.

Suponha então uma pessoa que realize as seguintes atividades diárias:

1. Ela acorda em casa.
2. Depois, se desloca para o trabalho.
3. Trabalha com informações sensíveis no computador.
4. Utiliza o telefone celular durante todo o dia.
5. Por fim, se desloca para a casa para descansar.

Vamos pensar no funcionamento de cada uma dessas coisas. Para isso podemos apelar para modelos bem esquemáticos, ou seja, conceitos apenas com os detalhes essenciais de cada uma dessas coisas:

1. Casa: caixa feita de material rígido, com portas trancáveis, usada para proteger pessoas e bens. Uma casa não é apenas isso, mas suponha que seja neste momento!
2. Deslocamento na cidade: podemos supor aqui que seja feito via transporte público.
3. Trabalho com o computador: mais pra frente, neste guia, trataremos do funcionamento esquemático do computador. Por enquanto podemos assumir que ele é uma caixa onde entram e saem informações.
4. Telefone celular: idem ao caso do computador anterior: podemos pensá-lo como uma caixinha por onde circulam informações.

Essa é a versão muito simplificada da vida de uma pessoa. Na prática, fazemos muito mais coisas e num nível de detalha muito maior. O importante agora é começar com o básico e complicar somente caso necessário.

O que pode dar errado em cada uma dessas situações? Se quiséssemos detonar o dia dessa pessoa, neutralizá-la ou mesmo roubar as informações que ela possui, o que faríamos?

1. Casa: arrombamento das portas; fingir que somos funcionários de alguma empresa para conseguir entrar e render seus ocupantes; esperar que a pessoa saia de casa e rendê-la; impedir que a pessoa saia de casa; corte de comunicação com o mundo exterior para que ela não consiga acionar a emergência, etc.
2. Deslocamento: a pessoa pode ser atropelada; desastres naturais podem impedi-la de chegar o trabalho; assaltos e sequestros, etc.

3. Trabalho com computador: o computador pode estar grampeado, levando à extração de todas as informações nele colocadas ou alterando as informações para causar danos; ele pode simplesmente parar de funcionar e impedir que a pessoa trabalhe, etc.

4. Telefone celular: veremos que ele pode ser utilizado para rastrear a localização da pessoa; ele pode estar grampeado e as comunicações da pessoa serem interceptadas, etc.

Note que a lista de ameaças sempre é interminável! Podemos continuar, continuar, continuar indefinidamente, mas numa hora teremos que ordená-la e apagar algumas coisas dela, com o seguinte critério:

:: A ameaça é provável? O quanto ela me afeta?

Vale notar que muitas ameaças só são prováveis a partir do momento em que uma pessoa se torna um alvo específico, pois são ameaças que tem um custo para serem realizadas. No entanto, é difícil saber se somos ou não alvos.

Em seguida, podemos partir para as defesas possíveis:

1. Casa: paredes sólidas; portas reforçadas; fechaduras que resistam um bom tempo mesmo sendo atacadas por chaveiros hábeis; janelas blindadas; sistema de comunicação de emergência, etc. Você até pode pensar em morar numa casa escondida! Como seria isso?

2. Deslocamento: atenção no trânsito e nas demais pessoas; usar rotas de baixo risco; sair em horários diferenciados; alternar trajeto para evitar alguém despistando, etc.

3. Computador: adotar as medidas que serão tratadas neste guia, por exemplo usar criptografia no armazenamento e nas comunicações.

4. Telefone celular: idem ao caso do computador: adotar as medidas abordadas ao longo do guia, como por exemplo deixá-lo numa outra sala durante conversas sensíveis.

Da mesma forma como a lista das ameaças, a lista das defesas é interminável. Escolheremos então as nossas defesas de acordo com os seguintes critérios:

1. Custo (financeiro, pessoal, etc).

2. Eficácia.

É importante que as defesas escolhidas de fato representem proteções contra as ameaças que escolhemos combater. Mas podemos também deixar listadas as ameaças que não serão combatidas no momento, para termos consciência de tudo o que nos ameaça.

Lembre-se também que nenhuma defesa é totalmente eficaz ou cobre todos os aspectos de uma dada ameaça.

Juntando isso tudo, teremos o seguinte Checklist ou Modelo de Segurança:

- **Casa:**
  - **Ameaças prováveis:**
    - Arrombamento.
  - **Defesas adotadas:**
    - Portas e janelas reforçadas.
    - Fechaduras que demorem mais de X horas para serem neutralizadas.
  - **Ameaças não cobertas:**
    - Sequestradores disfarçados.
    - etc
- **Deslocamento:**
  - **Ameaças prováveis:**

        * Atropelamentos.
        * Assaltos.
    - **Defesas adotadas:**
        * Atenção ao andar.
    - **Ameaças não cobertas:**
        * Rastreadores de pessoas.
        * Falhas no sistema de transporte.
        * etc
- **Trabalho no computador:**
    - **Ameaças prováveis:**
        * Roubo.
        * Adulteração de informações.
    - **Defesas adotadas:**
        * Armazenamento criptografado (confidencialidade e integridade).
        * Comunicação criptografada (confidencialidade, integridade, autenticidade).
    - **Ameaças não cobertas:**
        * Defeitos no computador.
        * Instalação de programas maliciosos.
        * etc
- **Telefone celular:**
    - **Ameaças prováveis:**
        * Utilização como escuta ambiental.
    - **Defesas adotadas:**
        * Deixar o celular numa outra sala ao realizar conversas sensíveis ao vivo.
    - **Ameaças não cobertas:**
        * Interceptação de conversas telefônicas.
        * Interceptação em comunicadores instantâneos.
        * etc

Esta é uma versão bem simplificada do modelo, mas serve muito bem para começar. Versões complicadas podem incluir inclusive ameaças oriundas da própria adoção de determinadas defesas, etc. Mas não vamos levar isso em conta porque, no momento, seria adotar uma complexidade desnecessária.

Existem vários formatos possíveis para essa lista, descubra a forma que for mais apropriada para a suas necessidades.

O mais importante é extrair do modelo as ameaças prováveis, as defesas, seus limites e as ameaças que não serão cobertas por falta de tempo, energia ou outros recursos. Note que no caso das defesas digitais, foram incluídas as propriedades de segurança da informação mínimas que elas devem implementar (por exemplo confidencialidade, integridade e autenticidade).

Perceba que essa é uma tarefa que requer método e sistemática mas que pode ser feita de forma incremental, isto é, aos poucos, e começar a partir de um brainstorm ou chuva de ideias e passar por uma análise crítica posterior.

Com nosso modelo de ameaças pronto, teremos um conhecimento maior dos **vetores** de ataque prováveis contra nós, isto é, as portas de entradas de ameaças. A esse conjunto de vetores de ataque damos o nome de **superfície de ataque**.

5.3 Resumo

Hora do resumo! Ao pensar numa atividade ou ferramenta, pensamos em três eixos:

1. Funcionamento: entendimento é o primeiro passo.
2. Ameaças: entendendo, conseguimos avaliar as ameaças possíveis.
3. Defesas: conhecendo as ameaças, podemos pensar em defesas.

Todas as atividades relevantes de uma pessoa ou organização podem ser organizadas numa lista, incluindo as possíveis e prováveis ameaças àquelas atividades juntamente com as defesas a serem adotadas.

Essa lista é chamada aqui de Checklist de Segurança ou Modelo de Ameaças.

5.4 Atividades

1. Esboce um modelo de ameaça básico. Liste suas atividades e prováveis ameaças. Depois organize-as em ordem de acordo com as defesas mais importantes que você pretende adotar.
2. Com o seu modelo de ameaças, você conseguiria planejar um cronograma para adotar algumas práticas de segurança? Tente ser razoável e honesto(a) com você mesmo(a) e escolher um calendário factível!

5.5 Referências

- Plano de Autodefesa.

CAPÍTULO 6

Comunicação Digital

6.1 Funcionamento

Trataremos agora a respeito de segurança em sistemas digitais. Para isso, usaremos uma versão modificada da teoria clássica da comunicação.

```
.                    grampo ativo ou passivo
                                |
                                |
Emissor/a ---meio-----------meio-------------meio------ Emissor/a
Receptor/a           -----mensagem-1------>              Receptor/a
    1                <----mensagem-2-------                 2
```

Classicamente, diremos que toda a comunicação é baseada pelo menos por um **emissor** que envia uma **mensagem** para um **receptor** através de um **meio**. A comunicação pode ser bidirecional, indicando que uma das pontas da comunicação pode ser emissora e receptora de mensagens ao mesmo tempo.

Esse modelo está incompleto no que diz respeito à segurança e à privacidade: ele não contém um elemento que está cada dia mais presente nas comunicações, que é o **grampo** ou **escuta**, isto é, a interceptação da comunicação.

É fundamental considerarmos a interceptação ou grampo como entidade sempre presente na comunicação.

Primeiro, porque queremos seguir uma regra geral de simplicidade: se uma comunicação **pode** ser grampeada, assuma que ela está sendo grampeada. Independentemente do grampo estar sendo realizado ou não, ao assumí-lo, você já se protege de antemão.

Em segundo lugar, porque a forma como a comunicação flui no nosso mundo prático se dá através da **cópia** da informação por onde ela passa até chegar ao seu destino. O próprio movimento de uma comunicação, por exemplo de uma onda sonora, pode ser explicado simplificadamente em termos da **cópia** da informação para a posição subsequente seguida pelo apagamento dessa informação.

Isso simplesmente decorre do fato de que uma mensagem se movendo em um meio percorre uma porção do espaço até chegar ao seu destino. Nesse caminho, a mensagem pode ser interceptada sem que nem o emissor ou o receptor consigam perceber. Pode até ser que eles consigam, mas isso não é garantido.

O próprio fato da comunicação passar de um ponto a outro do espaço pode ser entendida, metaforicamente, como a interceptação da comunicação por aquele ponto do espaço. Assim, diremos que a propriedade de todo meio de comunicação é a sua **grampeabilidade**.

Note que os fenômenos envolvidos na transmissão física de informações são mais complexos, mas esta nossa noção intuitiva é suficiente para entendermos porque o grampo deve ser assumido como parte integral da comunicação, mesmo que ele não esteja ocorrendo.

No caso da comunicação por meios digitais, essa noção intuitiva acaba necessariamente sendo um **fato**! Um meio de comunicação digital pode ser entendido, de maneira bem simplificada, como se fosse uma brincadeira de telefone sem fio.

Segundo a Wikipedia,

```
Telefone sem fio é uma tradicional brincadeira popular, na qual uma pessoa
fala uma palavra ou frase (o "segredo") ao ouvido de outra pessoa ao seu
lado, de modo que os demais participantes não escutem ou descubram
imediatamente qual é o "segredo".

A que ouviu o segredo tenta então repeti-lo para o próximo participante, e
assim por diante até chegar ao último participante, que deve contar o
segredo em voz alta. Uma das regras do jogo é que o segredo não pode ser
repetida ao ouvinte da vez.

Por esse motivo é comum o segredo ser mal entendido e por isso passado ao
demais ouvintes de forma cada vez mais deturpada, chegando totalmente
diferente ao ouvinte final, e isso é o que torna a brincadeira divertida. É
possível competir dois grupos para ver qual grupo chega com a palavra mais
fielmente ao destino.

-- https://pt.wikipedia.org/wiki/Telefone_sem_fio_(brincadeira)
```

No caso, a grande diferença entre um meio de comunicação digital é que seu objetivo **intencional** é que a mensagem (ou o **segredo**) não seja deturpado ao chegar ao seu destino, mas que chegue de modo inalterado. Aliás, os sistemas de comunicação foram passando do analógico para o digital justamente porque no digital é mais simples garantir a integridade da informação. Mas essa é outra história...

A brincadeira do telefone sem fio tem ainda outra coisa muito importante a nos ensinar sobre os meios de comunicação digitais: em ambos, a **mensagem** só é um segredo para quem está de fora do jogo: tanto as pessoas os ou os elementos de comunicação envolvidos na brincadeira precisam receber a informação para que possam passá-la para frente.

Ou seja, o **segredo** não está sendo muito bem protegido, né? Se for uma informação sigilosa que só a primeira e a última pessoa do telefone sem fio deveriam conhecer, então o segredo foi para o brejo logo no início da brincadeira.

Chamaremos esta nossa concepção de comunicação com emissor, receptor, mensagem, meio e grampo de **Teoria da Comunicação Hacker**. E chamaremos de **grampeabilidade** esta estranha propriedade dos meios de comunicação – especialmente digitais – de poderem ser grampeados.

É importante entender que num determinado meio de comunicação podem haver vários grampos instalados, pois em cada ponto por onde trafega a informação, pode ser instalado um interceptador que desvie ou copie a mensagem. Assim, toda a vez que pensarmos num meio de comunicação digital, tentaremos esboçar um diagrama básico de funcionamento para, em seguida, mostrar onde podem ser instalado o aparato de vigilância e como se defender dele.

```
.
   ponta                          meio                                ponta
|---------|-------------------------------------------------|---------|
                grampo 1        grampo 2        grampo n
                   |               |               |
```

(continues on next page)

(continued from previous page)

```
emissor  <-> aparelho 1 <-> aparelho 2 <-> aparelho n <-> receptor
receptor                                                  emissor
```

Daqui para a frente, **assumiremos que todos os meios de comunicação estão grampeados**!

AAAAH!!!! Isto é o fim do mundo????

Não.

Veremos que é possível ter um nível razoável de segurança mesmo se houver um grampo instalado nos meios de comunicação. Porém, se as pontas da comunicação estiverem grampeadas, estão o jogo está perdido.

As pontas da comunicação são as portas de entrada e saída entre os meios de comunicação e seus emissores(as) e receptores. Se elas estiverem comprometidas, não há muito o que fazer.

Ao longo do guia, trataremos basicamente de formas de proteger as pontas da comunicação e a mensagem contra a interceptação e adulteração da nossa comunicação.

6.2 Ataques

Já entedemos o funcionamento bem básico e esquemático dos meios de comunicação digital e vimos que eles são intrinsecamente vulneráveis à interceptação de mensagens.

Mas quais são os ataques específicos que podem acontecer? Neste capítulo trataremos dos principais.

6.2.1 Interceptação de dados

O ataque mais básico, e que já citamos de algum modo, é a **interceptação de dados**.

Existem dois tipos: os passivos, que simplesmente copiam silenciosamente a comunicação, e os ativos, que interceptam e modificam a comunicação.

Os grampos ativos são os mais perigosos, pois podem modificar o conteúdo da mensagem ou mesmo inviabilizar as medidas de segurança adotadas para a proteção da mensagem em meios hostis.

Por outro lado, os grampos ativos são mais fáceis de serem detectados caso a comunicação esteja protegida com **criptografia forte e bem implementada**, como veremos adiante no curso.

6.2.2 Interceptação de metadados

Outro ataque básico é a **interceptação de metadados** que, em algumas circunstâncias, é conhecida como **retenção de dados**.

Dizemos que dados são o conteúdo da mensagem, enquanto que os metadados são os **dados de endereçamento** da mensagem, isto é, as metainformações necessárias para que a mensagem consiga chegar até o seu destino.

Os sistemas modernos de comunicação são baseados em **protocolos**, que são basicamente convenções bem definidas de como máquinas podem trocar informações entre si, evitando que a comunicação seja interrompida ou que haja falhas nas transmissões.

Em tais protocolos, é a própria mensagem que possui as informações básicas sobre o seu destino e muitas vezes por onde passou. Isso é muito semelhante ao sistema postal, no qual as cartas possuem endereços escritos no envelope e vão recebendo carimbos conforme passam de um lugar para o outro.

São essas informações, chamadas de metadados que dizem aos sistemas para onde a mensagem deve ser enviada, quem a enviou, em que momento, etc.

Metadados tipicamente contém remetente, destinatário, data de envio e podem incluir assunto, sistemas por onde passou, localização das partes envolvidas na comunicação, etc.

Também podem receber informações adicionais, como duração completa da comunicação, horário de encerramento, quantidade total de informação trocada, etc.

Você pode pensar em metadados como podendo ser compostos por quaisquer informações sobre a mensagem, exceto o próprio conteúdo da mensagem.

```
.
 ____________
|            |    quem fala com quem (emissor, receptor),
| metadados  | -> etc: diz ao meio como enviar a mensagem,
|            |    ou seja, trata do endereçamento, arquivamento,
|------------|    isto é, do ciclo de vida da comunicação.
|            |
|  dados     | -> o que é dito, isto é, a mensagem.
|____________|
```

Na realidade, dados e metadados formam uma matrioska com muitas camadas de significado ou discurso: o que é dado para uma dada interpretação pode ser metadado para outra. Ou seja, se uma informação é dado ou metadado vai depender de como um determinado sistema ou ator a interpreta. Em outras palavras, dados e metadados são noções bem relativas a respeito da informação.

Mas por que essa diferenciação é importante? Além disso, metadados não são informações inofensivas e cuja captura é irrelevante para a segurança?

É importante diferenciar dados de metadados porque hoje em dia o processamento de metadados representa a maior parte da vigilância automática: enquanto que uma boa interpretação do conteúdo da comunicação atualmente necessita da ação humana, os metadados podem ser interpretados e processados por computadores sem intervenção humana.

Essa diferença decorre do fato de que os metadados estão codificados de acordo com os protocolos de comunicação digital. Assim como os metadados são processados automaticamente para que uma mensagem chegue ao seu destino, eles também podem ser processados para fins de vigilância.

Ou seja, quando mensagens são interpretadas automaticamente, seus metadados também são processados automaticamente, enquanto que os dados são, em geral, processados apenas parcialmente, necessitando de alguma pessoa para fazer a interpretação completa.

Mesmo nos casos em que a interpretação parcial dos dados é realizada, o seu custo computacional ainda é alto. É muito barato guardar dados e metadados mas processar automaticamente apenas os metadados. E é mais barato ainda apenas gravar e processar automaticamente os metadados.

Os metadados não são irrelevantes! Muito pelo contrário!

Pela facilidade de coleta, processamento e interpretação, os metadados são informações muito sensíveis. Com eles, é possível reconstruir toda a rede social de comunicação entre um conjunto de usuários(as), descobrindo quem fala com quem, quais são as pessoas mais comunicativas, quem se relaciona mais com quem e assim por diante. Tudo isso sem precisar prestar atenção no conteúdo da comunicação!

Noutras palavras, a coleta dos metadados permite a criação do «grafo» social, que é o desenho da rede de relacionamento entre as partes envolvidas na comunicação e é uma informação tão valiosa quanto a coleta dos dados.

Podemos notar o quanto captura apenas dos metadados já é suficiente para obter muitas informações sobre a comunicação: detalhes de quem está comunicando com quem, assunto, duração das mensagens, etc.

No entanto, a interceptação de metadados acabou por não ser considerada como grande violação da privacidade, o que é um grande perigo.

Existem inclusive leis em todo o mundo que obrigam empresas que dão acesso à internet ou que distribuem conteúdo de gravarem automaticamente metadados de acesso dos usuários dos seus sistemas. Os metadados são mantidos por

períodos de meses ou até anos.

Essa prática é conhecida como **retenção de dados** e é justamente realizada para facilitar a identificação de usuários.

Em algumas situações a retenção de dados pode ser proibida, mas mesmo assim ela ocorre. Agências governamentais e empresas podem estar coletando informações de usuário com ou sem consentimento.

Uma interceptação de comunicação pode, ao mesmo tempo, grampear toda a mensagem, isto é, tanto os seus dados quanto os seus metadados. Assim, é importante pensar em medidas de proteção tanto dos dados quanto dos metadados da mensagem. Diferentes tecnologias protegem dados, metadados ou ambos.

6.3 Defesas

Quais as defesas contra a interceptação de mensagens, seja de dados, metadados ou ambos?

Neste capítulo trataremos dos tipos genéricos de defesa, enquanto que nos capítulos posteriores trataremos efetivamente das ferramentas práticas.

É bom notar que a segurança da informação é um campo em mudança constante. Muitas vezes uma solução tem um «prazo de validade» que depende de alguma nova descoberta de falha ou mudanças na própria arquitetura dos sistemas.

Por exemplo, uma solução que funciona hoje pode ser insuficiente no futuro.

6.3.1 Defesas físicas

Podemos pensar em defesas físicas como o controle efetivo dos dispositivos, equipamentos e linhas de transmissão de mensagens.

Isso requer um custo muito alto e depende de muitas pessoas e equipamento para que seja efetivo. E é um problema de pouca solução: se mais pessoas e equipamentos são necessários para fiscalizar e proteger as pessoas e o equipamento existente, quem vai proteger essas novas pessoas e equipamentos?

Ou seja, a proteção física de toda uma infraestrutura nem é prática e nem é totalmente efetiva.

Podemos, no entanto, escolher proteger as partes da comunicação mais sensíveis a ataques.

Se tivermos de dar prioridade a algumas partes, diria que precisamos proteger as pontas da comunicação e utilizar criptografia de ponta a ponta para que a mensagem criptografada possa trafegar num meio de comunicação desprotegido.

A mensagem pode estar criptografada durante o trânsito e tornar inefetiva a interceptação no meio de comunicação, mas é nas pontas da comunicação que ela precisa ser descriptografada. Se as pontas estiverem desprotegidas ou em poder do atacante, o risco de captura da mensagem é muito alto.

Assim, uma defesa física das pontas é importante. Uma ponta pode ser seu computador ou seu telefone móvel. Deixar esses aparelhos em locais desprotegidos ou longe da sua atenção não é uma boa ideia.

Ao mesmo tempo, devemos considerar alguns aspectos:

1. O velho dito de que «a ocasião faz o ladrão»: você não precisa ser um alvo, isto é, não é preciso que alguém esteja atrás de você para que seu equipamento seja comprometido.
2. Defesa física não significa apenas roubo do seu aparelho, mas também a instalação de equipamentos físicos de grampo.
3. Mesmo que você defenda fisicamente o seu equipamento, ele ainda estará sujeito a invasões de software. Tirando o roubo de equipamento para fins econômicos, as ameaças de software são as mais importantes. Mas ter um mínimo de cuidado com a defesa física não faz mal a ninguém.

Ou seja, a defesa física é importante, necessária mas não suficiente para proteger sua comunicação.

6.3.2 Defesas Computacionais

Do que adianta ter um equipamento fisicamente seguro se o seu software está cheio de problemas ou se os protocolos de comunicação utilizados são inseguros?

Você pode proteger:

- Os softwares e as informações que estão armazenadas no seu computador.
- As mensagens que entram e saem do seu computador.

As mensagens e o conteúdo armazenado no computador podem ser protegidas usando criptografia.

Não existe um único tipo de criptografia, protocolo ou programa de computador que faça isso. Também não existe um único sistema criptográfico que proteja todas as informações do computador.

Em algumas situações você até pode agregar diversas comunicações num único canal criptografado, mas infelizmente em geral a criptografia precisa ser feita caso a caso. Ao longo do guia veremos diversas ferramentas que possuem suporte a criptografia.

6.3.3 Defesas Jurídicas

A interceptação e retenção de dados e metadados pode ser feita legal ou ilegalmente. Sabemos que ela pode acontecer mesmo nas situações em que a lei proíbe.

Legislações fortes podem evitar a interceptação generalizada da população, mas isso vai depender também do contexto político.

É importante conhecer seus direitos. Aqui isto não será detalhado, mas deixamos referências de onde você pode encontrar essas informações.

6.3.4 Defesas Sociais

As defesas sociais são aquelas tomadas por todo um grupo, seja um conjunto de amigos, família, empresa, grupos de interesse, comunidade ou mesmo de toda uma sociedade.

Essas defesas podem ser combinadas, o que é fácil de se fazer num grupo pequeno, para que exista uma uniformidade no padrão de segurança daquele grupo. Conforme o número de pessoas aumenta, ter uma mesma política de segurança passa a ser mais difícil.

É importante levar em conta que o nível de segurança tende a ser o nível de segurança do elo mais fraco. Ou seja, mesmo que algumas pessoas tenham um nível mais alto de autodefesa, o grupo continuará bem vulnerável por conta das pessoas com nível mais baixo.

Isso pode ser resolvido por compartimentalização, o que nem sempre é bom, mas também pela busca de um padrão mínimo de segurança que todas as pessoas do grupo queiram concordar, consigam aprender e pratiquem.

6.4 Resumo

1. Temos que considerar a interceptação ou grampo como entidade sempre presente na comunicação, independentemente dele estar ou não ocorrendo.
2. Os ataques fundamentais da vigilância das comunicações são a interceptação de dados e a de metadados. Dados constituem o conteúdo da mensagem e metadados são informações sobre a mensagem, por exemplo endereçamento. Ambos os tipos de interceptação são perigosos.
3. Contra a interceptação de mensagens existem defesas físicas, computacionais, jurídicas ou sociais.

6.5 Atividades

1. Qual seria o «Kit Básico» de segurança que toda a pessoa de um grupo deveria ter, por exemplo colegas de trabalho? Esboce um grupo hipotético e um kit básico de procedimentos e ferramentas de segurança.

   Você pode se basear nas atividades de capítulos anteriores caso você já tenha esboçado seu Checklist de Segurança.

6.6 Referências

- Telefone sem fio (brincadeira) - Wikipédia, a enciclopédia livre.
- Vigilância das comunicações pelo Estado Brasileiro e a proteção a direitos fundamentais. Em especial os quadros das páginas 10 a 13.

CAPÍTULO 7

Criptografia Básica

7.1 Funcionamento

Este não é um guia sobre criptografia, mas daremos os conceitos mais básicos para que você consiga usá-la na vida prática sabendo em linhas gerais o que está – ou pelo menos deveria estar – acontecendo na sua comunicação criptografada.

A criptografia é o método de codificar dados e metadados para que a informação possua um ou mais critérios de segurança como confidencialidade, integridade e autenticididade.

Em sua aplicação mais básica, a criptografia é a técnica de codificar mensagens de tal modo que apenas quem possuir o segredo de como decodificá-las pode acessar seu conteúdo original.

A criptografia ainda pode ser utilizada para checar a autenticidade de uma mensagem, ou seja, checar a autoria da mensagem, e ainda para verificar se a mensagem não foi adulterada em seu trânsito.

Essas e outras propriedades da segurança da informação podem ser obtidas juntas ou separadas dependendo do sistema criptográfico em uso.

A criptografia é baseada num processo onde a mensagem original é combinada com uma chave de codificação e uma operação criptográfica para produzir um texto codificado:

```
mensagem original -> operação cifrar, chave -> mensagem codificada
```

Para obter a mensagem original a partir da mensagem criptográfica, é preciso ter acesso a uma chave que permitae realizar uma operação no caminho inverso:

```
mensagem codificada -> operação decifrar, chave -> mensagem original
```

Como estamos lidando com criptografia em sistemas digitais, tanto a mensagem original quanto a codificada e as chaves utilizadas são apenas números.

A mensagem codificada pode então trafegar por qualquer meio de comunicação, pois suas propriedades de segurança da informação estarão operando. Ou seja, essa criptografia, desde que bem implementada, oferece **confidencialidade** à comunicação.

Por exemplo, se a mensagem codificada tiver a propriedade da confidencialidade, ela só poderá ser lida por quem tiver condições de decifrá-la, isto é, por quem tiver a chave de criptografia correta.

Existem dois tipos de chaves:

1. Chaves simétricas.
2. Chave assimétricas.

Veremos nos dois próximos capítulos como opera a criptografia com cada uma delas.

7.2 Chaves simétricas

Na criptografia baseada em chaves simétricas, ambas as partes de uma comunicação compartilham a mesma chave criptográfica e esta é usada tanto para cifrar quanto para decifrar mensagens.

Assim, é crucial para o funcionamento seguro da comunicação que a chave seja mantida em segredo. Revelar a chave significa revelar a comunicação e até permitir que terceiros possam usar a chave para enviar mensagens.

A criptografia de chave simétrica é bastante utilizada, porém na prática ela oferece um problema: como compartilhar a chave entre as partes envolvidas?

No caso de duas pessoas se encontrarem pessoalmente para combinarem uma chave simétrica, não há problema. Ou se a chave for transmitida de uma para outra num canal de comunicação que ambas considerem seguros por terem efetivamente controle físico sobre ele.

Também não há problema no caso da criptografia usada para criptografar conteúdo armazenado em discos, pois a chave não precisa ser transmitida.

Mas o que acontece se quisermos compartilhar a mesma chave com uma pessoa distante e usando a internet como meio? Uma interceptação na comunicação poderia facilmente capturar a chave durante sua transmissão, comprometendo toda a criptografia posterior.

E não poderíamos passar a chave usando uma comunicação criptografada, pois o outro lado precisaria da própria chave para poder decifrá-la!

Uma das formas de contornar parcialmente esse problema é a utilização da criptografia de chave assimétrica.

7.3 Chaves assimétricas

Já a criptografia assimétrica é baseada em pares de chaves:

1. Uma chave pública, que pode (mas não precisa) ser divulgada amplamente.
2. Uma chave privada, que deve ser mantida em sigilo.

Cada parte envolvida na comunicação precisa de um par de chaves. Suponha uma comunicação entre Fulana e Beltrana:

1. Fulana possui uma chave privada que chamaremos de Fulana Privada. E uma chave pública que chamaremos de Fulana Pública.
2. O mesmo ocorre com Beltrana: ela tem uma chave Beltrana Pública e uma Beltrana Privada.

A comunicação entra ambas funciona da seguinte maneira:

1. Fulana e Beltrana trocam suas chaves públicas. Isso quer dizer que Fulana recebe uma cópia de Beltrana Pública. Beltrana, por sua vez, recebe uma cópia de Fulana Pública.
2. Fulana pode criar uma mensagem para Beltrana usando o seguinte caminho

```
mensagem original -> operação cifrar, chave Beltrana Pública -> mensagem codificada
```

Após receber a mensagem condificada, Beltrana pode decodificá-la usando o esquema

```
mensagem codificada -> operação decifrar, chave Beltrana Privada -> mensagem original
```

Se Beltrana quiser responder com outra mensagem, ela deve seguir o seguinte caminho:

```
mensagem original -> operação cifrar, chave Fulana Pública -> mensagem codificada
```

E Fulana poderá decifrá-la usando

```
mensagem codificada -> operação decifrar, chave Fulana Privada -> mensagem original
```

Na prática, com a criptografia de chaves assimétricas, só esses caminhos são viáveis para codificar e decodificar mensagens.

Com o uso de computadores para a realização das operações, a criptografia se torna prática e eficiente.

7.4 Identificação

A criptografia de chaves assimétricas resolve o problema da transmissão da chave num meio desprotegido, já que a captura da chave pública por oponentes não gera perigo adicional para a comunicação criptografada.

Mas essa transmissão de chaves não resolve um problema adicional: como garantir que a chave não foi interceptada e substituída por outra, falsa?

E se alguém trocar a chave pública de uma pessoa por uma falsa e começar a agir como se fosse essa pessoa?

Ou seja: como fazer a relação entre uma pessoa, instituição ou sistema e uma chave pública? No nosso contexto de criptografia básica, podemos chamar esse processo de **identificação** da chave pública: a quem ela pertence? Quem tem o controle sobre ela?

A transmissão da chave pública não resolve todo o problema da segurança da comunicação. Para confirmar se uma chave pública pertence a alguém, precisamos ter alguma forma adicional para checá-la.

A maneira mais imediata é uma confirmação da chave pública ao vivo com ambas as partes da comunicação certificando as duas chaves públicas, isto é, uma chave pública por parte envolvida.

Ou então elas podem eleger um canal de comunicação que elas controlem ou usar alguma outra forma de identificação: por exemplo, se as pessoas se conhecem e concordarem com a relativa segurança do método, podem usar uma chamada telefônica e ditarem um para o outro o conteúdo de suas chaves públicas.

Isso pode funcionar bem se um já conhece a voz do outro ou da outra e se assumirmos que não existe um interceptador capaz de simular vozes convincentes.

O importante aqui é cada parte concordar com o processo de identificação.

Mas existe outro problema: muitos pares de chave que oferecem alguma segurança tem um tamanho grande, o que complica muito a confirmação do tamanho da chave.

Para resolver isso utiliza-se a chamada **impressão digital** de uma chave pública, como veremos no próximo capítulo.

7.5 Impressão digital

Digamos que a impressão digital de uma chave seja sua versão resumida. É possível que duas chaves públicas possuam a mesma impressão digital, mas isso é muito difícil de acontecer. Sendo menor que a chave original mas ainda assim

praticamente única, é mais fácil utilizar uma impressão digital.

Impressões digitais existem tanto para criptografia simétrica quanto assimétrica.

A impressão digital é uma sequência de números expressados tipicamente usando o **sistema hexadecimal**, que utiliza os números de 0 a 9 e os algarismos de A a F:

```
268F 448F CCD7 AF34 183E  52D8 9BDE 1A08 9E98 BC16
```

Muitos softwares de criptografia possuem uma função de identificação de chaves, ajudando tanto no processo de identificação quanto informando ao usuário se determinadas chaves dos seus contatos já foram identificadas.

7.6 Assinatura digital

Já vimos que podemos trocar chaves e fazer a identificação entre uma chave e uma pessoa ou entidade. Queremos também ter um processo para checar se uma mensagem foi enviada por determinada pessoa, entidade ou sistema.

Como podemos fazer essa verificação? Como podemos adicionar **autenticidade** à nossa comunicação?

O próximo passo na criptografia é o uso das assinaturas digitais. Aqui trataremos apenas do caso da criptografia assimétrica, onde uma assinatura digital pode ser criada pelo seguinte processo:

```
mensagem original -> operação assinar, chave privada -> assinatura da mensagem␣
↪original
```

Ou, alternativamente:

```
mensagem codificada -> operação assinar, chave privada -> assinatura da mensagem␣
↪codificada
```

Ou seja, para a criação de uma assinatura deve ser utilizada a chave privada.

É possível também apenas assinar uma mensagem, sem criptografá-la, isto é, sem codificar seu conteúdo:

```
mensagem -> operação assinar, chave privada -> assinatura
```

A mensagem – codificada ou não – pode assim ser transmitida num meio qualquer juntamente com a assinatura e, na outra ponta, ser verificada.

Para checar a assinatura, a seguinte operação é usada:

```
mensagem, assinatura -> operação verificar, chave pública -> confirmação ou não-
↪confirmação
```

Voltando ao nosso exemplo de Fulana e Beltrana, Fulana pode assinar uma mensagem usando

```
mensagem -> operação assinar, chave Fulana Privada -> assinatura
```

Em seguida, Fulana envia a mensagem e a assinatura para Beltrana, que verifica a procedência da mensagem usando

```
mensagem, assinatura -> operação verificar, chave Fulana Pública -> confirmação ou não
```

Ou seja, para criar a assinatura, Fulana usa sua chave privada, enquanto que Beltrana pode checar a assinatura usando a chave pública de Fulana!

De quebra, a checagem de assinatura ainda oferece a propriedade da **integridade** à nossa comunicação, já que mensagens que não puderem ter sua assinatura verificada podem conter erros de transmissão ou terem sido adulteradas em trânsito.

Se a mensagem estiver apenas assinada, então uma interceptação poderá acessar seu conteúdo, mas não conseguirá adulterar a mensagem sem que ocorra uma falha na checagem da assinatura.

Em várias aplicações apenas a assinatura digital é utilizada, por exemplo para permitir que um comunicado ou uma versão de um software publicamente distribuídos possam ser verificados.

Mas, para proteger o conteúdo da mensagem, recomenda-se utilizar tanto a criptografia do conteúdo quanto uma assinatura digital.

Tanto a mensagem original quanto a mensagem codificada podem ser assinadas e essa é uma escolha que depende da implementação específica de criptografia que está sendo usada. Em caso de possibilidade de escolha, assine e então criptografe.

7.7 Certificação: a rede de confiança

É possível até **assinar uma chave pública**:

1. Suponha que Fulana e Beltrana troquem chaves públicas e se identifiquem mutuamente, ou seja, atestem de algum modo que as chaves públicas realmente pertençam a uma e à outra.
2. Agora, imagine que Beltrana viaje para longe e encontre com Sicrana. Beltrana e Sicrana também trocam chaves públicas e realizam a identificação das chaves.
3. Mas Sicrana também quer ter alguma forma de identificar se a cópia da chave de Fulana, com quem ela nunca encontrou, também é válida.
4. Se Sicrana confia em Beltrana enquanto capaz de identificar Fulana corretamente, então Sicrana pode simplesmente consultar Beltrana a respeito dessa identificação. Noutras palavras, Beltrana pode **certificar** Sicrana sobre a chave de Fulana.
5. Uma forma de certificar uma chave pública é criar uma assinatura nessa chave.

A certificação usando assinatura funciona de modo análogo à assinatura de uma mensagem, com a diferença que a mensagem é a própria chave pública.

Assim, Beltrana pode criar uma assinatura da chave de Fulana, deixá-la disponível publicamente ou então enviá-la para Sicrana.

Sicrana, por sua vez, pode checar essa assinatura e, caso a assinatura seja válida e Sicrana confie na capacidade de Beltrana de realizar a identificação correta de Fulana, ela pode também criar uma assinatura sobre a chave de Fulana.

A certificação cria um esquema de cadeia ou rede de confiança que permite que pessoas, instituições e sistemas distantes identifiquem-se uns aos outros.

Note que a confiança aqui não implica em confiança irrestrita, mas apenas uma atestação restrita de que determinada chave pública é considerada mesmo como pertencente a determinada pessoa.

Esse conceito é muito útil na implementação prática da segurança da informação e é utilizado diariamente, como você verá a seguir no guia.

7.8 Sigilo futuro

O último conceito sobre criptografia deste guia é chamado de **Sigilo Futuro** e é muito importante para a proteção a longo prazo de uma comunicação.

Suponha que Fulana e Beltrana trocaram chaves públicas, se identificaram mutuamente e usam criptografia para a comunicação diária.

Suponha que isso ocorra por muitos anos. E que por muitos anos um espião esteja gravando toda essa comunicação.

Sem ter pelo menos uma das chaves privadas – a de Fulana ou Beltrana – o espião não conseguirá fazer nada além disso: gravar as mensagens criptografadas.

Mas suponha agora que, num belo dia, o espião consiga roubar uma das chaves privadas. A partir deste momento o espião pode decifrar retrospectivamente todas as mensagens trocadas entre ambas as partes que sejam decifráveis com a chave roubada. Se ambas as chaves forem obtidas, o sigilo de toda a comunicação foi pro espaço.

E agora, o que fazer?

Bom, uma solução simples seria fazer com que Fulana e Beltrana destruíssem periodicamente seus pares de chaves depois de substituí-las por pares novos. Elas poderiam, antes de destruir as chaves antigas, usá-las para identificarem as novas, num processo conhecido como **rolagem de chaves**.

Assim, se o espião capturasse uma chave privada, ele só teria acesso a um pedaço menor da comunicação trocada.

Com isso, Fulana e Beltrana obtém uma propriedade da comunicação criptografada chamada de **sigilo futuro**, que significa a proteção da maior parte da comunicação no caso de perdas futuras de material criptográfico.

O sigilo futuro pode ser obtido manualmente com a rolagem periódica de chaves, mas também pode ser feito automaticamente. Alguns sistemas criptográficos possuem modos de operação com sigilo futuro.

7.9 Ataques

Do que falamos até agora, podemos extrair diversos ataques a sistemas criptográficos e incluir mais alguns outros:

1. O sistema criptográfico pode ter falhas conceituais: neste caso, o próprio princípio ou a matemática do sistema possui falhas que podem ser exploradas para quebrar a segurança da informação.
2. O sistema criptográfico pode ter falhas na implementação: aqui, é o hardware ou o software criptográfico que apresenta defeitos que podem ser usados para quebrar a segurança.
3. O sistema criptográfico pode ser mal utilizado, quando o uso incorreto de um sistema ocasiona em quebras na segurança. Isso depende muito de onde e como um sistema é usado, do nível de conhecimento de quem o utiliza e assim por diante.
4. Roubo de material criptográfico, isto é, roubo de chaves privadas. Isso pode ser usado para forjar mensagens e assinaturas e também para decifrar mensagens.

Alguns ataques podem levar a outros: falhas conceituais, de implementação ou de uso podem levar ao roubo do material criptográfico.

É importante saber que a criptografia não resolve tudo. Ela não é o remédio para todos os problemas de insegurança na comunicação digital. Mas ela é uma medida importante e necessária.

A criptografia também não é infalível. Ela é baseada no conhecimento matemático e na capacidade técnica de um dado momento da história. Nada garante que, num dado momento, não seja descoberta uma forma de detonar um sistema.

Isso é o equivalente a dizer que é possível num dado momento a descoberta de falhas conceituais ou de implementação no sistema criptográfico.

É possível até que alguém já saiba fazer isso, mas que prefira manter esse conhecimento em segredo por razões óbvias: se a falha se torna pública, ela pode ser corrigida ou o sistema ser substituído.

Mas, nesses casos, não é apenas a sua criptografia que vai por água abaixo, mas a criptografia utilizada por milhões de pessoas, por empresas e instituições.

Até onde sabemos, o conhecimento e a capacidade dos atores mais poderosos hoje no mundo não é capaz de quebrar uma criptografia forte e bem implementada. Ao invés disso, esses atacantes tem investido na **trapaça** e em métodos de invasão que contornem a criptografia explorando outras vulnerabilidades nos sistemas.

7.10 Defesas

O que é uma criptografia forte e bem implementada? Como podemos avaliar isso?

Para responder essa pergunta, seria necessário entrar nos detalhes de como a criptografia funciona, o que deixamos para as nossas referências do guia.

Se não temos condições, pelo menos no momento, de entender mais como a criptografia funciona, podemos ao menos confiar na opinião da comunidade de segurança sobre quais padrões de criptografia são recomendáveis.

O mesmo acontece com as implementações, isto é, os softwares que utilizam de determinados processos criptográficos.

Isso significa que não devemos usar um software que se diz seguro apenas por sua propaganda, porque o site dele é bonito ou porque ele possui um cadeado no seu logotipo. Existem centenas de softwares que se propõem como alternativas viáveis para comunicação segura.

Então tome cuidado e use apenas softwares que você pode avaliar a segurança por conta própria ou confie na opinião da comunidade de pesquisa.

Além desta importante observação, seguem outras dicas:

1. Proteja as suas chaves privadas! Você pode usar até a criptografia de armazenamento do seu dispositivo para isso, como veremos adiante.
2. Mantenha seus softwares de criptografia sempre atualizados. Softwares desatualizados podem conter falhas conhecidas e portanto fáceis de serem exploradas por qualquer pessoa.

   Muitos sistemas possuem procedimentos automáticos de atualização que já dão conta disso. Outros precisam que a atualização seja feita manualmente de tempos em tempos. Existem, ainda, fontes de notícia de softwares ou de segurança que informam sobre vulnerabilidades encontradas e atualizações disponíveis.

Daremos dicas mais específicas quando abordarmos os softwares de criptografia recomendados neste curso.

7.11 Resumo

- Chaves simétricas e assimétricas.
- Cifrar e decifrar mensagens: fornecem **confidencialidade**.
- Assinaturas digitais: fornecem **autenticidade** e **integridade**.
- Identificação de chaves com pessoas, entidades ou sistemas: fornecem **autenticidade**.
- A identificação feita por terceiros é chamada neste guia de **certificação**.
- Use apenas soluções de criptografia forte que sejam consagradas pela comunidade de segurança.

7.12 Atividades

1. Você conseguiria dizer quais meios de comunicação que você utiliza que estão com criptografia disponível e ativada? Você conseguiria classificar a qualidade da criptografia? Faça uma pesquisa rápida!

7.13 Referências

- Abre-te Sésamo: as senhas da nossa vida digital | Oficina Antivigilância.

- Response to XKCD - Passwords.

CAPÍTULO 8

Autenticação com Senhas

8.1 Funcionamento

Para ter acesso a determinados sistemas ou lugares, pode ser necessário fornecer algo para que ocorra uma **autenticação**, isto é, uma permissão de acesso.

O processo de autenticação consiste em fornecer uma prova de acesso a um sistema e consequentemente receber a permissão de acesso ao mesmo.

Existem vários tipos de autenticação:

1. A autenticação pode ser baseada em algo que você carrega: por exemplo um cartão de crédito, um crachá ou documento de identificação.
2. A autenticação pode ser baseada em algo que só você ou um grupo restrito de pessoas sabe. Chamamos essa informação de **senha**.
3. Ela também pode se basear em alguma característica física sua e nesta caso estamos falando de **biometria**.

Neste curso falaremos apenas sobre senhas, que é a forma de autenticação mais utilizada na comunicação digital.

Biometria pode ser forjada e algo que você carrega no bolso pode ser roubado. Mas extrair uma senha da sua mente já envolve mais trabalho. Daí o poder das senhas!

A ideia de uma senha é muito simples: só você ou um grupo restrito de pessoas tem acesso à senha, isto é, só quem deve ter a permissão de acessar um sistema é quem deve ter as credenciais de acesso.

8.2 Ataques

Alguns sistemas são baseados num único fator de autenticação. Outros em dois ou até três: algo que você carrega consigo, algo que você sabe e algo que faz parte de você.

Note que, no limite, todas essas três características podem ser roubadas ou forjadas, com inúmeros graus de sofisticação. Ou seja, a autenticação a um sistema será sempre limitada.

Os principais ataques à autenticação com senha são:

- Esquecimento: você esqueceu sua senha e ficou fora do sistema!
- Ataques marotos: alguém pode simplesmente te induzir a fornecer a senha. Por exemplo num sistema falso mas que pareça ser o original.

  Ou alguém que pergunte a senha pra você, por exemplo se oferecendo para avaliar se a sua senha é boa ou ruim. Existem até sites que se oferecem a isso. Não confie neles! Não confie em ninguém para guardar ou avaliar sua senhas!
- Surfistas de ombros, do inglês **shoulder surfing**, é o ataque para obtenção de senhas baseada no fenômeno do zoião, isto é, em alguém ou algum dispositivo observando diretamente você digitando sua senha.

  Existem também métodos indiretos para fazer essa observação.

  Um método simples para evitar esse tipo de safadeza é tapar a visão do teclado e das mãos no momento da digitação. Por exemplo, você pode tampar seu laptop com a tela enquanto digita a senha.
- Interceptação no meio de transmissão ou recepção de uma senha. A senha pode ser digitada num teclado que possui um grampo do tipo keylogger instalado. Ou a senha pode ser enviada para outro local sem que haja criptografia implementada na transmissão. Ou mesmo essa criptografia pode ser ruim e revelar o conteúdo da senha.
- Alguém pode extrair senhas em interrogatórios. Ou achar senhas salvas no próprio dispositivo de acesso, em anotações ou até em lixo de escritório, acredite se quiser!
- Às vezes, uma senha nem precisa ser roubada. Ela pode ser descoberta:
  - O chamado «Ataque de Força Bruta» consiste em descobrir uma senha usando da tentativa e do erro. Computadores conseguem tentar várias combinações num período de tempo curto.

    Se o tamanho de uma senha for curto, o que pode ocorrer em sistemas que impõem um tamanho máximo, então o tempo para descobrir a senha por tentativa e erro também é curto.

    É claro que tentar todas as combinações possíveis pode demorar muito tempo. Para reduzir o intervalo entre várias tentativas e um sucesso, os atacantes partem de um conjunto de hipóteses sobre uma senha.

    Uma das hipóteses é que a senha é feita de uma ou mais palavras conhecidas.

    Existem os chamados dicionários, que são conjuntos de senhas ou palavras usadas como base nas tentativas. Esses dicionários podem ser compostos por conjuntos de senhas mais comuns encontradas por aí ou estatisticamente relevantes. Sim, existem estatísticas sobre senhas populares! E podemos dizer que uma das piores características de uma senha é a sua popularidade!

    Assim, ataques de força bruta podem tentar inúmeras combinações de senhas e palavras comuns.

    Ataques mais refinados podem ainda utilizar outros padrões estaticamente conhecidos para diminuir ainda mais o conjunto de possibilidades de descoberta.
  - Se você usa como senha alguma informação sobre a sua vida, de pessoas próximas ou algo do tipo, você estará automaticamente diminuindo a segurança da sua senha.

    Muita gente usa datas importantes, como aniversários e outras informações pessoais como senhas, porque são mais difíceis de serem esquecidas. Mas, com isso, acabam se esquecendo que esse tipo de escolha facilita a obtenção de senhas por algum atacante que consiga obter essas informações.

    Mesmo que você misture datas e informações pessoais conhecidas, a quantidade de tentativas necessárias para descobrir sua senha é baixa o suficiente para uma série de tentativas automatizadas ter sucesso.

8.3 Defesas

Como proteger uma senha de roubos? Aliás, o que é uma boa senha?

Podemos pensar em algumas características importantes para uma senha decente:

1. Memorizável: uma senha muito difícil de lembrar pode levar ao seu esquecimento e ser difícil de digitar.

   Já uma senha muito fácil de lembrar também pode ser muito fácil de alguém descobrir. Senhas muito fáceis em geral também tem um tamanho pequeno, então pense num tamanho mínimo e memorizável quando criar sua senha.

2. Difícil de descobrir: quanto mais difícil de descobri-la, melhor, mas isso pode acarretar numa complexidade da senha que a torna difícil de lembrar.

3. Pouco ou não compartilhada: se você usa a senha para uma coisa, e uma única coisa apenas, é mais difícil dela ser descoberta. Quanto mais compartilhada, maior o risco, pois a superfície de ataque à senha aumenta.

   Esta característica vem diretamente do princípio da compartimentalização: se uma senha for comprometida, o dano estaria restrito apenas a um ou poucos sistemas.

   Uma senha roubada pode ser usada como tentativa para invadir outros sistemas. Se você usa a mesma senha para mais de um sistema, e ela for roubada, trate logo de mudar a senha em todos esses sistemas.

A verdade é que não existe uma regra geral para uma boa senha. Porque qualquer regra acaba fornecendo um padrão para a construção de senhas. E aqui queremos justamente libertar sua imaginação do máximo possível de padrões.

O importante é respeitar ao máximo essas três características: ser memorizável, difícil de descobrir e minimamente compartilhada entre pesssoas e sistemas.

8.3.1 Exemplos de criação de senhas

Vamos dar alguns exemplos de criação de senhas razoáveis. Estas senhas que vamos gerar agora não são seguras, já que as estamos divulgando não só para você, mas para o resto do universo!

A intenção aqui é mostrar algumas técnicas possíveis para a criação de senhas para que você possa descobrir qual é a forma que funciona mais para você.

Aqui vão algumas técnicas:

1. Crie uma sequência de símbolos o mais aleatória possível. Por exemplo **6e»I‘g[r 7YV!7P**.

   Muitos sistemas permitem que a senha possuam espaços e até combinações de caracteres especiais, o que é interessante. Mas, nesses casos, você pode se confundir se tiver de digitar a senha em teclados ou sistemas com diferentes configurações.

   Essa senha pode ser gerada de várias maneiras. Mas tome cuidado que às vezes a nossa seleção manual pode não ser tão boa. Por exemplo, digitar a esmo no teclado pode produzir sequências bem preditáveis pelo fato de nossa digitação estar «viciada» a teclar estatisticamente em um grupo restrito de teclas ou a seguir um padrão de digitação já bem determinável.

   Assim como é fácil gerar essa senha, também é fácil programar um computador para fazer o mesmo e tentar usar senhas geradas aleatoriamente para acessar sistemas.

   Esse tipo de senha também tende a ser difícil de ser lembrado, então seu uso deve ser avaliado com cuidado.

2. Crie uma palavra qualquer. Isso mesmo, invente uma palavra! Por exemplo **fletuciladamente**. Não faço a mínima ideia do que ela significa. Na real, ela não quer dizer nada. Tanto melhor!

   A facilidade aqui é que temos uma memória muito boa para decorar palavras pronunciáveis. E com pouca dificuldade podemos criar senhas de tamanho razoável.

   Note que existem muitos padrões gramaticais que são aplicados sem que levemos em conta ao criarmos palavras.

   Por exemplo, há uma tendência de uma ou duas consoantes serem seguidas por uma vogal e assim por diante. Em tese não seria difícil para um atacante construir um programa que reproduza essas regras para construir um dicionário de palavras pronunciáveis.

3. Que tal misturar essa palavra com alguns caracteres? Podemos pensar em **flEtuci|0d4mente**.

   É comum a substituição de letras por seus «equivalentes» em números, isto é, por números cuja forma se assemelha às letras distorcidas.

   Assim, *E* pode ser trocada por *3*. Mas muito cuidado em basear sua segurança somente nesse tipo de troca, já que ataques minimamente sofisticados podem tentar a mesma coisa sem nenhuma dificuldade!

4. Que tal usar várias palavras, de preferência inventadas? Podemos pensar em **impelícia devora ecriterbeção***. Apesar de ser uma senha grande, ela não é tão difícil de memorizar, especialmente porque temos uma tendência de fazer associação de ideias mesmo com palavras sem significado.

   Também, em tese, não seria difícil fazer um programa que gere esse tipo de combinação.

   Você pode obter palavras buscando-as aleatoriamente num dicionário, tendo o cuidado de não repetir os padrões que temos ao abrirmos livros, mas ao invés disso usando, por exemplo, sequências de jogadas com dados para determinar o número de uma página, de uma linha, etc.

   Existe até um método chamado de **Diceware** que é baseado justamente em jogadas com dados e listas de palavras.

Existem muitas outras técnicas possíveis. Qual usar? A resposta é muito pessoal. Se você puder escolhar, escolha o maior número possível de técnicas ou tente usar algo mais aleatório possível que você consiga decorar.

8.3.2 Memorizando senhas

O limite da senha depende da capacidade e vontade de cada pessoa.

Se você tiver dificuldades com memorização mas quiser tentar uma senha mais complexa, você pode tentar primeiro decorar a senha e só quando se sentir seguro ou segura proceder com a alteração no respectivo sistema.

Tanto a criação quanto a memorização de senhas são processos que, para funcionar bem, dependem de autoconhecimento: qual é o nosso processo de criação de senhas? Quais são aquelas que conseguimos memorizar? Isso é algo bem pessoal.

Uma maneira válida para memorização, porém controversa, é a anotação de senhas. Controversa porque você pode perder ou se esquecer de apagar a anotação.

Contudo, pode ser razoável você manter a senha com você durante o processo de memorização. Mas isso depende muito da situação em que você se encontra. Se o fizer, lembre-se ao menos de queimar o papel assim que tiver decorado a senha!

8.3.3 Compartilhamento e gerenciamento de senhas

Tudo bem. Já temos uma ideia do que precisamos para melhorarmos a qualidade das nossas senhas. Mas teremos de fazer isso para todas as nossas senhas?

Vivemos num mundo de muitos sistemas, muitas contas, e por isso mesmo temos que ter muitas senhas. O que fazer se devemos evitar ao máximo reutilizar a mesma senha em diversos serviços?

Podemos pensar em duas abordagens:

1. Usar **círculos** ou **níveis de senhas**. A ideia aqui é reduzir a reutilização de senhas dependendo do nível que um serviço for crítico aplicando o princípio da compartimentalização.

   Serviços mais básicos, com os quais você não se preocuparia tanto com invasões, poderiam utilizar uma mesma senha. Talvez essa senha não precise ser tão complexa.

   Um nível intermediário seria composto apenas por sistemas nos quais a perda dos dados seria mais danosa e por isso teria uma senha mais complexa. Um nível avançado poderia ter uma senha mais difícil ainda.

Esse agrupamento também pode ser feito pelo nível de segurança que determinado sistema oferece. Existem muitos sistemas de baixa qualidade que podem ser invadidos a qualquer momento.

Note que, potencialmente, o comprometimento da senha de um nível ou compartimento pode comprometer a segurança de todos os serviços que se encontram no mesmo nível.

2. Para alguns serviços, você pode até escolher o salvamento da senha nos seus dispositivos de acesso, caso você os confie para isso.

   Se o seu dispositivo estiver com armazenamento criptografado e não se tratar de um serviço sensível, talvez essa não seja uma má ideia.

   Neste caso você não precisa de uma senha compartilhada. Neste caso você talvez possa até esquecer sua senha!

   Caso você precise resetá-la, por exemplo ao perder ou ganhar um dispositivo, você pode solicitar ao serviço uma senha nova por email, por exemplo. Mas cuidado para não esquecer a senha do email ou do canal de comunicação que você use para receber a nova senha. E mude essa nova senha assim que recebê-la!

3. Outra abordagem é utilizar um software de gerenciamento de senhas.

   Basicamente, ele cria um pequeno banco de dados com todas as suas senhas. Esse banco de dados é protegido criptograficamente com uma **senha mestre**. Você precisa lembrar dessa senha mestre para «destravar» esse banco de dados, mas em seguida pode acessar qualquer uma das senhas salvas e copiá-las para utilização em outros programas, como, por exemplo, num navegador web.

   Gerenciadores de senha também podem ser usados para criar senhas aleatórias para você, poupando seu esforço para criar senhas apenas para aquelas que você precisa decorar.

   É possível até que você nunca precise ver uma senha: seu gerenciador pode criá-la sem que você a veja e você pode copiá-la e colar noutro software do seu computador.

   Assim, você minimiza não só a quantidade de senhas que precisa decorar, mas também diminui o contato desnecessário com a sua senha.

   Existem vários gerenciadores de senha disponíveis.

   Dê preferência a gerenciadores de senhas que sejam instaláveis no seu computador para evitar a possibilidade da sua senha mestre ser capturada por alguma invasão ou má intenção de um serviço remoto de hospedagem de senhas.

   Também dê preferência para softwares livres, pos eles permitem a auditoria do código.

   Os gerenciadores são ótimos também no processo de memorização de senhas. Com eles você não tem motivos para anotar uma senha num papel, pois a qualquer momento pode consultar a senha usando o próprio gerenciador.

   A melhor abordagem, na nossa opinião, é usar o gerenciador de senhas.

   Assim, podemos minimizar o número de senhas sem perda significativa de segurança.

   Imagine então a seguinte situação onde uma pessoa possui um conjunto mínimo de senhas:

   1. Senha para ligar e usar um computador com armazenamento criptografado.
   2. Senha para destravar o gerenciador de senhas do computador.
   3. Senha para ligar e usar o telefone móvel com armazenamento criptografado.
   4. Senha do banco para pode realizar operações financeiras sem precisar consultar nenhum dispositivo.

   Essa pessoa precisa saber apenas 4 senhas! O inconveniente é que, para usar outras senhas, ela precisará ter acesso ao seu computador e ao seu gerenciador de senhas.

   Além disso, é recomendável que ela possua um backup do seu computador, incluindo a base de dados do gerenciador de senhas. Já que, no caso de perda do computador, ela pode recuperar suas senhas a partir de um backup criptografado.

Lembre-se que o arquivo de senhas deve estar disponível em algum lugar acessível. Se você deixá-lo apenas em volumes criptografados cujas senhas você não souber de cabeça irá criar um problema lógico que poderá impedir acessos futuros às suas senhas, já que para acessar o arquivo de senhas você precisaria acessar uma senha que está dentro do próprio arquivo de senhas. Portanto, certifique-se que você sempre consiga acessar um backup do seu arquivo de senhas só com senhas que você guarda na própria cabeça.

A quantidade total de senhas que uma pessoa precisa decorar vai depender muito do planejamento que uma pessoa fizer e do que for mais confortável para ela.

Algumas pessoas podem ter apenas uma ou duas senhas que permitam acessar o gerenciador de senhas.

Outras podem necessitar de mais senhas na cabeça para uso diário. Pode até acontecer que você comece a decorar senhas de tanto usá-las.

8.3.4 Digitando senhas

O momento da digitação de uma senha é especialmente vulnerável já que é a hora em que ela passa da sua cabeça para o computador, passando por um meio intermediário onde ela possivelmente possa «vazar». Alguns cuidados ajudam:

- Apenas digite sua senha quando o computador estiver esperando por ela; pode acontecer de você digitar seu usuário e logo de cara começar a entrar com a senha mesmo antes do computador pedi-la. Nesse meio tempo, pode acontecer da senha aparecer na tela, principalmente em computadores mais lentos.
- Experimente digitar qualquer coisa no lugar da senha para ver como o computador se comporta; existem ocasiões em que o computador preenche cada caractere digitado com um asterisco (*), outras a senha pode até aparecer normalmente (!); depois de se certificar de que está tudo bem com o pedido de senha, apague tudo o que você digitou anteriormente e entre com sua senha correta.
- Verifique se as teclas Num Lock e Caps Lock do teclado estão ligadas, desligando-as caso desejado.

8.3.5 Limite da confiabilidade de senhas

Por mais que uma senha seja longa e difícil, sempre é possível que alguém a descubra por tentativa e erro. Mas se você tomar os cuidados da seção anterior, vai demorar muito tempo até que alguém consiga quebrá-la.

É possível ainda que você passe por interrogatórios ou até mesmo por torturas. Nesse caso, dependerá apenas do seu estômago se você fornecerá ou não a senha para o torturador. O importante, nessa discussão, é você ter em mente que senhas nem sempre implicam na a inviolabilidade das suas informações e que você deve ter consciência do que pode acontecer caso seus dados sejam obtidos por terceiros. Torturas e interrogatórios são casos extremos, porém pode acontecer de terceiros descobrirem sua senha por outros meios, tanto pela tentativa e erro quanto por falhas de protocolo ou falhas de implementação.

8.4 Resumo

Boas senhas possuem as seguintes características:

1. São memorizáveis.
2. Difíceis de descobrir.
3. Pouco ou não compartilhadas.

8.5 Atividades

1. Expanda o seu Checklist de Segurança incluindo uma estratégia de senhas para você. Se preferir, pense num cenário de curto prazo e noutro de médio ou longo prazo para que você consiga melhorar a qualidades e seu esquema de senhas com calma.

8.6 Referências

- Abre-te Sésamo: as senhas da nossa vida digital | Oficina Antivigilância.

CAPÍTULO 9

Computadores

9.1 Funcionamento

O computador se transformou no elemento básico da comunicação digital.

Precisamos conhecer o funcionamento de um computador em linhas gerais para que possamos entender a maioria das vulnerabilidades dos sistemas digitais.

Computadores são sistemas bem complexos. Aqui usaremos um modelo bem simplificado mas que seja suficiente para mostrar como um computador pode ser invadido.

Na história da tecnologia, sabemos que para cada função que uma ferramenta ou instrumento deveria cumprir existem formas específicas de montagem, escolha de materiais, etc.

É o que acontece com máquinas. Por exemplo, um motor tem um arranjo e um conjunto específico de peças, é feito de determinados materiais, etc. Existem diversos tipos, ou linhagens de motores, mas todos possuem algumas características essenciais que os diferenciam, por exemplo, de um barco a remo.

O mesmo acontecia nos primórdios da eletrônica e da comunicação digital: era construído um aparelho específico para cada aplicação. Um tipo de equipamento cumpria a função de radiocomunicador, outro de sistema de alarme, um outro usado como sensor de temperatura e assim por diante.

O computador é diferente de todas essas máquinas específicas porque ele é uma máquina genérica: ele possui uma complexidade suficiente que permite que ele simule o comportamento de qualquer outra máquina simulável.

Isso não significa que qualquer computador pode ser usado como guindaste, mas que qualquer computador pode simular o comportamento de um guindaste.

Hã? Qual a diferença entre simular e realizar?

Imagine um sinal de trânsito composto pela cor verde, indicando a veículos e pedestres para que sigam adiante; amarelo, indicando atenção pois em breve a indicação irá mudar; e vermelho, indicando que veículos e pedestres aguardem até a cor verde para prosseguir.

Sabemos que um sinal de trânsito vai do verde para o amarelo e em seguida para o vermelho, voltando então para o verde. E sabemos que ele permanece em cada uma dessas situações por um intervalo de tempo. Dizemos que cada uma dessas situações são **estados** da máquina conhecida como **sinal de trânsito**.

Simular, no nosso caso, pode ser entendido como marcar mentalmente qual a cor atual do sinal, manter a contagem do tempo, e mudar a cor ou estado do sinal quando o tempo passar. Se além disso usarmos placas coloridas e formos para a rua exibi-las de acordo com o estado atual da nossa contagem mental, estaremos não apenas simulando como nos comportando como um sinal de trânsito.

Assim, para que um computador seja efetivamente um guindaste, basta que liguemos a ele o braço mecânico de um guindaste e a simulação passa a efetivamente controlar uma aplicação real.

O computador pode assumir o comportamento de outras máquinas. Inclusive, um computador pode simular seu próprio funcionamento, isto é, um computador pode simular um computador! Incrível, né?

É nesse sentido que dizemos que o computador é uma máquina genérica, também chamada de máquina abstrata. O computador processa informações e esse processamento pode ser ligado a mecanismos que realizem atividades de acordo com essas informações?

Mas como isso pode ser feito? O que o computador tem que o faz ser uma máquina genérica, diferentemente das máquinas específicas?

O segredo está no fato de que o computador é um dispositivo que aceita um conjunto grande de instruções de operação de natureza lógica, matemática. Essas operações são, por exemplo, de somar ou subtrair dois números ou mesmo de buscar por mais instruções.

As instruções são seguidas por uma parte do computador, chamada de processador, ou Unidade de Processamento Central (CPU).

As instruções ficam guardadas em dispositivos de armazenamento de longo prazo (também chamados de disco ou disco rígido) mesmo quando o computador estiver desligado.

Durante a operação do computador, essas instruções permanecem também numa memória de curto prazo, conhecida como Memória de Acesso Aleatório (RAM).

Para que o computador possa interagir com o mundo externo, e principalmente com humanos, ele é provido de elementos de entrada e saída de dados, como, por exemplo, teclado, mouse, tela de vídeo, caixas de som, interfaces de rede, etc.

E, para que essas partes possam ser interligadas, existem canais de comunicação conhecidos como barramentos de dados.

Assim, um computador pode ser pensado simplificadamente como um agregado dos seguintes elementos:

- Processador (CPU): executa instruções genéricas para manipulação e transferência de dados da e para a memória, para dispositivos de armazenamento ou para interfaces de entrada e saída.
- Memória de Curto Prazo (RAM): é uma memória usada para armazenar instruções e dados que serão manipulados pelo processador, enviados ou recebidos pelo armazenamento de longo prazo ou para as interfaces de entrada e saída.

  As informações guardadas na RAM desaparecem naturalmente e aos poucos depois que um computador é desligado.
- Armazenamento ou Memória de Longo Prazo (Disco): é o dispositivo que guarda as informações para acesso posterior. Essas informações não são apagadas naturalmente depois que um computador é desligado, estando disponíveis quando o computador é religado.
- Entrada e Saída (Vídeo, teclado, mouse, som, rede): são os dispositivos que nos colocam em contato com o computador e permitem a interação dele com o mundo à sua volta.
- Barramentos: conectam os elementos do computador uns aos outros. Tipicamente o barramento conecta o processador e a memória com os outros dispositivos.

  O armazenamento de longo prazo e os dispositivos de entrada e saída podem acessar informações que estejam na memória de curto prazo usando o processador como intermediário ou então acessar diretamente a memória, o que veremos que pode ser uma forma de ataque ao sistema.



Damos o nome de **hardware** a esses dispositivos físicos. Hardware significa ferramenta dura, uma referência à resistência natural que ferramentas físicas oferecem para serem modificadas, simplesmente porque são feitas de matéria.

Damos o nome de **software** aos conjuntos de instruções – ou código – que podem ser interpretadas pelo computador. Software significa ferramenta maleável, isto é, à facilidade de mudança da função do computador apenas com a mudança das instruções dadas a ele. Mudando o software, mudamos o funcionamento do computador.

Software e hardware. Instruções maleáveis que fazem com que um equipamento duro opere de inúmeras maneiras, cumprindo determinados **programas** de operação.

Mas como o computador opera?

A operação rotineira de um computador se dá do seguinte modo:

- Ao ser ligado, o computador busca num dos seus dispositivos de armazenamento de longo prazo chamado de BIOS algumas instruções básicas para que ele consiga reconhecer os outros dispositivos instalados, como a memória, as interfaces de entrada e saída e outros dispositivos de armazenamento de longo prazo.

  Essas instruções compõem um tipo de software conhecido como **firmware**, que são os programas feitos para que os dispositivos de hardware possam ser controlados. Ou seja, o software da BIOS é responsável pelo funcionamento básico do computador.

- Depois que o computador é ligado e executa, isto é, processa as instruções da BIOS, ele procura por outros softwares nos outros dispositivos de armazenamento de longo prazo.

- A maioria dos computadores que usamos não possuem um único software instalado no seu armazenamento de longo prazo, mas sim diversos softwares. No entanto, para que um computador possa executar vários softwares simultaneamente, é utilizado um software gerenciador conhecido como Sistema Operacional.

- Se o computador encontra um sistema operacional armazenado em disco, isto é, num armazenamento de longo prazo, ele começa o processamento desse sistema operacional e em seguida o computador estará disponível para executar outros softwares, chamados de **aplicações**.

9.1.1 Resumindo

O computador é uma máquina genérica que pode realizar qualquer tarefa que pode ser explicada numa **receita** chamada de **algoritmo**. Como ela é uma máquina genérica, ela pode fazer tudo quanto é coisa.

Em outras palavras, não existe a priori uma atividade intencional no computador, já que as pessoas que o projetaram não estavam pensando numa aplicação específica.

Toda a intenção de uso do computador depende do seu dono, porém é muito difícil fazer com que uma máquina genérica desempenhe apenas um conjunto mais restrito de operações que sejam consideradas seguras. Assim, é quase que um milagre que seja possível ter o mínimo de segurança com um computador!

Nosso modelo de computador é muito simplificado: além de cada elemento dele ser muito complexo, hoje em dia a maioria dos computadores é na verdade uma rede de computadores menores. Cada um deles rodando seu próprio software.

9.2 Ataques

Por que tratamos de tantos detalhes de funcionamento de um computador?

A resposta é direta: porque muitos ataques são baseados exatamente no funcionamento de todo ou de parte do computador.

Além do mais, o computador se encontra num dos níveis mais básicos de proteção da informação. Considerando que a segurança se dá em níveis e que o comprometimento de um nível compromete todos os níveis superiores, a perda da segurança no computador acarreta na perda da segurança em todas as aplicações que rodam nele.

A seguir detalharemos os tipos de ataque mais comuns a computadores.

9.2.1 Acesso físico

O primeiro tipo de ataque possível é o de acesso físico.

Quando alguém tem acesso físico direto, tempo e conhecimento pode usar o fato de estar em contato com o computador para instalar softwares ou hardwares espiões e também analisar os dados que estiverem armazenados.

O acesso físico não autorizado pode ou não ser detectado. A ausência de sinais não implica que um computador não tenha sofrido uma invasão de acesso físico.

Aqui estamos pensando no atacante como sendo um/a analista forense que obteve o seu computador ligado ou desligado e que quer obter as informações nele contidas ou instalar software e hardware malicioso e devolvê-lo a você para que essas informações possam ser extraídas posteriormente.

Vamos listar alguns destes ataques físicos:

1. Falta de criptografia nos dados que estão dentro do computador: a criptografia no armazenamento de longo prazo é uma medida que protege os dados no caso de uma captura ou invasão física do dispositivo.

   Ou seja, se o seu computador for roubado e o armazenamento estiver criptografado, seus dados podem estar a salvo! Isso só funcionará bem se o computador estiver desligado quando for roubado, como veremos mais à frente.

   Se você não utiliza criptografia no armazenamento. Bom, infelizmente os dados armazenados estarão disponíveis a qualquer pessoa que obter acesso físico ao seu computador, independente dele estar ligado ou desligado.

2. Keyloggers e data loggers:

   Dispositivos espiões básicos incluem os registradores de digitação, chamados de keyloggers, que gravam e eventualmente enviam os dados digitados para algum local remoto.

   Tais keyloggers podem inclusive registrar a senha usada para destravar o armazenamento criptografado do computador.

   Com acesso físico, também é possível a instalação de extratores gerais de dados e não apenas da digitação do teclado, mas também do conteúdo da memória RAM ou de qualquer outro ponto de medição do computador.

   Tanto a versão software quanto hardware dos loggers podem ser de difícil detecção. No caso dos modelos em hardware mais grosseiros, uma inspeção cuidadosa no hardware pode detectá-los.

3. DMA, ou Acesso Direto à Memória é um esquema que permite dispositivos do computador acessarem diretamente a memória de curto prazo, sem que o conteúdo da memória tenha que passar pelo processador.

   DMA é um método desenvolvido para acelerar grandes transferências de dados entre dispositivos e a memória, liberando o processador para realizar outras atividades.

A vulnerabilidade aqui é explícita: sem controles apropriados, dispositivos poderiam não apenas ler todo o conteúdo da memória, incluindo senhas usadas para criptografia de armazenamento, mas também para adulterar o conteúdo da memória.

Alguns dispositivos que utilizam a conexão Firewire tem capacidade de leitura direta da RAM e podem ser facilmente espetados num computador.

4. Canais laterais.

   Alguns ataques parecem mais esotéricos, porém já foram comprovados em experiências de laboratório e podem se tornar bem viáveis a médio prazo.

   Eles são chamados de **ataques de canal lateral** pois obtém informações fora das vias principais. Em geral é mais difícil de se defender contra eles pois precisam de intervenções mais pesadas no hardware.

   Não se assuste! Hoje os ataques a canais laterais ainda são muito raros e foram incluídos no curso mais para você ter consciência de que fenômenos físicos estão muito envolvidos na computação.

   Eles incluem:

   - Tempestade eletromagnética, ou simplesmente TEMPEST: equipamentos elétricos são como antenas: emitem radiações eletromagnéticas. Com a aparelhagem apropriada e uma boa antena, é possível medir essas emissões e delas extrair informações sensíveis.

     Em alguns casos, já se conseguiu até extrair chaves criptográficas!

     E isso pode ser feito a curtas distâncias, da ordem de metros. Atacantes podem se posicionar na sala ao lado e obter informações com bastante conforto e sem o constrangimento de serem pegos com a mão na massa!

   - Ruídos sonoros: de forma similar ao TEMPEST, equipamentos elétricos também emitem ruídos sonoros, muitos deles inaudíveis pelo ser humano porém captáveis com microfones especiais. Tais ruídos também podem extrair informações de do computador a curta distância.

     Ruidos de digitação do teclado também podem revelar informações sobre a digitação, baseados em pequenas diferencas de tempos levados na digitação sucessiva de teclas: teclas mais distantes demoram diferencialmente mais tempo para serem alcançadas pelos dedos. Tais diferenças poderiam ser utilizadas para reconstruir o que é digitado.

     Em alguns casos seria até possível diferenciar pequenas variações do ruído da própria tecla!

   - Interferência em cabeamento é outro tipo de vazamento indireto de informações do computador. Em tese pode ser detectado no cabeamento elétrico, de rede ou mesmo de som.

   - Microsismografia: o sensor de movimento de um telefone móvel pode ser posicionado na mesma mesa onde se encontra o teclado de um computador para detectar pequenas variações de deslocamento da mesa e com isso tentar determinar quais teclas estão sendo digitadas.

9.2.2 Falhas de hardware

Classificaremos aqui como ataques a hardware aqueles que são baseados em dispositivos físicos mas que não precisam necessariamente ser explorados presencialmente por um atacante. Ou seja, estes são ataques ao hardware que também podem ser feitos remotamente e via software.

Essas falhas podem ser usadas como **portas dos fundos**, também chamadas de **backdoors**, ou seja, portas de entrada alternativas ao computador que estão disponíveis a quem souber atacar.

Falaremos aqui um pouco sobre as principais falhas em determinados dispositivos:

- Processador: começaremos pelo pior caso, que são os problemas em processadores.

Algumas desses backdoors existem e são documentados, como é o caso dos gerenciadores remotos, que são subprocessadores contidos dentro dos próprios processadores usados para dar acesso remoto a inúmeras funções de hardware, como reiniciar a máquina, alterar configurações, etc.

Esse tipo de ferramente é conhecido como **out-of-band management**, que podemos chamar de gerenciamento remoto indireto e que pode ser acionado mesmo que o computador esteja desligado ou em estado de espera.

Às vezes também são chamados de **Lights-out Management (LOM)**.

Podemos entender esse tipo de hardware como uma espécie de interruptor ou controle remoto do computador.

Das tecnologias mais comuns, destacam-se:

  - O Intelligent Platform Management Interface (IPMI).
  - E mais recentemente o Intel Management Engine (ME).

O funcionamento desses dispositivos é obscuro e muitas vezes eles nem mesmo podem ser desligados!

- Wireless, ou wifi: a conexão de rede sem fio também tem seus problemas:
  - Monitoramento de dispositivos: os dispositivos de rede sem fio possuem identificadores únicos que são chamados de **endereços MAC**, ou endereços de controle de acesso de meio. Esses endereços são utilizados na comunicação entre os dispositivos de rede wireless.

    Qualquer dispositivo wireless pode observar e gravar todos os endereços MAC que estão ao seu alcance. Não é preciso modificar o dispositivo para realizar essa coleta. Qualquer computador com o mínimo de configurações pode fazê-lo.

    Isso inclui não só o endereço dos pontos de acesso à rede mas de todos os computadores e outros dispositivos com wireless habilitado.

    Com a coleta dos endereços MAC, é possível monitorar o deslocamento de dispositivos num mesmo local – por exemplo shopping center ou aeroporto – e até mesmo construir bancos de dados globais dessa informação.

    Podemos entender os endereços MAC como sendo um metadado que permite a identificação de um computador.

  - Problemas no firmware ou software, também chamado de **driver**, de operação.

    Isso é agravado pelo fato de que muitos softwares de operação são protegidos por segredos industriais e tem seu código fechado para análises.

  - Problemas na criptografia utilizada: é possível usar rede wireless sem criptografia alguma e nestes casos toda a comunicação é interceptável por qualquer computador que possua dispositivo wireless.

    Por esse motivo que é muito difundida o uso de criptografia em redes sem fio. No entanto, existem alguns padrões de criptografia muito fracos e com vulnerabilidades bem conhecidas como é o caso do WEP. Esse tipo de criptografia ruim pode ser quebrada com relativa facilidade.

- Rede com fios, também chamada de **ethernet**: analogamente ao caso da rede sem fio, a rede ethernet também é baseada em endereços MAC que podem ser coletados por qualquer outro computador conectado à mesma rede local.

  O software que controla a rede ethernet também pode conter várias falhas e, além disso, o ethernet é um dos canais principais utilizados para o **out-of-band management** que acabamos de mencionar.

- Bluetooth é um padrão de compartilhamento entre dispositivos que também pode estar sujeito tanto a ataques de leitura de endereço MAC quanto as outras vulnerabilidades existentes para redes sem fio.

- USB é um tipo de conexão para dispositivos que é muito prático mas que também pode ser uma grande fonte de problemas. Além de falhas de hardware e software, o padrão USB ainda tem uma funcionalidade que pode ser facilmente explorada: dispositivos USB podem ser «anunciar» ao sistema como sendo outros dispositivos.

Assim, um pendrive USB podem se anunciar como outro tipo de hardware, por exemplo, uma placa de rede, fazendo com que o sistema tente inicializá-la como tal, o que pode se transformar num vetor de ataque ao sistema.

Esse tipo de vulnerabilidade é conhecido como **BadUSB**.

Tome cuidado ao utilizar dispositivos USB de terceiros ou encontrados por aí. E mesmo os seus dispositivos USB podem ser infectados com firmware malicioso.

- Teclado e mouse sem fio também podem ser grampeados. Alguns fabricantes destes produtos informam que os dispositivos sem fio são protegidos por criptografia forte, porém é difícil avaliar essa segurança de fato porque em geral os softwares que eles rodam não estão facilmente disponíveis para auditoria.

  Por isso, de preferência não use esse tipo de produto.

- Microfones: computadores recentes, especialmente laptops, vem equipados com microfones que podem ser ligados arbitrariamente por softwares espiões para operá-los como escuta ambiental.

- Câmera: o mesmo acontece com as câmeras existentes nos computadores mais novos, que também podem ser ligadas à revelia do usuário.

9.2.3 Falhas de software

A exploração de falhas de software é muito mais comum, dentre outros fatores porque elas são mais simples de ser disseminadas.

O limite da exploração das falhas do sistema é o comprometimento não só dos dados do computador mas também a utilização da máquina para outros fins.

Existem vários vetores de ataques possíveis, mas o conceito de infecção básico é sempre o mesmo: alguma fonte de dados ou software que são processados pelo computador contém instruções que conseguem contornar o comportamento esperado, produzindo erros, defeitos ou até mesmo conseguindo executar instruções arbitrárias.

A possível existência de backdoors e falhas, ou bugs de software é análoga ao que acontece com o hardware: os softwares não estão livres de defeitos, sejam oriundos de falhas de design, de programação ou até intencionalmente colocados.

Essas falhas podem ser exploradas manualmente. Isto é, uma pessoa pode operar remotamente ou diretamente um computador para invadi-lo com a execução passo-a-passo de operações. Isso acontece mas não é tão comum.

O que é mais comum é a invasão automatizada, muitas vezes sem nenhuma intervenção humana. Procedimentos automatizados para a invasão desses sistemas são chamados de **exploits**, os exploradores de falhas.

Existem vários tipos de exploits e muitas formas de classificá-los. Aqui dividiremos em dois grupos:

1. Exploits remotos, quando o software de invasão roda remotamente a partir de um outro computador. Isso implica que existe alguma conexão de rede entre os dois computadores.

2. Exploits locais, que chamaremos de **malware**.

   Quando o vetor é um software que vai rodar no computador a ser infectado, ele é chamado de **malware**, ou software malicioso, que não precisa necessariamente ser executado pelo usuário. Muitos malwares aparentam ser arquivos comuns, e não programas, mas quando abertos disparam a execução de código arbitrário.

   Por exemplo, uma simples imagem ou um documento de texto podem conter instruções que aproveitam brechas nos softwares interpretadores desses arquivos para executar comandos arbitrários num sistema.

   A pessoa que abrir esses arquivos não perceberá o mal funcionamento, porque os arquivos aparentemente abrirão da forma correta: ela conseguirá ver a imagem e ler o documento, mas paralelamente o exploit estará rodando.

   Em laboratório até já se estudou a possibilidade de infecção através do microfone do computador!

A infecção por exploits podem ocorrer pela rede ou por qualquer outra forma de entrada de dados, como discos externos, CDs e pendrives USB.

O método de propagação do malware também pode ocorrer na forma de **vírus** – programas auto-reprodutíveis que infectam outros programas – ou **worms**, vermes – programas mal-intencionados que se reproduzem.

Alguns malwares se disfarçam como softwares inofensivos que desempenham alguma tarefa de fachada mas que, além disso, realizam alguma atividade escusa sem que o usuário perceba, como roubar dados do usuário, espioná-lo, etc. Estes malwares ganham o nome de **Cavalo de Tróia**.

Vejamos alguns tipos de **malware** de acordo com o que eles fazem com o seu computador:

1. Ransomware: nesse tipo de ataque os arquivos da vítima são criptografados com uma chave que só o atacante possui. Para liberar os arquivos, o atacante exige o pagamento de um resgate. É uma espécie de sequestro de arquivos.

2. Spyware: são softwares espiões, cujo objetivo é espionar o usuário, roubar arquivos, etc.

3. Robôs zumbis em botnets: muitos invasores não estão interessados em você ou nos dados do seu computador, mas sim em utilizar seus recursos computacionais para desempenhar tarefas.

   Estamos aqui falando de apropriação de recursos computacionais para todo o tipo de fim, incluindo enviar SPAM, invadir outras máquinas, propagar malware e assim por diante.

O caminho de uma invasão nem sempre é linear: kits de invasão podem consistir em malwares e exploits remotos que disparem várias condições especiais no computador, produzindo negação de serviço, execução arbitrária de código e até escalada de privilégios.

9.3 Defesas

Existem muitas formas de defender o seu computador. Algumas são mais eficazes do que outras. Algumas são mais fáceis do que outras.

Uma coisa que precisamos entender sobre o atual estado de coisas é que ele é conveniente para parte da indústria de software e para governos que desejam espionar as pessoas.

Parte da indústria que vende a solução dos problemas depende da indústria que vende os problemas. Sabemos que soluções para computação mais seguras existem e são viáveis, porém não interessam realmente à indústria. Quando não há uma monopolização do mercado para forçar a continuidade de produtos ruins, a própria competição degrada a segurança, pois a prioridade passa a ser o lançamento de inovações em alta velocidade, sem tempo para se preocupar com aspectos como a privacidade dos usuários.

Por isso, não podemos nem devemos esperar que as soluções de segurança sejam desenvolvidas por esses atores. Em alguns casos podemos esperar sentados. Noutros casos, as soluções que surgem são remendos que não atacam a raíz do problema, como é o caso dos anti-virus.

Ter um computador com alto nível de segurança, hoje em dia, não é tarefa fácil, mas também não é uma tarefa difícil ou extremamente difícil. Requer dedicação e às vezes um pouco de recursos.

Agora, ter um computador com um nível razoável de segurança e acima da média já está sim ao alcance de quem quiser.

Mostrarei algumas defesas, que vão do razoável, acima da média, até o alto nível. Assim você pode ir se preparando aos poucos, com calma e até chegar no nível que você achar suficiente.

9.3.1 De que computador estamos falando?

Mas antes de falar sobre essas defesas, vale a seguinte pergunta: de computador estamos falando:

1. Estamos falando de qualquer computador, isto é, o computador disponível no seu trabalho, escola ou numa lan house?

   Nestes casos estamos falando de um **Computador Público**, isto é, de computadores que estão fora do seu controle: você não sabe quem mais os utiliza, o que está instalado neles, se estão desprotegidos ou mal configurados, se existem mecanismos de espionagem instalados e assim por diante.

   Esta é uma situação bem duvidosa em termos de segurança. Evite esse tipo de computador para realizar qualquer atividade que tenha algum significado à sua privacidade. Se você não puder evitar você poderá ao menos utilizar algumas das defesas que mencionaremos adiante.

   Pode até ser que o computador público seja confiável em termos de segurança, a depender da competência de quem o administra e também da confiança de você tem de quem o opera, mas isso não está garantido a priori.

2. Estamos falando do seu computador pessoal, isto é, de um computador que é seu e está em seu controle.

   Se você protege esse seu computador com algum esquema de segurança e o utiliza para lidar com informações sensíveis à sua privacidade, diremos que este é o seu **Computador Pessoal Confiável**.

   Este então é um computador com o qual você estabelece uma relação de confiança, por mais que você não confie totalmente que ele esteja livre de invasões.

   Caso você não proteja esse seu computador de modo algum, então estamos tratando de um **Computador Pessoal** que é quase igual a um **Computador Público** em termos de segurança.

Por isso digo: o fator número zero na segurança do computador é saber **quem** controla o computador. É a partir disso que temos condições de intervir no seu funcionamento para melhorar suas defesas e evitar que ataques sejam perpetrados.

9.3.2 Acesso físico

As primeiras defesas estão no nível do acesso físicos:

1. Ter o seu próprio **Computador Pessoal Confiável** é um passo importante nesse sentido.

   Se você ainda não tem um computador pessoal e acha que esta seja uma medida importante para a sua privacidade, considere adquirir um. Você não precisa começar com o último modelo. Dê uma olhada nos usados. Se comprar um computador usado, tente pelo menos substituir seu disco por um novo, pois esse é um dos componentes que mais falham nos usados. Também dê uma olhada na expectativa de vida da bateria, no caso de um laptop.

   Depois, você pode prepará-lo para ter um bom nível de segurança e mantê-lo sempre em bom funcionamento, mas é importante também evitar que ele seja fisicamente capturado, o que traria fortes suspeitas de instalação de grampos.

   É uma boa política você não usar mais o seu computador depois que ele for capturado, não importa como e por quem. Se você descobriu que ele foi capturado, procure não utilizá-lo mais.

   Pode ser que você não tenha condições financeiras para simplesmente deixar de usá-lo. Neste caso, tente conseguir ajuda para alguém com conhecimentos fazer o **exorcismo** da máquina, isto é, tentar tirar na medida do possível qualquer indício de invasão, reinstalar o sistema, etc.

   Ou, se você não conseguir esse tipo de assistência, tente vendê-lo para alguém ciente do problema e com condições de reutilizá-lo sem sofrer danos. Assim você consegue pelo menos recuperar o dinheiro para comprar um hardware novo.

   Problema maior ainda é saber **se** o seu computador pessoal foi capturado ou não. A não ser que você faça vigílias constantes e mantenha seu computador sempre junto a si, você nunca vai saber. De fato, algumas pessoas que são alvos de vigilância pesada acabam por adotar a prática de sempre andarem junto do seu computador.

Mas essa é uma prática para casos extremos. Num nível de segurança acima da média, você pode simplesmente evitar de deixar seu computador dando sopa em qualquer lugar. Deixe-o apenas em lugares que você tiver uma confiança mínima a respeito da segurança. Não estamos falando apenas de roubo, mas também da implantação de hardware e software malicioso usando acesso físico à máquina.

2 - Usar defesas básicas, que são muito simples de serem adotadas:

- Se for um laptop, usar um cadeado do tipo Kensington para evitar roubos ligeiros.
- Deixar a tela travada se tiver de deixar o computador ligado e desatendido, o que evita os atacantes curiosos e menos refinados.
- Aqui vale a regra do **Protect Your Belongings**, ou Proteja os seus pertences. Também tente não ostentar demais o equipamento e manter uma linha mais low profile.

3 - Criptografia de armazenamento: protege os arquivos armazenados no computador, mas não protege todos os softwares.

Os softwares básicos de inicialização (BIOS e carregador do sistema operacional) continuam expostos à adulteração por atacantes físicos e remotos. Um atacante pode colocar um leitor de senhas no seu computador e capturá-las no momento que você as digita ao iniciar seus discos criptografados, num ataque conhecido como **Evil Maid**, em referência aos serviços de quarto em hotéis que podem ser compostos por espiões disfarçados.

Apesar disso, a criptografia de disco oferece boa proteção caso o seu computador seja capturado e esteja desligado.

Note que isso implica que você pode criptografar não só os seus arquivos mas também o próprio sistema operacional, o que chamamos de **Full Disk Encryption (FDE)**, mas mesmo assim você ainda estará à mercê de ataques mais sofisticados como o Evil Maid.

Se o seu computador for capturado enquanto estiver ligado, então um atacante poderá tentar ler as chaves de criptografia de disco diretamente da memória RAM, em ataques de **análise forense de memória**.

Vou dizer mais uma vez. A criptografia de disco não oferecerá grandes proteções se o sistema for roubado ou invadido enquanto ele estiver ligado, pois nessa condição as informações estarão disponíveis para acesso.

O mesmo acontece se o computador for capturado enquanto estiver no estado semi-desligado de baixa atividade conhecido como **suspensão**. Nesse estado, muitas partes do computador estão desligados mas a memória de curto prazo (RAM) estará ativa e armazenando a chave criptográfica do seu dispositivo criptografado.

Em algumas situações é possível resgatar as senhas criptográficas momentos depois que o computador é desligado, a depender do tipo de memória RAM que o computador utiliza, num ataque conhecido como **Cold Boot**.

- Ande com o computador sempre desligado, pois isso evita que um adversário habilidoso consiga extrair senhas que estejam na memória operacional (RAM) do computador.
- Desligue o computador quando não for usá-lo. Alguns sistemas possuem a funcionalidade de **hibernação**, que, ao contrário da **suspensão**, armazena o estado da memória RAM no disco criptografado e posteriormente desligando efetivamente a máquina.

  Na dúvia se seu sistema utiliza hibernação ou suspensão, recomendo que você simplesmente desligue seu computador quando não for utilizá-lo.

4. Defesas contra canais laterais: estas são mais difíceis, porém são contra ataques não muito difundidos hoje em dia até onde se sabe. Aqui coloco apenas ilustrativamente.

   Você tanto pode comprar computadores que possuem blindagem a diferentes tipos de emanações, que são difíceis de encontrar, ou tentar utilizá-los sempre fora da tomada ou dentro de instalações que você julga serem seguras.

Estas são algumas das defesas físicas possíveis para computadores.

9.3.3 Hardware

Agora falaremos das defesas contra ataques ao seu hardware que independem de acesso físico à máquina!

A recomendação básica é: se você não estiver usando um dispositivo de entrada ou saída, deixe-o desligado ou desativado.

1. Uma das defesas mais básicas consiste em cobrir a câmera com um adesivo, para que, mesmo que um software espião ligue a sua câmera, ele não consiga capturar alguma imagem.

2. Com relação ao Bluetooth, mantenha-o ligado apenas durante o uso ou, se não for utilizá-lo, desabilite-o completamente.

3. Para as redes sem fios, procure utilizar apenas pontos de acesso que usem criptografia do tipo WPA2+AES e uma senha de tamanho razoável.

   Se você for configurar um ponto de acesso wireless, use também o padrão WPA2+AES.

   Mesmo assim, não conte com essa criptografia para a proteção dos seus dados e procure usar serviços que também utilizem criptografia, de modo que você esteja utilizando diversas camadas de criptografia ao mesmo tempo.

   Considere que a criptografia do ponto de acesso oferece proteção baixa e só opera entre o seu computador e o ponto de acesso, deixando de fazer efeito conforme as mensagens trafegam no resto da rede.

4. Backdoors de hardware: em alguns casos é possível corrigir a falha através da atualização do firmware, do software que o utiliza ou pela substituição do dispositivo. Em outros casos tudo o que podemos fazer é desabilitar o aparelho ou conviver com a falha.

   - Se o seu computador possui conextão firewire, desabilite-a. Habilite apenas durante o uso.
   - Se possível, desabilite a manunteção remota, o que é feito pela BIOS. Alguns processadores mais novos não permitem que isso seja desabilitado. Então você pode escolher conviver com essa possibilidade de invasão ou então tentar comprar um computador cujo processador não possui essa funcionalidade ou que ao mesmo permita o seu desligamento.

   Outra defesa contra backdoors é a utilização de hardware livre, mas essa é uma alternativa ainda pouco acessível.

5. Nível hardenado: só para ilustrar, vou falar de algumas coisas que você pode fazer se quiser ter um computador de nível **hardenado**, isto é, muito acima da média. Mas atenção: isso acarreta em mudanças que podem quebrar seu computador se você não souber fazer corretamente. Isto é por sua conta e risco e não nos responsabilizaremos por quaisquer danos:

   - Subsituição da BIOS, isto é, do firmware principal. Existem projetos como o Libreboot que implementação versões em software livre da BIOS do computador. Só funciona para alguns modelos específicos de computadores.
   - Ativação de senha da BIOS para inicialização do computador ou para mudar configurações básicas. Essa não é uma super medida de segurança mas pelo menos pode atrasar o tempo de trabalho de um atacante.
   - Desligamento físico de alguns dispositivos, como microfones e adaptadores bluetooth. Estando fisicamente desligados pelo corte de fios e pinos, eles não tem como ser ativados.
   - Troca de dispositivos proprietários por versões mais abertas: é a substituição de componentes do computador como placas de rede e vídeo por alternativas que sejam mais compatíveis com software livre e que também tenham um histórico de funcionamento, segurança e estabilidade maiores.
   - Randomização de endereço MAC: é possível configurar o seu computador para que ele sempre utilize um endereço MAC aleatório tanto para conexões com fio padrão ethernet quanto para wireless.

     Isso evita o rastreamento de dispositivos via coleta de endereço MAC, mas não evita outros tipos de identificação.

- Defesas contra ataques na USB, isto é, mitigação ao BadUSB, são em geral bem desconfortáveis. Elas vão desde a desabilitação das portas USB, passando pela habilitação durante o seu uso, o que evita um atacante plugue um dispositivo USB malicioso mas não evita que você faça isso deliberadamente quando usa um dispositivo infectado sem saber.

  Outra alternativa é o uso das chamadas «camisinhas USB», consistindo em usar um outro computador para fazer a conexão USB com o dispositivo, compartilhando-o com o seu computador através de algum outro meio. Esse tipo de defesa é poquíssimo usada.

  Outra mitigação possível é o bloquear todos os dispositivos USB exceto aqueles que apresentarem os identificadores correspondentes aos dispositivos que você conhece. Novamente, isso pode eliminar algumas tentativas de ataque mas não impedem que um dispositivo malicioso utilize um dos IDs autorizados.

- Air gap, ou isolamento físico do computador, é a prática de deixar o computador o mais isolado possivel do mundo externo. Isso implica em cortar qualquer possibilidade de conexão de rede e usar apenas meios considerados seguros para transmissão de arquivos.

  O conceito de Air gap é controverso, porque os computadores foram feitos para operar em rede.

  Manter um computador desse tipo atualizado é uma tarefa complicada e nada garante que algum arquivo transferido para ele não contenha algum código malicioso que possa ser usado para a extração de dados.

9.3.4 Software

Por fim, falaremos agora das defesas que podem ser adotadas no nível de software.

1. Use **Software Livre**, que é o oposto do chamado **Software Proprietário**. Todo software livre é baseado em pelo menos quatro liberdades fundamentais:

   0. Rodar o software no seu computador.

   1. Estudar o software, isto é, analisar o seu código. Muitos softwares são escritos em linguagens mais inteligíveis para seres humanos do que o código que é interpretado pelo processador do computador.

      Para que possam rodar no computador, o código do software escrito por alguém, chamado de **código fonte**, precisa ser traduzido para a linguagem da máquina, procedimento conhecido como **compilação**.

      A liberdade de estudar o software implica na capacidade de qualquer pessoa de acessar o código fonte do software, e não apenas a versão compilada, também chamada de **binária**, do software, como é o caso dos softwares proprietários.

   2. Redistribuir o software sem restrições. Isso implica que você pode vender o software livre e prestar serviços com ele mesmo que você não tenha escrito o software! Por outro lado, você não pode impedir alguém de fazer o mesmo.

      Sempre tem alguém distribuindo software livre sem cobrar financeiramente por isso, então ele também é gratuito nesse sentido.

   3. Melhorar o software, isto é, alterar o seu código corrigindo falhas ou implementando novas funcionalidades.

   Todas essas quatro liberdades são essenciais para a segurança da informação:

   0. Rodar o software implica que você pode utilizá-lo no seu próprio computador, ao invés de ter que depender necessariamente do software rodando num computador que você controla e que portanto você não sabe se está em controle de atores mal intencionados.

   1. Estudar o software significa que qualquer pessoa pode estudá-lo em buscas de mal funcionamento e problemas de segurança.

   2. Redistribuir implica em colaborar para a difusão do software, o que pode atrair mais pessoas, por exemplo, para estudar o seu funcionamento e encontrar possíveis falhas.

3. Melhorar o software implica que qualquer pessoa com capacidade técnica pode corrigir algum problema de segurança que foi encontrado.

Ter essas quatro propriedades não implica necessariamente que essas quatro propriedades estão sendo **exercidas** automaticamente. O software é apenas uma porção de código, enquanto que a sua evolução depende da atividade de pessoas.

Não é todo mundo que tem os meios de rodá-lo (é preciso ter um computador), de estudá-lo (é preciso de tempo e conhecimento), redistribuí-lo (o que hoje em dia depende mais de vontade) e de melhorá-lo (novamente, tempo e conhecimento).

Por isso, com o software livre é muito mais fácil fazer uma auditoria de segurança pois para isso não é preciso pedir permissão a ninguém, mas isso não quer dizer que automaticamente todo o software livre é auditado.

Essa transparência também é refletida nos anúncios de atualização dos softwares livres, que muitas vezes indicam quais vulnerabilidades estão sendo corrigidas.

Assim, rodar software livre pode ser considerado um pré-requisito para a segurança da informação. É uma condição necessária, porém não suficiente para a segurança.

Benefícios:

- Usuário comum não tem superprivilégios por padrão nestes sistemas.
- Arquivos anexados não são executados por padrão.
- Canais – ou lojas – de instalação de software fazem parte do próprio sistema, minimizando a instalação de programas distribuídos por terceiros.
- Não te espionam por padrão como outros sistemas operacionais proprietários.

Problemas:

- Arquitetura não é 100% segura. O foco do desenvolvimento tem sido performance e suporte e não segurança. Mas ainda assim são muito melhores do que os sistemas operacionais proprietários.

2. Use Sistemas Operacionais Livres!

   Você pode rodar não só programas livres mas todo o software de operação do seu computador pode ser livre.

   Eu recomendo você utilizar o Debian, que é um sistema operacional desenvolvido de forma comunitária e com uma política de segurança razoável.

   Se você não conseguir usar o Debian, uma alternativa é o Ubuntu, que é mantido por uma empresa e é baseado no Debian.

   Sistemas como o Debian já vem com perfis de segurança razoáveis e podem ser instalados de forma criptografada no armazenamento do seu computador.

3. Use virtualização!

   Computadores são máquinas que podem simular máquinas. Podem até simular a si mesmos. Uma máquina virtual é um programa de computador que simula um computador.

   No contexto da segurança, máquinas virtuais são criadas para criar um cordão de isolamento para que vulnerabilidades de um programa rodando dentro de uma máquina virtual não consigam escapar para o resto do computador.

   Na prática, é possível rodar um sistema operacional inteiro juntamente com aplicativos dentro de uma máquina virtual. Se você tem um computador razoável, pode tranquilamente rodar uma máquina virtual com navegador web, editor de textos e até ser capaz de assistir um filme!

   Este isolamento é muito bom mas não é isento de problemas. Falhas no software virtualizador podem ser utilizadas para que programas maliciosos consigam escapar da máquina virtual e infectar outras partes do seu sistema.

Contudo, máquinas virtuais ainda oferecem um bom nível de proteção, em muitos casos permitindo até que você rode um sistema operacional ou softwares proprietários em ambiente virtualizado.

Lembre-se que a virtualização protege o resto do sistema contra vulnerabilidades nas aplicações virtualizadas, e não o contrário!

3. Tenha mais de um dispositivo e compartimente o uso.

   Pode ser que por algum infortúnio você precise usar software proprietário. Ou que tenha que usar serviços de segurança duvidosa e assim por diante.

   Nesses casos, você pode utilizar mais de um dispositivo com perfis de uso distintos.

   Por exemplo, um dispositivo mais «sério», mais protegido e com dados sensíveis. E um outro dispositivo para qualquer outra coisa. Esse segundo dispositivo pode ser um tablet ou um computador velho.

   Pode ser um dispositivo apenas com software livre e outro em que seja permitido o uso de software proprietário.

   Esta pode ser uma boa alternativa caso você não confie na proteção oferecida pelas máquins virtuais.

4. Tenha mais de um sistema operacional no seu computador, compartimentalizando o uso de softwares mais e menos confiáveis assim como informações mais ou menos sigilosas, o que mitiga um pouco o problema de rodar softwares não tão confiáveis, mas não é tão eficaz pois a invasão de um sistema pode levar à invasão de outro.

   Adote essa alternativa apenas em casos que você precise de dois perfis de uso e as opções anteriores não possam ser adotadas.

5. Use sistemas operacionais super-seguros.

   Três sistemas operacionais livres e orientados à segurança são o Tails, o Subgraph e o Qubes.

   Todos os três podem ser rodados no modo **live**, isto é, não precisam ser instalados no armazenamento do seu computador e podem ser mantidos num pendrive USB. Se você usar um pendrive pequeno, ele pode até ficar dentro da sua carteira para você tê-lo à mão sempre que precisar e esta pode ser uma boa alternativa se você tem apenas um único computador e quer ter dois perfis de segurança distintos.

   O Tails é um sistema operacional baseado em Debian que é feito para oferecer segurança e anonimato e sobretudo não deixar rastros de que foi rodado.

   Ele possui uma série de melhorias de segurança e todo o tráfego de rede que ele gera segue através da rede de roteamento Tor, sobre a qual veremos adiante no curso.

   O Tails pode até ser utilizado em computadores de terceiros desde que você consiga reiniciá-los, oferecendo um nível razoável de segurança, a não ser que o hardware do computador já esteja bem comprometido.

   O Subgraph, até o momento que este curso foi feito, ainda não foi lançado oficialmente, mas promete ser uma versão melhorada do Tails. Além do tráfego roteado pelo Tor e diversas melhorias de segurança, o Subgraph ainda roda diversos programas dentro de ambientes virtualizados, garantindo o isolamento de aplicações como navegadores web e leitores de documentos.

   O Qubes é um sistema parecido com o Subgraph nesse sentido, com a diferença que não roteia todo o tráfego pelo Tor por padrão mas pode ser instalado no seu computador além de rodar no modo live e também possui uma maturidade maior pela sua idade.

   Outro sistema que você pode tentar é o OpenBSD, um dos mais seguros em existência. Demora um tempo para aprender a usar, mas ele é muito bem feito!

   Se quiser seguir o caminho do aprendizado, você pode pegar um sistema como o Debian e ir aplicando mudanças de segurança como por exemplo o PaX e o grsecurity, ou pelo menos tentar o AppArmor, que forçam políticas restritivas de execução de aplicações, dentre outras melhorias de segurança.

6. Rode a menor quantidade de software possível. Esta é a aplicação pura do princípio da simplicidade, ou complexidade necessária: quanto menos código você roda, menor é a probabilidade de falhas.

Considerando que um computador típico roda uma quantidade de instruções correspondentes a milhões de linhas de código, a quantidade de vulnerabilidades de segurança é igualmente enorme.

Esta pode ser uma opção controversa, mas ela tem suas razões considerando a quantidade enorme de falhas em software que são reveladas toda a semana.

Se você puder e quiser seguir esta linha, procure também os softwares cujo código seja menor, sejam mais bem escritos, tenham poucas funcionalidades mas boa qualidade de funcionamento, tenham uma boa base de usuários e sobretudo um histórico de falhas baixo.

7. Mantenha seus softwares sempre atualizados!

   Toda semana existem várias atualizações de segurança para tudo quanto é tipo de software. Isso significa que, pelo menos a partir do momento desses lançamentos, as vulnerabilidades existentes nesses softwares passam a ser públicas.

   Isso implica que, caso você deixe de fazer uma atualização de segurança, você estará deixando softwares no seu computador que possuem falhas de segurança conhecidas.

   Por isso, mantenha sempre que possível todo o seu software atualizado.

   Isso não vai oferecer uma proteção total, mas já é um começo. Podem ser que existam vulnerabilidades nos softwares que você usa mas que não sejam conhecidas.

   Esse tipo de vulnerabilidade é chamada de **zero-day**, ou vulnerabilidade de zero-dias, indicando que ela ainda não é pública e por isso tem zero dias de vida pública.

   É até possível que alguém conheça essas vulnerabilidades mas não as divulga para justamente poder tirar vantagem da ignorância sobre elas.

   Ou seja, manter seu software atualizado não te protege contra falhas de zero dias, mas protege das falhas conhecidas que já foram corrigidas.

8. Não instale qualquer software.

   Esta é uma dica básica. Cuidado com o software que você for instalar no seu computador. Não execute qualquer programa que enviarem pra você.

   Se você está usando um sistema operacional livre como o Debian, use a própria central de instalação de programas que ele oferece para encontrar softwares que satisfaçam sua necessidade.

   Os programas são distribuídos nessa central num formato chamado de **pacote**, que são versões dos programas bem compatíveis com o sistema operacional, fazendo a instalação, remoção ou atualização de modo facilitado.

   Mesmo usando essa central de programas, tome cuidado: não é porque está listado na central que é um software seguro.

   Se você tiver na dúvida sobre algum software mas precisa rodá-lo, use a abordagem do isolamento com máquinas virtuais ou num computador secundário.

9. Não instale softwares de fontes desconhecidas.

   Você pode confiar num determinado software, mas cuidado ao baixá-lo: você está baixando do local oficial de distribuição? Esse download é feito com conexão criptografada? Você possui algum meio de verificar se você baixou o software legítimo e não uma versão contendo código malicioso?

   Existem algumas formas de fazer a checagem de integridade do software que você baixou.

   Sistemas livres como o Debian já fazem isso quando você instala um pacote, fazendo uma checagem criptográfica dos arquivos baixados.

   Mas você ainda precisa fazer isso ao menos uma única vez... quando for baixar o Debian em si.

   Para fazer essa checagem no Debian ou em qualquer outro software, consulte a documentação correspondente.

10. Anti-virus e detectores de intrusão.

    Um anti-virus pode te ajudar a eliminar alguns softwares maliciosos do seu computador, mas essa é uma media bem paliativa.

    Anti-virus são softwares que varrem o seu computador em busca de arquivos e regiões da memória infectados por softwares maliciosos já bem conhecidos.

    Eles tem várias limitações: não detectam softwares maliciosos ainda pouco conhecidos.

    Sistemas operacionais como o Debian, que são baseados no ecosistema conhecido como GNU/Linux são feitos numa arquitetura que torna mais difícil a contaminação por malware.

    Mesmo assim existem softwares similares aos anti-virus mas que também detectam outros tipos de invasão. Estes são conhecidos como **detectores de intrusão**.

11. Firewall.

    Outra media importante é a utilização de um **firewall**, que é uma barreira erguida nas conexões de rede do seu computador para filtrar, recusar ou descartar conexões indesejadas. Assim, você pode limitar o contato do seu computador na rede.

Estas são as principais defesas que você pode aplicar nos seus computadores. Existem muitas outras!

9.4 Resumo

1. O computador é uma máquina de processamento geral. Isso implica que ela pode ser utilizada por terceiros para obter suas informações.
2. Existem muitas falhas nos computadores em em todos os níveis: no hardware, no sistema operacional e nos programas utilizados, assim como muitas formas de defender.

   O básico inclui o uso de software livre, criptografia de armazenamento e manter o sistema sempre atualizado. Outras alternativas simples são ter mais de um computador por perfil de uso ou o uso de sistemas operativos mais seguros e que rodam sem instalação, como o Tails e o Subgraph.

9.5 Atividades

1. Agora você pode completar o seu Checklist de Segurança para incluir uma política de defesa em relação ao uso de computadores.

   Assim, proceda criando um item na lista para tratar com os seus computadores e com computadores de terceiros.

   Você terá um computador sob seu controle? Outras pessoas terão acesso a ele?

   Você usará computadores que você não controla? Para que tipo de atividades?

   Você terá um segundo dispositivo para usar com atividades não muito sensíveis?

   Qual serão as defesas que você adotará em cada um desses casos?

1. Instale o Tails num pendrive USB e teste-o em diversos computadores.
2. Faça o mesmo com o Subgraph.
3. Teste o Qubes.
4. Gostou do GNU/Linux? Instale no seu computador usando armazenamento criptografado. Mas **ATENÇÃO**: faça backups de todos os seus dados num outro lugar antes de proceder com a instalação, pois ela passará por cima dos arquivos armazenados.

CAPÍTULO 10

Telefones celulares

10.1 Funcionamento

Como um celular funciona?

O celular é basicamente um rádio comunicador que permite a comunicação entre duas partes que estejam distantes uma da outra. Cada uma das partes possui um número único para que possa ser contatada. Isso provavelmente você já sabe.

O que talvez você não saiba é que, como um telefone móvel é um aparelho pequeno, ele não tem potência suficiente para que suas ondas de rádio cheguem até destinos que estejam muito distantes.

Para contornar esse problema foi desenvolvido o sistema de telefonia celular, onde diversas antenas – ou células, também chamadas de Estações Rádio Base (ERBs) – são instaladas num território e fazem a comunicação entre os aparelhos de telefone móveis e o resto do sistema telefônico.

```
aparelho celular <-> estação rádio base <-> sistema telefônico <-> estação rádio base
↪<-> aparelho celular
```

O interessante dessa tecnologia é que os aparelhos de celular podem se mover de um lugar para o outro sem que haja interrupção na comunicação: conforme um aparelho se afasta de uma estação rádio base e se aproxima de outro, ele passa por um processo de troca de estação, se registrando na ERB nova e em seguida se desregistrando da velha.

A comunicação em rede de celular pode consistir no tráfego de conversas telefônicas, mensagens de texto simples ou dados genéricos.

Mas um aparelho de celular não faz apenas isso!

Agora que sabemos o básico da comunicação em rede celular móvel, vamos adicionar o elemento que estava faltando no celular moderno, também conhecido por smartphone: o computador.

```
smartphone: celular clássico + computador
```

É lógico que mesmo os telefones celulares clássicos possuem um computador responsável pela comunicação e funcionamento do aparelho, porém nós ressaltamos que o smartphone é um celular clássico e mais um computador porque

este é um computador muito poderoso e ainda porque o processamento dos aparelhos modernos são feitos por dois elementos:

- Processador de banda base, ou baseband, que é o responsável pela comunicação usando os protocolos da rede de celular.
- Processador genérico usado para a interação com o usuário(a), como processamento de aplicativos, tela, fone e botões.

Os celulares modernos ainda possuem uma série de outros dispositivos:

- Adaptador para conexão de redes sem fio – wireless/wifi.
- Sensores de posicionamento global (GPS e GLONASS).
- Sensores de movimento.
- Interfaces de comunicação de curta distância (Bluetooth/NFC).

Essa quantidade de dispositivos pode ser controlada não só pelos aplicativos que rodam no celular como também por agente remotos.

10.2 Ataques

No capítulo anterior vimos como o celular funciona. Ele tem tantas formas de ser atacado que ele é uma verdadeira catástrofe em termos de segurança e privacidade!

Façamos uma rápida passagem pela lista de ataques a estes dispositivos:

1. Ataques ao computador: como um smartphone também é um computador, você pode pensar em todos os ataques possíveis que abordamos na aula passada, exceto aqueles que não se aplicam por depender de interfaces que o smartphone não possui.

   Ataques de acesso físico podem ser realizados com o auxílio de alguns equipamentos especializados em extração de dados de telefones móveis!

   Um software espião – por exemplo um aplicativo mal intencionado – pode gravar o que você fala, o que você digita, tirar fotos, registrar sua posição, ler arquivos e conteúdo de conversas, etc.

   Esses ataques podem ocorrer tanto nos componentes tradicionais do computador – processador, memória de curto e longo prazo, etc, quanto no processador de banda base responsável pelas comunicações de rádio com a rede de telefonia.

2. Interceptação de dados: como qualquer meio de comunicação digital, o sistema de telefonia móvel está sujeito ao grampo.

   As companhias telefônicas podem realizar o grampo, uma vez que elas são donas da maior parte da infraestrutura por onde trafega a comunicação; mas ela também pode ser feita por qualquer ator que possua um equipamento específico, seja invadindo o local de uma Estação Rádio Base para implantar um grampo – o que é mais arriscado pois é mais fácil ser percebido – ou usando os aparelhos conhecidos como **maletas**, que nada mais são do que dispositivos para interceptação ativa ou passiva.

   Tanto conversas telefônicas, mensagens de texto ou dados genéricos podem ser interceptados dessas maneiras.

   Alguns padrões de comunicação celular possuem criptografia, como o GSM, mas que é tão fraca e fácil de quebrar que nós nem consideramos que essa comunicação está protegida. Comunicações como SMS podem basicamente serem lidas por qualquer agente que consiga interceptá-las.

3. Interceptação de metadados: por questões de cobrança, as companhias telefônicas já registram, por padrão, informações de ligações como origem, número de destino, data, hora e duração da chamada.

No caso dos telefones celulares uma informação adicional também pode ser registrada por padrão: a localização aproximada do telefone através da informação sobre qual torre o telefone esteve conectado.

Ainda é possível obter a localização do aparelho em tempo real e com grande precisão.

Os telefones móveis são dispositivos rastreadores **por design**: eles podem estar em contato com várias estações rádio base ao mesmo tempo, cada uma delas registrando esse contato. Sabendo a potência do sinal do aparelho em cada estação, é possível facilmente determinar a posição do aparelho com precisão.

Por isso, dizemos que **o celular é um aparelho rastreador que possui a funcionalidade de realizar chamadas telefônicas**.

10.3 Defesas

Gente, tenho más notícias quanto aos smartphones. É muito difícil tê-los e possuir segurança e privacidade em níveis relativamente altos.

Hoje, o telefone móvel é o calcanhar de Aquiles da segurança da informação. Não porque ele seja a única grande vulnerabilidade existente, mas porque é aquela que não tem uma mitigação que permita usar esse tipo de aparelho sem perda significativa de privacidade.

A solução simples consiste em não utilizar telefones celulares. Porém, hoje, está cada vez mais difícil viver sem eles. Em poucos anos a sociedade se tornou extremamente dependente deste aparelho de tal modo que é muito difícil viver sem ele. Assim, as medidas aqui sugeridas são bem paliativas.

Muitas das defesas descritas na aula sobre computadores podem ser adaptadas para o contexto dos telefones móveis pois seguem a mesma lógica, como é o caso de ter dois dispositivos: um deles rodando poucos aplicativos e outro rodando qualquer coisa.

10.3.1 Medidas básicas

Vejamos algumas medidas bem básicas para proteger seu smartphone.

- Travar a tela com senha: é melhor do que usar um padrão gráfico de travamento, pois as possibilidades são maiores. Na pior das hipóteses você estará dando um trabalho adicional para o atacante, o que pode te dar tempo para tomar outras medidas como apagar remotamente o conteúdo do telefone ou desabilitá-lo.
- Criptografar o armazenamento interno e usar memória externa só para aplicações não-sensíveis.

  Sistemas como o Android suportam criptografia no armazenamento interno, mas nem todo telefone suporta criptografia no cartão SD externo, então a recomendação aqui é para usar apenas a memória interna do telefone.

  Como medida adicional, em situações de risco em que você consiga se antecipar de um perigo de perda do telefone, tente desligá-lo antes pois isso tornará a criptografia do armazenamento interno ainda mais efetiva contra ataques pós-furto.
- Usar senha no SIM card: para complicar um pouco mais a vida de ladrões comuns, você ainda pode ativas os códigos PIN e PUK do seu SIM Card.
- Software anti-furto para desabilitar o seu telefone é uma possibilidade viável se você teme o roubo do celular como forma de tomarem controle dos seus dados.

  Com esses softwares, você pode configurar para que o apagamento de dados ou a inutilização do aparelho sejam acionados remotamente por você em caso de perda do dispositivo.

  Alguns desses softwares também rastreiam o seu dispositivo caso você pense em recuperá-lo de algum modo.

  Mas cuidado! Esses softwares também podem acabar monitorando sua vida diária! Informe-se antes de usá-los.

10.3.2 Medidas anti-grampo ambiental

Se você for conversar pessoalmente com alguém e quiser evitar qualquer tipo de grampo que pode estar instalado no seu telefone, pense nas seguintes possibilidades:

1. Desligar o celular quando for conversar com alguém: esta é uma medida bem simples, porém pode não ser totalmente eficaz: um software malicioso poderia simular o desligamento do telefone e ao mesmo tempo mantê-lo ligado fazendo escuta ambiental.

2. Deixá-lo num apostendo separado também é uma opção. Quanto mais afastado e isolado do local onde a reunião será realizada, melhor. Assim possíveis escutas ambientais instaladas no telefone não conseguirão captar a conversa.

3. Retirar a bateria: nem todo smartphone tem bateria removível. Aliás, a tendência atual é da maioria dos smartphones terem bateria interna, de modo que seja quase impossível desligá-los completamente.

   Naqueles que possuem, a retirada da bateria é uma medida interessante para evitar escutas ambientais.

4. Deixá-lo em casa em situações sensíveis: das medidas anti-grampo mais simples esta é a melhor: além de você ficar fora do raio de atuação de um possível grampo no celular, ele não estará rastreando a sua localização: para um espião que acredite estar de rastreando, ele poderá acreditar que você está em casa.

   Melhor ainda, ele terá dificuldades de descobrir que algumas pessoas estão reunidas num mesmo local se todas deixarem seus telefones em casa.

Falaremos em aplicações de comunicação mais seguras para evitar grampos em conversas telefônicas na aula sobre mensageria.

10.3.3 Softwares: medidas básicas

O que mais afeta hoje a privacidade de toda uma população é a quantidade de dados coletada automaticamente por aplicativos.

Por um lado, muitos aplicativos oferecem várias funcionalidades gratuitamente. Por outro, você está trocando com eles a sua privacidade. Pior que isso, até serviços pelos quais você paga estão coletando informações a seu respeito.

A arquitetura dos smartphones foi pensada exatamente para isso. Então é muito difícil de utilizá-la sem o efeito colateral de fornecer dados em excesso para empresas e governos.

Vou deixar então algumas dicas que não eliminam toda a vigilância realizada pelo seu telefone, mas que reduzem um pouco:

1. Preste atenção nas permissões solicitadas por cada aplicativo que você instalar.

   Repare que aplicativos maliciosos podem encontrar maneiras de burlar restrições no sistema.

2. Quanto menos aplicativos você usar, melhor. Isso depende do que você quer para a sua vida e para as pessoas que estão à sua volta. Mesmo aplicativos que pareçam ser inofensivos podem causar danos.

3. Dê preferência para softwares livres ou abertos. Além da loja de aplicativos padrão do seu telefone, você pode instalar lojas que oferecem apenas softwares livres, como é o caso do **F-Droid** para o Android. Sempre procure uma opção livre antes de buscar por um software proprietário.

10.3.4 Softwares: medidas avançadas

Se você quiser realmente usar um smartphone com um padrão de segurança mais alto, considere usar um telefone com sistema operacional livre ou aberto. Você pode, por exemplo, usar uma versão do Android padrão sem as customização das operadoras ou dos fabricantes, que tendem a colocar softwares com muitos bugs ou aplicativos com funcionalidades associadas à vigilância.

Você pode usar algum outro sistema baseado em Android como o **LineageOS**.

Atenção que, ao substituir o sistema operacional do seu smartphone, você pode perder a garantia do aparelho.

Ainda, a substituição exige que você desbloqueie o aparelho, isto é, fazer o **root** nele, o que pode diminuir a segurança pois aplicações terão mais privilégios de execução. Nesse caso, tome cuidado com as aplicações que você vai usar. Recomendaria nem usar a loja de aplicativos padrão, mas sim apenas aquelas que oferecem software livre e formas autenticadas de obteção de softwares, como o **F-Droid**.

Nas outras aulas serão apresentados softwares de comunicação e navegação específicos para telefones móveis.

10.4 Resumo

1. O telefone móvel é um dispositivo de rastreamento.
2. É possível ter um uso menos nocivo do telefone em termos de privacidade, mas não existe possibilidade razoavelmente segura.

10.5 Atividades

1. Expanda seu Checklist de Segurança para incluir seu telefone móvel.

CAPÍTULO 11

A Internet e a Web

11.1 Funcionamento

Os meios de comunicação digital estão convergindo rapidamente para a internet. Assim, o entendimento da segurança da informação na internet pode ser aproveitado para muitos casos de uso.

Nesta aula falaremos sobre o funcionamento básico da internet, que pode ser aplicado tanto ao contexto do acesso via computadores quanto smartphones.

A Internet é uma **rede de dados digital** baseada em diversos **protocolos**.

Por **rede** entendemos computadores que podem trocar mensagens entre si.

Já a **Web** pode ser definida como a parte da internet que interage com os usuários.

Apesar desta aula ser mais focada no navegador, a maior parte do que é dito aqui vale para outros aplicativos, tanto em computadores quanto em smartphones.

O uso seguro da web depende muitos fatores, por exemplo:

1. Problemas de segurança nos dispositivos de acesso. No caso deste curso, estamos falando de computadores e smartphones.
2. Fatores clássicos da segurança da informação: autenticidade, disponibilidade integridade e confidencialidade de cada interação realizada na internet.
4. Identificação e monitoramento de usuários.
5. Privacidade e uso de dados pessoais.

11.2 Ataques

Vamos nos concentrar nos principais ataques realizados na web:

1. Malware. É importante assumir que qualquer informação que recebemos da web pode conter algum código malicioso.

Esta é a forma mais acessível para invadir o sistema de alguém, pois não depende de ter acesso privilegiado a nenhum sistema. Qualquer pessoa pode fazer, não apenas empresas e governos mal intencionados.

Assim, tome cuidado ao abrir anexos e sites pouco confiáveis. Na dúvida, use alguma defesa apresentada na aula sobre computadores, como por exemplo abrir anexos usando um sistema virtualizado.

2. Vulnerabilidades no navegador também são portas de entrada possíveis para malware. A exploração de vulnerabilidades torna possível a infecção sem qualquer participação do usuário.

3. Sítios falsos: será que você está acessando o site correto ou é um clone tentando te convencer a fornecer informações pessoais ou te fornecendo informações falsas?

4. As redes sociais são também fontes de ataques à sua segurança.

   O modelo de negócios da maioria dessas plataformas é baseado na oferta do serviço em troca das sua interação. Todas as informações que você fornece às redes sociais podem ser revendidas ou usadas para qualquer fim estratégico, como propagandas, experimentos psicológicos ou controle social.

5. Dados pessoais e vazamentos. Pense que a publicação de um conteúdo é um caminho sem volta: podem até esquecer do que você disse, mas você não tem garantias que um conteúdo sumirá com o tempo e nem que você conseguirá apagar todas as cópias existentes.

   Considere que toda a mensagem, áudio, foto ou vídeo que você enviar para qualquer pessoa pode ser vazada. Esse vazamento pode ser restrito a um círculo de pessoas ou pode ser irrestrito.

   O vazamento pode ser involuntário ou não: pode ter a participação de quem recebeu sua mensagem ou pode ser feito por alguém que invadiu o sistema da pessoa.

   Pode ser alguém que invadiu um sistema onde estão essas informações.

   O vazamento nem sempre é focado em você: pode ser que toda uma plataforma de conteúdo tenha os dados vazados de todos os seus usuários e sua informação estar no meio.

11.2.1 Quais são as informações coletadas por cada serviço?

Virtualmente, qualquer coisa que enviamos para eles, sabendo ou não.

É fácil nos conscientizarmos de quais informações enviamos voluntariamente, porém é mais difícil perceber informações adicionais, ou metadados, que são enviados automaticamente pelos softwares que interagem com esses serviços.

Navegadores web enviam, por padrão, uma série de informações que podem ser usadas para nos identificar. Por exemplo:

- Informações específicas do navegador e o do sistema operacional, como versões, plugins suportados e assim por diante.
- Qual foi a página anterior visitada antes da página atual.
- Informações persistentes de interação com sites conhecidas como **cookies**, que podem ser criadas por qualquer site e ficam armazenadas no seu computador.

11.2.2 Quais são as informações que nos identificam e rastreiam nossos hábitos?

Rastreadores embarcados nos sites, como coletores de estatísticas e botões do tipo «curtir» conseguem estimar se estamos autenticados na respectiva rede social, qual o nosso login, etc.

Uma única página da web pode vir embutida com rastreadores de diversos serviços.

Este é o grande resumo que vale para redes sociais, mensageria, dados de formulário, informações de buscas, etc: Basicamente **TUDO** o que você envia na internet pode ser guardado indefinidamente, integrado a bancos de dados ou vazado.

E bastam poucas dessas informações para que seja possível nos identificar unicamente.

11.3 Defesas

Como podemos nos defender de uma situação em que qualquer interação pode ser registrada e utilizada indefinidamente? Existe uma saída para a segurança da informação ou este é o fim da privacidade?

Estas são boas perguntas. A história dirá. Por hora, temos algumas medidas de segurança possíveis para melhorar um pouco nossa situação.

1. Garantir a segurança da informação básica: a comunicação criptografada usando **HTTPS** é a forma básica de se transferir informações na web.

   O uso do HTTPS nos dá mais garantias de que estamos acessando o sítio legítimo e não uma versão falsa. Também garante que a comunicação não poderá ser interpretada ou adulterada por interceptadores.

   O uso do HTTPS depende da oferta deste pelo site ou serviço que você queira acessar. Um sítio que use HTTPS terá o seu endereço no navegador começando por **https://**, como por exemplo **https://wikipedia.org**.

   O fato do HTTPS estar disponível num site não implica necessariamente que a conexão é segura. O HTTPS possui vários problemas, como a dependência da certificação criptográfica feita por terceiros que podem ser invadidos ou serem compelidos a emitir certificações falsas.

   Ainda, o HTTPS pode estar mal implementado nos sites.

   Se você quiser avaliar a qualidade de uma conexão HTTPS, você pode testá-la usando um aplicativo específico ou então um serviço como o SSL Labs.

   Se ele for bem implementado, pode fornecer propriedades adicionais como sigilo futuro e usar algoritmos criptográficos bem fortes.

2. Usar logins e serviços somente quando necessário: você precisa estar autenticado(a) o tempo todo nas redes sociais? Quanto menos você usá-las, menos irão te rastrear.

3. Limitar o que o seu navegador pode fazer.

   Você pode limpar os arquivos locais armazenados pelo seu navegador, como cookies e histórico de navegação.

   Isso impede que eles sejam reutilizados, o que em si já é uma medida que dificulta a identificação de usuário.

   Isso também impede que esse tipo de informação seja obtida caso seu dispositivo seja invadido.

   Você também pode configurar seu navegador para nunca guardar esse tipo de informações ou para apagá-las toda vez que você for desligar o navegador.

   Uma medida adicional pode ser limitar a capacidade do seu navegador de processar sites, como por exemplo desligar o processamento do Javascript. Isso pode quebrar o funcionamento de alguns sites mas, por outro lado, pode impedir que sites maliciosos possem executar qualquer tipo de instrução no navegador.

4. Você pode usar serviços que possuam uma melhor política de privacidade. Por exemplo, você pode usar um mecanismo de busca alternativo como o **Duckduckgo**, que respeita muito mais a sua privacidade do que outros mais conhecidos.

5. Você pode utilizar um navegador especial feito para proteger a sua privacidade.

   Recomendo você utilizar o **Tor Browser** no seu computador e, no seu smartphone, o **Orfox** juntamente com o **Orbot**.

   Ambos os softwares utilizam a rede **Tor**, que é uma plataforma de navegação mais anônima. Ela utiliza criptografia e uma grande rede de computadores distribuídos pela internet que dificulta muito a localização dos usuários que estão navegando.

O Tor Browser é um navegador que usa a rede **Tor** em todas as suas conexões. Isso significa que ao navegar usando o Tor Browser você já estará, por padrão, dificultando sua localização na internet.

Mas **ATENÇÃO**: certifique-se de sempre usar conexão HTTPS ao acessar qualquer site usando o Tor Browser, do contrário você estará muito mais suscetível a ataques de interceptação e de site falso.

O Tor Browser também possui uma série de modificações de segurança para que a sua navegação fique mais segura.

Já o Orbot permite que seus aplicativos no smartphone utilizem a rede Tor.

11.4 Resumo

Navegar na internet pode parecer algo inofensivo, só que muitas vulnerabilidades em navegadores estão sendo exploradas para inúmeros fins, dentre eles a obtenção de dados do usuário disponíveis pelo navegador. Fora isso, sítios maliciosos podem levar o internauta a revelar voluntariamente seus dados. Contra essas e outras vulnerabilidades, tome as seguintes providências:

- Limpe sempre seu histórico de navegação, os arquivos temporários (cache) e os cookies
- Não salve no navegador suas senhas de formulários
- Saiba suspeitar quando um sítio é falso, ou seja, quando ele aparenta ser o sítio de uma empresa ou organização (em geral bancos) mas na verdade é apenas pretende obter suas senhas ou dados pessoais
- Use, sempre que disponível, conexão segura (https ao invés de http)
- Utilize alguma ferramenta de navegação anônima, como o Tor

11.5 Referências

- Panopticlick e Browserprint.
- Orbot para dispositivos Android | security in-a-box.
- Orfox: A Tor Browser for Android – Guardian Project.

CAPÍTULO 12

Mensageria

12.1 Funcionamento

Neste curso falaremos de mensageria instantânea e não instantânea.

Falaremos de comunicação por envio de texto, imagens, áudio e vídeo e também de chamadas de voz.

Em termos de segurança, tudo isso pode ser tratado conjuntamente, já que o princípio de funcionamento da mensageria é baseado naquilo que já foi dito ao longo do curso sobre transmissão de mensagens em meios digitais.

No entanto, na prática existem muitas aplicações, muitos padrões e muitos protocolos de comunicação. Existem as defasagens de segurança comuns a todos eles e também problemas específicos de cada plataforma.

Nos dois próximos capítulos trataremos de ataques e defesas na mensageria.

12.2 Ataques

Nós já mencionamos neste curso diversos ataques à segurança da informação: interceptação de comunicação, invasão de sistemas, roubo de material criptográfico, etc.

A maioria deles também se aplica à mensageria. Aqui vamos nos concentrar nos ataques específicos ou que devemos prestar atenção especial no caso da mensageria.

1. A aplicação de mensageria é bem estabelecida? Existem inúmeros aplicativos para comunicação instantânea, muitos deles afirmando inclusive serem seguros quando não são. O primeiro fator de insegurança pode ser um aplicativo que em si é inseguro.

2. No caso do aplicativo oferecer criptografia, ela é de ponto a ponto? Ou o conteúdo das mensagens pode ser acessado pelo serviço de mensageria?

   Pode ser importante observar também se a criptografia de ponta a ponta oferece negação plausível e a possibilidade de identificar chaves a usuários.

   No geral, a criptografia do aplicativo é bem implementada?

   A criptografia opera também nos metadados?

Nem sempre é fácil responder essas perguntas e por isso é importante ficar de olho nos aplicativos recomendados pela comunidade de segurança.

3. Como é feito o login na aplicação?

   Aplicativos que funcionam no computador em geral possuem autenticação com senha. Mas, no caso dos comunicadores de celular a criação de contas envolve a checagem com número de telefone como identificador global de usuários.

   Isso tem vários problemas. O número de telefone não é um dado anônimo e nem propriedade do usuário, mas sim da companhia telefônica. Além disso, se mal implementada essa confirmação pode ser burlada por atacantes para roubar sua conta ou espionarem a sua comunicação.

4. Onde ficam armazenadas as mensagens?

   É importante saber se as mensagens ainda não entregues ficam armazenadas no servidor sem criptografia. E, se depois de entregues, ficam armazenadas no dispositivo do usuário também sem criptografia.

12.3 Defesas

Para defender sua segurança na mensageria, vou recomendar algumas tecnologias e aplicativos que estão disponíveis em 2016.

Consulte sempre documentações atualizadas e confiáveis para novidades.

1. Para mensageria instantânia no smartphone, utilize o aplicativo Signal. Ele não é perfeito, mas é o melhor dentre todas as aplicações de mensagem instantânea para telefones.

   Benefícios do Signal incluem:

   - Faz chamadas por voz criptografadas usando o padrão ZRTP.
   - Criptografia ponto-a-ponto.
   - Sigilo futuro.
   - Armazenamento criptografado das suas mensagens no seu telefone caso você configure uma senha de bloqueio.
   - Permite que você faça a identificação de contatos com chaves criptográficas, processo conhecido como identificação criptográfica.
   - Possui um cliente de desktop que opera pareado ao smartphone.

   Limitações do Signal:

   - Apesar do cliente do Signal ser em código aberto, a parte do servidor não está inteiramente disponível.
   - O Signal utiliza a infraestrutura de mensageria do Google, o que não é muito bom em termos de privacidade e autonomia. Existe uma versão do Signal chamada de LibreSignal que não tem essa limitação, mas ela ainda não é muito estabelecida e talvez deixe de ser mantida.

2. Para mensageria instantânea no smartphone ou no computador, Comuncação Off-The-Record, ou OTR, que além de criptografia ponta-a-ponta suporta **negação plausível**.

   Existem vários softwares livres que implementam o protocolo OTR. Consulte as referências para detalhes.

3. Para comunicação por áudio e vídeo no seu computador, utilize o Jitsi diretamente no seu navegador.

4. Se você usa email e quer proteger sua comunicação, procure um provedor que respeite sua privacidade e suporte a tecnologia STARTTLS, que trocando em miúdos é o equivalente ao HTTPS no contexto do email

   Para proteger o conteúdo da mensagem ainda mais, utilize o padrão OpenPGP.

Nas referências você encontra links de manuais e guias de instalação de softwares de mensageria.

12.4 Email

O email é um sistema de comunicação muito popular que remonta às primeiras redes computacionais. Quando o sistema de email foi criado, não existia SPAM, vírus de email ou pessoas querendo interceptar suas mensagens. Por isso, os protocolos de comunicação de email não foram preparados para esses tipos de ataques. Em outras palavras, a insegurança do sistema de email já conhece pela arquitetura do próprio protocolo.

A falha do protocolo de email já começa com a problemática da privacidade, que é descrita nesta seção do Manual de Criptografia.

Além desse problema de terceiros poderem ler suas mensagens, o correio eletrônico ainda é uma porta para o recebimento de vírus. Para evitar esse tipo de inconveniente, use programas de email e um sistema operacional que sejam o mais imune possível.

Outro problema do sistema de email é a possibilidade de, apenas observando uma mensagem, descobrir por onde ela foi enviada. Isso não é exatamente uma vulnerabilidade, novamente é uma questão de design do sistema de email, onde as mensagens são etiquetadas por cada servidor por onde ela passou. Assim, se você receber um email de uma pessoa, em geral você pode olhar os cabeçalhos da mensagem e descobrir qual servidor a pessoa usou para enviar a mensagem! Essa informação é o chute inicial para que você descubra qual é o provedor que a pessoa usa e dependendo de quem você for é até possível descobrir de que local físico o email foi enviado.

Qual a solução para esses problemas com email?

- Use sempre Criptografia_e_internet conexão segura
- Verifique se o seu serviço de email oferece conexão segura e tem uma boa política de privacidade
- Evite ler emails de computadores públicos
- Use um sistema operacional seguro e um programa para ler emails que também seja seguro, caso contrário não abra anexos que contenham códigos que possam ser executados pelo seu sistema
- Se você acessa seu email via web, não esqueça de se desconectar dele após o uso

12.5 Listas de discussão

Participar de listas de discussão também requer medidas básicas de segurança:

- Sempre que você entrar numa lista de discussão, verifique se os arquivos da lista ficam disponíveis publicamente na internet.
- A lista de discussão, apesar de ter arquivos fechados, pode ser pública, ou seja, qualquer pessoa pode se inscrever e a partir disso ter acesso aos arquivos. Mesmo que ela seja fecha e com inscrição restrita, ainda pode haver vazamento dos arquivos.
- Não divulgue dados pessoais seus ou de terceiros em listas de discussão. Quando necessário, apenas faça isso em mensagens privadas.

12.6 Referências

- Autodefesa no E-mail - um guia para combater a vigilância encriptando com GnuPG.

CAPÍTULO 13

Backups Criptografados

13.1 Funcionamento

Backups são importantes para não perdermos nossas informações no caso de roubos, falhas de dispositivos ou erros humanos no apagamento de dados.

Backups fazem parte da segurança da informação porque eles estão associados à propriedade da disponibilidade.

O princípio básico de um backup é a cópia de informações de um lugar para outro para que os dados não sejam perdidos no caso de perda do local original, seja um computador ou smartphone.

Para que esses backups tenham alguma segurança, é importante que eles estejam criptografados. Afinal, do que adianta protegermos nossos dados com criptografia nos nossos dispositivos se nossos backups não estiverem também criptografados?

O funcionamento da criptografia para backups é análogo ao que tratamos no capítulo sobre computadores. Até o mesmo software pode ser utilizado, com a diferença que ele estará realizando a criptografia num volume de armazenamento externo ao computador.

Por isso, prosseguiremos adiante já tratando de duas estratégias de backup:

1. Utilizando um dispositivo de armazenamento externo. Pode ser um pendrive USB se você quer fazer backups de poucos arquivos. Ou pode ser um disco rídigo de capacidade suficiente para armazenar todos os seus arquivos.

   Sistemas operacionais livres como o Debian já suportam criptografia em discos externos, usando por exemplo o padrão LUKS.

2. Usando algum serviço de hospedagem na internet, o que tipicamente é chamado de **nuvem**. Uma «nuvem» nada mais é, nesse caso, do computador de outra pessoa.

Note que se você utilizar um local externo para armazenar todos os seus dados e não deixar nada armazenado no seu computador você não estará de fato fazendo backup, mas sim usando o armazenamento externo como armazenador principal das suas coisas.

Para que o local externo seja um backup, ele deve ser uma **cópia** dos seus arquivos. E uma cópia que você não mexe a não ser que for substituí-la por outra cópia, se for o caso, ou para acessar seus arquivos. Fora isso você não escreve nela.

13.2 Ataques

Tratemos de alguns ataques ao backup:

1. Problemas do backup em disco externo:
    - O disco pode ser roubado juntamente com o seu computador!
    - O disco pode e vai falhar em algum momento e aí você precisará comprar um outro disco para substituí-lo.
2. Problemas do backup na nuvem:
    - Não permita que a criptografia dos arquivos seja feita na nuvem. Ela deve ser feita nos seus dispositivos e só então os arquivos podem ser transferidos para o computador remoto. Caso contrário, tanto o serviço de armazenamento quanto algum invasor podem ter acesso aos seus dados antes deles serem criptografados.
    - Leve em conta que a «nuvem» não é uma entidade mágica. Ela pode estar sujeita à falhas ou o serviço pode ser interrompido. Quando você armazena seus backups num sistema que você não tem o controle, você está delegando a terceiros a guarda do seu backup, o que envolve uma perda de autonomia.

13.3 Defesas

As defesas básicas para um bom backup externo são estas:

1. No caso de backups em discos externos, use o método do «backup offsite», isto é, um backup do seus dados que fique longe do seu computador, de modo que o roubo de um deles não acarrete na perda de todos os seus dados.
2. No caso dos backups na nuvem, vale o que foi dito anteriormente: apenas transfira dados que já estejam criptografados. O processo de criptografia deve ocorrer, sempre que possível, nos dispositivos que você controla.

    É claro que na vida você pode acabar tendo que usar a nuvem para armazenar e editar documentos sem criptografia, mas pelo menos agora você saberá quais os riscos que você estará correndo para que possa dosar esse uso.

Pense em como proceder no caso do seu computador ser roubado. Como você acessaria os dados do backup? Você lembraria da senha? A senha seria a mesma senha do armazenamento criptografado do seu computador?

Lembre-se que você não está limitado ou limitada a utilizar um único método.

Você pode ter um ou mais backups criptografados em discos externos, backups criptografados na nuvem e até andar com um pendrive USB com um backup criptografado dos seus dados mais importantes.

Planeje-se também para realizar backups e testes periódicos dos backups.

Apenas fazer backups de tempos em tempos não é suficiente: é preciso checar se os backups estão realmente sendo realizados e se todos os dados estão sendo copiados corretamente.

13.4 Resumo

- Backups são fundamentais. Na dúvida, faça sempre backups criptografados.

13.5 Atividades

1. Faça backups criptografados dos seus dados de acordo com as recomendações desta aula :)
2. Planeje uma rotina periódica de realização e testes de backups. Qual a frequência ideal para você?

13.6 Referências

- VeraCrypt - Home.

CAPÍTULO 14

Rastros Digitais

14.1 Identidade

Além da sua senha, a questão da identidade também é importante. Não é necessário usar sempre seu nome real. Muito pelo contrário, é muito interessante adotar um ou mais pseudônimos, como o fez Fernando Pessoa, que inclusive reservou um estilo literário por heterônimo.

Você não precisa ser como Pessoa e criar muitos nomes e personalidades diferentes: o simples fato de você não usar seu nome ou seu nome completo já é grande progresso.

14.2 Apagamento de arquivos

Especial atenção também deve ser tomada na hora de apagar arquivos do seu computador. Se os arquivos contiverem informações que você não quer que de modo algum caiam nas mãos de terceiros, não adianta simplesmente apága-los da forma tradicional (usando os programas normalmente utilizados pelo seu sistema operacional). Isso porque:

- Em geral, quando você solicita a um programa para apagar um arquivo, ele apenas remove a referência do mesmo no «índice» do sistema de arquivos, mas os dados podem ou não continuarem dentro do disco rígido (veja por exemplo o truque do serrote do xmux.
- Mesmo que você tenha certeza que seu programa não só removeu a referência ao arquivo no índice do sistema de arquivos mas também sobrescreveu todos as informações do arquivo, ainda é possível recuperar os dados através de uma análise magnética do disco.

Uma ferramenta do GNU/Linux que tenta evitar ambos os problemas é o wipe. Um método complementar que funciona em algumas mídias é conhecido como ATA SECURE ERASE.

14.3 Identificação de fotografias

Ao publicar fotografias, tenha o cuidado de

1. Substituir o rosto das pessoas por operações irreversíveis (como por exemplo pintá-las nalgum programa de edição). Evite utilizar efeitos (como por exemplo espiralar regiões da imagem) porque muitas vezes eles podem ser desfeitos e revelar os rostos.
2. Remover os dados Exif (por exemplo com o programa jhead).

14.4 Bancos de dados de redes sociais

Redes sociais, como o famigerado Ferrabook ou as tradicionais correntes de emails são uma forma recente de se monitorar a associação entre pessoas. Pariticipar de uma rede social cuja infra-estrutura não tenha comprometimento com a preservação da privacidade dos usuários e usuárias é colaborar para a mineração de dados não-solicitada. Cuidado!

14.5 Tempestade eletromagnética

A chamada «tempestade eletromagnética» se refere à radiação emitida pelos equipamentos eletromagnéticos em funcionamento. Não é exclusividade de um transmissor emitir ondas eletromagnéticas moduladas: seu computador (principalmente seu monitor) faz isso o tempo todo.

Com aparelhos apropriados e a uma curta distância, é possível reconstruir a imagem que alguém está observando num monitor sem estar olhando diretamente para ele.

Este tópico está aqui de modo apenas ilustrativo, já que as técnicas utilizadas atualmente são dignas de filmes de espionagem e os equipamentos ainda são caros.

Como demostração, foi desenvolvido o software de GNU/Linux Tempest for Eliza, que permite qualquer pessoa transmitir uma mp3 em AM utilizando um monitor ligado num computador.

As contras medidas para esse tipo de ataque são:

- Compre um computador blindado smile (muito caro)
- Evite utilizar computadores em locais públicos ou de fácil acesso se você está realmente desconfiado/a de que exista alguém interessado em suas informações

14.6 Sobre

Texto originalmente publicado na Documentação do CMI Brasil

CAPÍTULO 15

Roteiros de Oficinas

Esta seção constitui um conjunto de roteiros modulares para ciclos de oficinas teóricas e práticas, com técnica e política sobre privacidade, vigilância, monitoramento e espionagem de massas em meios digitais.

Os temas estão divididos e podem ser aplicados na sequência ou separadamente conforme a necessidade do grupo.

Ela abrange o uso de ferramentas mais seguras usando o sistema operacional GNU/Linux e tópicos como criptografia, anonimato, segurança de conteúdo e de metadados, além de uma introdução à segurança em dispositivos móveis.

Além de recomendar práticas e ferramentas, o roteiro introduz o "mindset" de segurança, para que as próprias pessoas possam avaliar suas salvaguardas.

A segurança é abordada do pontos de vista técnico, sociológico, cultural, econômico e político. Existem várias formas de se acabar como movimentos sociais e a segurança pode ajudar não só em ofensivas violentas como também em casos de cooptação e desmobilização.

A análise da segurança a partir dos modos de produção, da forma de organização social e dos níveis tecnocientíficos existentes oferecem resultados de boa acurácia (open intelligence). Justificativa: o rombo contábil não pode ser imenso. Isso, porém, não exclui as possibilidades do desconhecido, do secreto e do espectulativo: cabe aos grupos fazerem suas análises, sínteses, etc.

A idéia destes roteiros é, mais do que dar o alimento, ensinar a produzi-lo.

15.1 Oficina Padrão

15.1.1 Metodologia

- Documentação da oficina pode ser redigida e complementada colaborativamente pelos/as participantes e publicada após o evento!
- Em cada dia será passada uma leitura de base para o conteúdo da aula seguinte.
- Todo dia alguém trazer algum caso prático ou teórico de vulnerabilidade.
- Elaborada para que seja reprodutível, oferecendo material suficiente para que a mesma possa ser reproduzida dentro dos critérios de segurança oferecidos.

15.1.2 Programação

Palestra: Segurança, privacidade e espionagem: o que está acontecendo e como podemos nos proteger?

Palestra introdutória contextualizando a necessidade de privacidade e anonimato utilizando modernas técnicas de criptografia frente às recentes revelações sobre espionagem de massa.

Dia 1: Discussão teórica sobre vigilância, espionagem e segurança.

Discussão de caráter técnico e político sobre o aparato existente de espionagem e monitoramento, com uma introdução sobre os conceitos básicos sobre segurança da informação.

Também será abordado:

- O uso e a qualidade de senhas.
- Conceitos básicos de criptografia, como chaves, impressões digitais e assinaturas.

Dia 2: Oficina Prática: Install Fest GNU/Linux com disco criptografado.

Dia para botar a mão na massa e instalar GNU/Linux no seu computador, já que o uso de software livre é um requisito para a segurança da informação.

Pré-requisitos:

- Trazer seu próprio computador laptop.
- Fazer um backup dos dados do seu computador ANTES da oficina se quiser instalar o GNU/Linux!

Dia 3: Discussão teórica e oficina prática: a rede de navegação anônima Tor e o sistema operacional amnésico Tails.

Discussão sobre anonimato e explicação sobre o funcionamento da rede Tor (The Onion Router - O Roteador Cebola) e de um sistema operacional orientado à segurança e anonimato conhecido como Tails (The Amnesic Incognito Live System).

Também será abordado:

- O uso e os perigos das redes sociais.
- Conexões criptografadas (HTTPS).

Traga seu laptop com GNU/Linux e aprenda a configurar o Tor! Traga um pendrive para instalar o Tails!

Se você não tiver um sistema GNU/Linux, traga seu computador mesmo assim para descobrir como instalar o Tor Browser Bundle!

Ainda, neste dia haverá um plantão especial para ajudar pessoas que tiveram dificuldade com seus GNU/Linux recém-instalados.

Dia 4: Discussão teórica: o mensageiro instantâneo off-the-record (OTR) e o padrão de criptografia OpenPGP.

O OTR é sistema de comunicação segura usado por Edward Snowden que possui:

- Criptografia ponto a ponto com sigilo futuro, isto é, possibilita que apenas as partes envolvidas na comunicação consigam interpretar as mensagens.
- Negação plausível, isto é, permite que ambas as partes neguem que tenham realizado a comunicação!

Já o OpenPGP foi o padrão que trouxe a criptografia para as massas e é amplamente utilizado na comunicação por email e também para a assinatura de dados e softwares.

Dia 5: Oficina prática: usando o OTR e o OpenPGP.

Traga seu laptop com GNU/Linux e aprenda:

- Configurar um programa comunicador instantâneo para usar o OTR.
- Configurar um leitor de email com suporte a OpenPGP, além de gerar o seu par de chaves.

E mais: ao final da oficina, uma mini-festa de assinatura de chaves OTR e OpenPGP.

Dia 6: Discussão teórica: segurança em dispositivos móveis.

A problemática da segurança nos dispositivos móveis será abordada, indicando mitigações e possibilidades futuras.

Dia 7: Revisão do conteúdo do ciclo de oficinas e aprofundamento de alguns temas.

Dia 8: Segurança para grupos.

15.2 Oficina Relâmpago

15.2.1 Missão

0. Explicar os conceitos básicos em segurança da informação
1. Recomendar práticas e ferramentas mais seguras
2. Introduzir a forma de pensar e agir em segurança para cultivar a autodefesa

15.2.2 Formato

0. Mini-palestra
1. Dúvidas anônimas anotadas em cartões coloridos por tópico
2. Respostas às dúvidas no final da oficina
3. Pode tirar fotos dos slides
4. Não tirar fotos ou filmar ninguém, incluindo a equipe da oficina
5. Não gravar o áudio da oficina

15.2.3 Conceitos

Conceitos que serão abordados brevemente (5 minutos cada tema):

0. A Economia da Segurança
1. O Plano de Autodefesa
2. A Segurança da Informação
3. A Teoria da Comunicação Hacker

15.2.4 Prática

O Plano Básico de Autodefesa Digital:

0. Senhas
1. Navegador Tor com HTTPS
2. Email mais seguro
3. Telefones móveis
4. Signal
5. Tarefas para a casa
6. Referências
7. Respostas e parte prática

15.2.5 A Economia da Segurança (5 min)

1. Segurança: toda prática que nos ajuda a agir ao reconhecer e reduzir riscos; é o oposto da paranóia.
2. Balanço: adote as práticas de segurança que sejam mais eficazes e menos custosas aos riscos que sejam mais prováveis!
3. Redução de danos: adote aos poucos as práticas de segurança.
4. Privacidade: conjunto de informações que queremos proteger.
5. Níveis: segurança se dá por níveis e procuramos proteger primeiro os níveis mais fundamentais.

15.2.6 A Economia da Segurança - 2

6. Compartimentalização: é a prática de segurança de isolar informações de acordo com a sua importância e necessidade. Por exemplo, falar com uma pessoa apenas o necessário para uma dada ação e manter algumas informações em círculos restritos de acesso.
7. Obscuridade: assuma que o inimigo conhece todas as suas defesas, mesmo que você não saiba se isso é verdade ou não. Isso vai te ajudar a contar apenas com a eficácia das suas defesas, e não com o fato dela ser ou não ser conhecida.
8. Resiliência: é a capacidade de resistir e se recuperar de ataques. Se as falhas não forem em pontos críticos, é possível se recuperar. Assim, é importante reduzir os pontos críticos de falha.

15.2.7 O Plano de Autodefesa

É o guardachuva de toda a segurança!

Item	Ameaça	Probabilidade	Defesa	Custo
Celular	Roubo	Alta	Backups cifrados	Baixo
			Celular desligado	Baixo
			Z	Alto
	X			
	Y			

Detalhes: https://plano.autodefesa.org/planilha.html

15.2.8 A Segurança da Informação

Propriedades úteis:

1. Confidencialidade: o conteúdo mensagem não será lida por pessoas ou sistemas indesejáveis.
2. Integridade: é a garantia de que o conteúdo da comunicação não foi adulterado por terceiros.
3. Disponibilidade: é a garantia de que o sistema de comunicação estará acessível sempre que necessário.
4. Autenticidade: garante que cada uma das partes possa verificar se está de fato se comunicando com quem pensa estar se comunicando, isto é, a garantia de que não há um impostor do outro lado da comunicação.

15.2.9 A Segurança da Informação - 2

5. Negação plausível: o oposto do não-repúdio é a negação plausível, no caso onde não é possível determinar com certeza se determinada pessoa participou da comunicação.
6. Anonimato: é garantia de que as partes envolvidas na comunicação não possam ser identificadas.
7. Auditabilidade: capacidade de inspecionar os sistemas de comunicação.

15.2.10 A Teoria da Comunicação Hacker

```
.                grampo ativo ou passivo
                           |
                           |
Emissor/a ---------------meio------------------ Emissor/a
Receptor/a       -----mensagem-1------>         Receptor/a
    1            <----mensagem-2-------            2
```

- Ataques: Interceptação de Dados e/ou Interceptação de Metadados.
- Algumas práticas de segurança protegem apenas os dados, enquanto outras apenas metadados; outras, ambos.

15.2.11 Senhas (cartões azuis) (10 minutos)

- Um segredo fácil de lembrar e difícil de descobrir para acessar sistemas.

- Como criar: dando asas à imaginação!
- Como memorizar: um pouco por dia; primeiro crie a senha, depois use.
- Como lidar com muitas senhas: uso, memória, círculos de senhas, gerenciadores de senha.

15.2.12 Navegador Tor com HTTPS (cartões verdes) (15 minutos)

- O que é?
- Do que protege
- Do que não protege

15.2.13 Email mais seguro (cartões amarelos) (10 minutos)

- O que é?
- Do que protege
- Do que não protege

15.2.14 Telefones móveis (cartões rosas) (10 minutos)

- Problemas: GSM, GPS, Wifi, Bluetooth, NFC, Câmera, Sensores, Sistema
- Como contorná-los

15.2.15 Signal (cartões laranjas) (20 minutos)

- O que é?
- Do que protege
- Do que não protege
- **Boas práticas**
  - Não usar o teclado padrão do telefone
  - Cuidado com o compartilhamento de contatos
  - Sempre usar mensagens temporárias
  - Frase senha de bloqueio do aplicativo
  - PIN code para evitar clonagem da conta
  - Verificação de contatos
  - Como perder um telefone corretamente

15.2.16 Bônus (cartões brancos) (10 minutos)

- Tails
- Etc!

15.2.17 Tarefas para a casa

0. Criar seu Plano Básico de Autodefesa
1. Criar senhas mais seguras
2. Instalar o Signal
3. Instalar o Navegador Tor
4. Criar email mais seguro
5. Ler o Guia de Autodefesa Digital
6. Bônus: usar o Tails

15.2.18 Referências

- Guia de Autodefesa Digital: https://guia.autodefesa.org
- Slides desta oficina: https://guia.autodefesa.org/_static/slides/relampago.pdf

15.2.19 Respostas e parte prática

?

15.3 Material de apoio

Não obrigatório, porém recomendável, ter todo o material para realizar a oficina offline, incluindo pacotes dos aplicativos que serão instalados:

- Lousa ou flip chart.
- Caneta pra lousa branca ou caneta piloto.
- Tomadas / réguas de luz (pelo menos 15 pontos de luz).
- Canetas e cartões coloridos (azuis, verdes, amarelos, vermelhos, rosas e brancos).
- Hub/switch ethernet e wireless (4 portas no mínimo).
- Cabos de rede (4 de 2 metros cada).
- Pendrives de 4GB.
- Projetor / datashow.
- Hub USB.
- Discos USB externos para backups cifrados.
- **Mini-NAS ou disco com:**
  - Loja F-Droid com apks úteis: OsmAnd, signal, briar, etc.
  - Espelhos locais APT (debian e ubuntu).
  - Cópias de distros (Debian, Ubuntu, etc) 32 e 64 bits com integridades verificadas.
  - Cópia checada do Virtual Box para Windows e OSX caso alguém não tenha feito backup da sua máquina mas queira ter uma noção do ambiente GNU/Linux.

CAPÍTULO 16

Referências

16.1 Referência Básica

Autodefesa digital: capacidade de uma pessoa ou grupo se proteger por conta própria de ameaças na comunicação eletrônica.

Por quê? A vigilância hoje é feita automaticamente e em larga escala: as pessoas são monitoradas mesmo que não sejam alvos específicos.

Segue um roteiro inicial ajudar você a se proteger e tomar escolhas conscientes! Este também é um convite para que você se aprofunde mais no assunto.

16.1.1 Os Princípios Básicos

1. Segurança: toda prática que nos ajuda a agir ao reconhecer e reduzir riscos.
2. Paranoia: é deixar de agir por conta de qualquer risco, real ou imaginário.
3. Privacidade: conjunto de informações que queremos proteger.
4. Conforto: quanto mais confortável e fácil for uma prática de segurança, mais chance ela tem de ser adotada. Cuidado com práticas super complicadas!
5. Redução de danos: adote procedimentos de segurança aos poucos, reduzindo os danos de forma sustentável, ao invés de tentar mudanças radicais que não sejam duradouras. Devagar e sempre!
6. Economia: procure adotar as práticas de segurança que sejam mais eficazes e menos custosas aos riscos que sejam mais prováveis! Uma boa segurança eleva o custo de alguém te atacar sem que você tenha um custo tão alto para se defender.
7. Simplicidade: não complique suas práticas desnecessariamente. A complexidade desnecessária pode criar falhas na segurança!
8. Níveis: uma boa segurança está presente em todos os níveis das tecnologias de comunicação, desde a segurança física dos dispositivos, passando pelos sistemas operacionais, pelos aplicativos e pelos protocolos de comunicação. O comprometimento de um dos níveis compromete no mínimo a segurança de todos os níveis superiores.

9. Compartimentalização: é a prática de segurança de isolar informações de acordo com a sua importância e necessidade. Por exemplo, falar com uma pessoa apenas o necessário para uma dada ação e manter algumas informações em círculos restritos de acesso.
10. Obscuridade: assuma que o inimigo conhece todas as suas defesas, mesmo que você não saiba se isso é verdade ou não. Isso vai te ajudar a contar apenas com a eficácia das suas defesas, e não com o fato dela ser ou não ser conhecida.
11. Abertura: busque sempre usar hardware, software e protocolos livres e abertos, porque eles podem ser analisados publicamente, o que facilita a correção de falhas de segurança. Mas cuidado, não assuma que todo o software e hardware livre é seguro e livre de falhas. Liberdade e abertura tecnológica são condições necessárias para a segurança, mas não são condições suficientes para a segurança.
12. Resiliência: é a capacidade de resistir e se recuperar de ataques. Se as falhas não forem em pontos críticos, é possível se recuperar. Assim, é importante reduzir os pontos críticos de falha.
13. Autoconsciência: cultive seu senso crítico e não deixe que as práticas de segurança tirem a sua naturalidade de agir ao tornar você uma pessoa robotizada.

16.1.2 Segurança da Informação

A segurança da informação é dividida em algumas propriedades:

1. Confidencialidade: é a garantia de que comunicação apenas poderá ser interpretada pelas partes envolvidas, isto é, mesmo havendo interceptação por terceiros, o conteúdo da comunicação estará protegido.

   Isso significa que, numa comunicação entre você e outra pessoa, haverá confidencialidade se apenas vocês tiverem acesso ao conteúdo da comunicação.
2. Integridade: é a garantia de que o conteúdo da comunicação não foi adulterado por terceiros.

   Ou seja, na comunicação entre você e outra pessoa, vocês conseguem identificar se alguém alterou o conteúdo das mensagens.
3. Disponibilidade: é a garantia de que o sistema de comunicação estará acessível sempre que necessário. Este é um requisito de segurança porque a falta de comunicação pode ser muito prejudicial.
4. Autenticidade: garante que cada uma das partes possa verificar se está de fato se comunicando com quem pensa estar se comunicando, isto é, a garantia de que não há um impostor do outro lado da comunicação.
5. Não-repúdio: garante que as partes envolvidas na comunicação não possam negar ter participado da comunicação. Esta propriedade é desejada em sistemas nos quais haja um controle sobre quem realizou determinados tipos de operações.
6. Negação plausível: o oposto do não-repúdio é a negação plausível, no caso onde não é possível determinar com certeza se determinada pessoa participou da comunicação.
7. Anonimato: é garantia de que as partes envolvidas na comunicação não possam ser identificadas.
8. Auditabilidade: capacidade de inspecionar os sistemas de comunicação.

Nem sempre os sistemas satisfazem todas essas propriedades, seja intencionalmente ou não. É importante observar o que cada sistema oferece em termos dessas propriedades e se elas estão bem implementadas no sistema.

Por exemplo, alguns sistemas foram criados para possuir a propriedade do não-repúdio, enquanto outros são baseados na negação plausível.

Em muitas situações, é possível combinar diversos sistemas que ofereçam propriedades distintas de segurança da informação para obter o máximo de propriedades possíveis.

16.1.3 Limites da segurança

Viver é perigoso! Mas o que seria viver sem arriscar? Segurança tem limites e faz parte de uma atitude segura saber quais são eles. Os principais são:

1. Incompletude: não existe segurança total ou sistema infalível. Todo sistema possui falhas.
2. Ceticismo: é possível descobrir se sua segurança está sendo comprometida, mas isso nem sempre acontece. Pode ser que sua segurança esteja sendo comprometida sem que você saiba. Adote um ceticismo saudável para não ter ilusões sobre a sua segurança.
3. Malícia: nem sempre uma falha é resultado de um ataque intencional. Às vezes a comunicação tem problemas por falta de qualidade e não porque alguém esteja te atacando.

   Muitas vezes é difícil saber se você está sendo atacada/o ou se está sofrendo apenas uma falha de funcionamento num dispositivo.

   É sempre bom estar alerta e não baixar a guarda, mas você não precisa assumir logo de cara que está sendo atacada/o sempre que houver falha. Menos paranoia, mais senso crítico e intuição!
4. Preparação: prepare-se para a possibilidade da suas prática seguras falharem. Quando a casa cair, o que você vai fazer? Se preparar para isso também é uma prática segura!

16.1.4 Checklist

Mais do que sair adotando práticas e ferramentas de segurança, é importante que você tenha uma noção do todo e também das partes, ou seja, que você organize suas práticas de segurança num todo consistente.

Uma maneira fácil de fazer isso é manter um Checklist de Segurança:

1. Faça uma lista das suas atividades. Como cada uma delas funciona? Elas dependem de algum dispositivo tecnológico? Como eles funcionam em linhas gerais? Pesquise!
2. Quais são as ameaças envolvidas nessas suas atividades? Quem poderia te atacar? Como os dispositivos tecnológicos poderiam falhar? Pesquise e use a sua imaginação!

3. A partir do conhecimento reunido, como você poderia se proteger? Existem diversos guias práticos sobre como se defender.

Por fim, faça escolhas:

- Comece pequeno e vá aos poucos. Você é capaz!
- Priorize as ameaças mais prováveis e as defesas que estejam ao alcance da sua capacidade. Cada pessoa tem seu ritmo.
- Segurança não é um fetiche: não adote uma prática só porque ela está na moda ou é considerada chique, mas sim se ela é útil para você.

16.1.5 Comunicação Digital

Nosso foco aqui é comunicação digital! Então vamos começar com nosso desenho esquemático da Teoria da Comunicação Hacker:

```
.                    grampo ativo ou passivo
                                |
                                |
Emissor/a ---meio----------meio-------------meio------ Emissor/a
```

(continues on next page)

(continued from previous page)

```
Receptor/a          -----mensagem-1------>          Receptor/a
    1               <----mensagem-2-------             2
```

Nesse desenho, duas partes envolvidas numa comunicação trocam mensagens entre si através de um meio que assumimos estar grampeado por padrão!

Ele não precisa estar necessariamente grampeado, mas se assumirmos que ele está, nós já estaremos nos preparando para as situações em que ele esteja!

Os ataques fundamentais da vigilância das comunicações são:

1. Interceptação de Dados: é a escuta do conteúdo da comunicação. Pode ser passiva – apenas grava a comunicação – ou ativa – quando também interfere na comunicação, alterando mensagens.

2. Interceptação de Metadados: quando apenas as informações básicas da comunicação são gravadas. Quem fala com quem, quando, onde, por quanto tempo, etc, sem que o conteúdo das mensagens seja obtido necessariamente.

É importante saber que algumas práticas de segurança protegem apenas os dados, enquanto outras protegem apenas os metadados da comunicação. Também existem práticas que protegem ambos!

Lembre-se que a vigilância é feita não apenas pelos governos, mas também por empresas.

16.1.6 Criptografia

Usamos criptografia para nos defender dos ataques à comunicação digital.

Ela codifica dados e/ou metadados para que a informação possua um ou mais critérios de segurança como confidencialidade, integridade e autenticididade.

Em sua aplicação mais básica, a criptografia é a técnica de codificar mensagens de tal modo que apenas quem possuir o segredo de como decodificá-las pode acessar seu conteúdo original.

Essas e outras propriedades da segurança da informação podem ser obtidas juntas ou separadas dependendo do sistema criptográfico em uso.

Hoje é essencial que meios de comunicação possuam algum tipo de criptografia, sendo essa uma condição básica para que resistam a ataques informacionais.

Para ser eficaz, a criptografia precisa usar padrões bem estabelecidos e ser bem implementada, do contrário ela só traz ilusão de segurança.

Também é importante que a criptografia seja de ponta-a-ponta, isto é, que seja realizada integralmente nos dispositivos de comunicação das pessoas e não em dispositivos intermediários e que estejam fora do nosso controle.

16.1.7 Senhas

Para usar sistemas de comunicação com mais segurança é importante saber o básico e essencial sobre senhas.

Para ter acesso a determinados sistemas ou lugares, pode ser necessário fornecer uma prova de acesso para que ocorra uma **autenticação**, isto é, uma permissão de acesso.

Existem vários tipos de autenticação:

1. A autenticação pode ser baseada em algo que você carrega: por exemplo um cartão de crédito, um crachá ou documento de identificação.

2. A autenticação pode ser baseada em algo que só você ou um grupo restrito de pessoas sabe. Chamamos essa informação de **senha**.

3. Ela também pode se basear em alguma característica física sua e nesta caso estamos falando de **biometria**.

Aqui trataremos apenas sobre senhas, que é a forma de autenticação mais utilizada na comunicação digital. Biometria pode ser forjada e algo que você carrega no bolso pode ser roubado. Mas extrair uma senha da sua mente já envolve mais trabalho. Daí o poder das senhas!

Boas senhas possuem as seguintes características:

1. Memorizável: uma senha muito difícil de lembrar pode levar ao seu esquecimento e ser difícil de digitar.

   Já uma senha muito fácil de lembrar também pode ser muito fácil de alguém descobrir. Senhas muito fáceis em geral também tem um tamanho pequeno, então pense num tamanho mínimo e memorizável quando criar sua senha.

2. Difícil de descobrir: quanto mais difícil de descobri-la, melhor. Mas isso pode acarretar numa complexidade da senha que a torna difícil de lembrar.

3. Pouco ou não compartilhada: se você usa a senha para uma coisa, e uma única coisa apenas, é mais difícil dela ser descoberta. Quanto mais compartilhada, maior o risco, pois a superfície de ataque à senha aumenta.

   Esta característica vem diretamente do princípio da compartimentalização: se uma senha for comprometida, o dano estaria restrito apenas a um ou poucos sistemas.

   Uma senha roubada pode ser usada como tentativa para invadir outros sistemas. Se você usa a mesma senha para mais de um sistema e ela for roubada, trate logo de mudar a senha em todos os sistemas.

16.1.8 Computadores

O computador se transformou no elemento básico da comunicação digital.

Existem muitas falhas nos computadores em todos os níveis: no hardware, no sistema operacional e nos programas utilizados, assim como muitas formas de se defender.

Medidas básicas de segurança para computadores incluem:

- Usar software livre, como o sistema operacional Debian GNU/Linux.
- Usar criptografia de armazenamento.
- Manter o sistema sempre atualizado.

Consulte documentações específicas para mais detalhes :)

16.1.9 Telefones

Os smartphones são uma catástrofe em termos de segurança e privacidade:

1. Seu funcionamento é baseado no rastreamento do aparelho, ou seja, todo telefone móvel é um dispositivo de rastreamento.
2. Existem problemas no hardware dos telefones que permitem acesso especial pelas operadoras de telefonia ou atacantes especializados.
3. O smartphone é também um computador, possuindo diversas das vulnerabilidades existentes em computadores.
4. O smartphone foi feito intencionalmente para ser um coletor automáticos de informações. Essas informações seguem para diversas empresas que a utilizam de forma estratégica para levarem vantagem em relação a toda a sociedade. Muitas dessas informações também acabam nas mãos dos governos e outras organizações.

É muito difícil usar um telefone de forma segura pois a arquitetura dos smartphones joga o tempo todo contra a segurança e a privacidade. Aqui não há espaço para uma análise detalhada então deixamos apenas as dicas mais básicas:

1. Mantenha o sistema do seu telefone sempre atualizado.
2. Preste atenção nas permissões solicitadas por cada aplicativo que você instalar.

   Repare que aplicativos maliciosos podem encontrar maneiras de burlar restrições no sistema.
3. Quanto menos aplicativos você usar, melhor. Pense no que é essencial para você. Mesmo aplicativos que pareçam ser inofensivos podem causar danos.
4. Dê preferência para softwares livres ou abertos. Além da loja de aplicativos padrão do seu telefone, você pode instalar lojas que oferecem apenas softwares livres.

   Sempre procure uma opção livre e aberta antes de buscar por um software fechado.
5. Quando precisar ter uma conversa sigilosa com alguém, combine com a pessoa para que vocês deixem seus telefones em casa antes de se encontrarem. Isso evita rastreamento e gravação de conversas via smartphone.

   A medida mais simples e eficaz é não usar telefone, mas hoje em dia está cada vez mais difícil viver sem ele por conta de imposições sociais. Assim, pode ser necessário fazer um uso estratégico dessa tecnologia.

16.1.10 Segurança na Rede

Qualquer informação que enviamos na internet está sujeita à vigilância.

É fácil nos conscientizarmos de quais informações enviamos voluntariamente, porém é mais difícil perceber informações adicionais, ou metadados, que são enviados automaticamente pelos softwares e serviços que utilizamos.

Quais são as informações que nos identificam e rastreiam nossos hábitos?

Rastreadores embarcados nos sites, como coletores de estatísticas e botões do tipo «curtir» conseguem estimar se estamos autenticados na respectiva rede social, qual o nosso login, etc.

Uma única página da web pode vir embutida com rastreadores de diversos serviços.

Este é o grande resumo que vale para redes sociais, mensageria, dados de formulário, informações de buscas, etc: Basicamente **TUDO** o que você envia na internet pode ser guardado indefinidamente, integrado a bancos de dados ou vazado.

E bastam poucas dessas informações para que seja possível nos identificar unicamente.

Como podemos nos defender de uma situação em que qualquer interação pode ser registrada e utilizada indefinidamente? Existe uma saída para a segurança da informação ou este é o fim da privacidade?

Estas são boas perguntas. A história dirá. Por hora, temos algumas medidas de segurança possíveis para melhorar um pouco nossa situação.

1. Garantir a segurança da informação básica: a comunicação criptografada usando **HTTPS** é a forma básica de se transferir informações na web.

   O uso do HTTPS nos dá mais garantias de que estamos acessando o sítio legítimo e não uma versão falsa. Também garante que a comunicação não poderá ser interpretada ou adulterada por interceptadores.

   O uso do HTTPS depende da oferta deste pelo site ou serviço que você queira acessar. Um sítio que use HTTPS terá o seu endereço no navegador começando por **https://**, como por exemplo **https://wikipedia.org**.

   O fato do HTTPS estar disponível em um site não implica necessariamente que a conexão é segura. O HTTPS possui vários problemas, como a dependência da certificação criptográfica feita por terceiros que podem ser invadidos ou serem compelidos a emitir certificações falsas.

   Ainda, o HTTPS pode estar mal implementado nos sites.
2. Usar logins e serviços somente quando necessário: você precisa estar autenticado(a) o tempo todo nas redes sociais? Quanto menos você usá-las, menos irão te rastrear.

3. Você pode utilizar um navegador especial feito para proteger a sua privacidade.

   Recomendamos que você utilize o **Tor Browser** no seu computador e, no seu smartphone, o **Orfox** juntamente com o **Orbot**.

   Ambos os softwares utilizam a rede **Tor**, que é uma plataforma de navegação mais anônima. Ela utiliza criptografia e uma grande rede de computadores distribuídos pela internet, que dificulta muito a localização dos usuários que estão navegando.

   O Tor Browser é um navegador que usa a rede **Tor** em todas as suas conexões. Isso significa que ao navegar usando o Tor Browser você já estará, por padrão, dificultando sua localização na internet.

   Mas **ATENÇÃO**: certifique-se de sempre usar conexão HTTPS ao acessar qualquer site usando o Tor Browser. Do contrário, você estará muito mais suscetível a ataques de interceptação e de site falso.

   O Tor Browser também possui uma série de modificações de segurança para que a sua navegação fique mais segura.

   Já o Orbot permite que seus aplicativos no smartphone utilizem a rede Tor.

4. Procure usar serviços que respeitem a sua privacidade e que não façam dinheiro a partir da coleta das suas informações.

16.1.11 Mensageria

A decisão de quais comunicadores instantâneos utilizar é muito importante. Aqui seguem dicas para que você tenha condições de escolher por conta própria:

1. A aplicação de mensageria é bem estabelecida? Existem inúmeros aplicativos para comunicação instantânea, muitos deles afirmando inclusive serem seguros quando não são. O primeiro fator de insegurança pode ser um aplicativo que em si é inseguro.

2. No caso do aplicativo oferecer criptografia, ela é de ponto a ponto? Ou o conteúdo das mensagens pode ser acessado pelo serviço de mensageria?

   Pode ser importante observar também se a criptografia de ponta a ponta oferece negação plausível e a possibilidade de identificar chaves a usuários.

   No geral, a criptografia do aplicativo é bem implementada?

   A criptografia opera também nos metadados?

   Nem sempre é fácil responder essas perguntas e por isso é importante ficar de olho nos aplicativos recomendados pela comunidade de segurança.

3. Como é feito o login na aplicação?

   Aplicativos que funcionam no computador, em geral, possuem autenticação com senha. Mas, no caso dos comunicadores de celular, a criação de contas envolve a checagem com número de telefone como identificador global de usuários.

   Isso tem vários problemas. O número de telefone não é um dado anônimo e nem propriedade do usuário, mas sim da companhia telefônica. Além disso, se mal implementada, essa confirmação pode ser burlada por atacantes para roubar sua conta ou espionarem a sua comunicação.

4. Onde ficam armazenadas as mensagens?

   É importante saber se as mensagens ainda não entregues ficam armazenadas no servidor sem criptografia. E, se depois de entregues, ficam armazenadas no dispositivo do usuário também sem criptografia.

16.1.12 Softwares Recomendados

No smartphone:

- Signal Messenger para comunicação instantânea.
- Orbot e Orfox para navegação anônima.
- No Android, use a central de aplicativos livres F-Droid.
- Se possível, utilize um sistema operacional livre como o LineageOS.

No computador:

- Adote um sistema operacional livre, como o Debian GNU/Linux.
- Use o Tor Browser Bundle para navegação na web com mais anonimato.
- Para situações críticas, use o Tails, um sistema operacional livre e mais seguro.

16.1.13 Referências

- Guia de Autodefesa Digital - https://guia.autodefesa.org
- Tem boi na linha? Guia prático de combate à vigilância na internet - https://temboinalinha.org
- A Criptografia Funciona - Como Proteger Sua Privacidade na Era da Vigilância em Massa - https://we.riseup.net/deriva/a-criptografia-funciona-como-proteger+260170
- Security in a Box - Ferramentas de Segurança Digital para todas as pessoas - https://securityinabox.org/pt/
- PRISM Break - https://prism-break.org/pt/
- Guia de Protestos - https://protestos.org

16.1.14 Licença

Este conteúdo está disponível sob a licença Creative Commons — Attribution-ShareAlike 3.0 Unported — CC BY-SA 3.0 - https://creativecommons.org/licenses/by-sa/3.0/

16.2 Bibliografia

16.2.1 Em português

Criptografia:

- O Livro dos Códigos, de Simon Singh.

Hacking:

- A Arte de Enganar, de Kevin Mitnick.

História e sociedade:

- Vigilância Líquida, de Zygmunt Bauman.
- Ministério do Silêncio.
- Quem pagou a conta? A CIA na guerra fria da cultura.
- Atividade de Inteligência e Legislação Correlata.

- Livros sobre o Snowden.
- **Wikileaks:**
  - Quando o Google encontra o Wikileaks.

Literatura:

- Livros do John le Carré.
- O Candidato da Manchúria.

16.2.2 Em espanhol

- Diagnósticos en seguridad digital para organizaciones defensoras de derechos humanos y del territorio: un manual para facilitadores.
- Zen y el arte de que la tecnología trabaje para ti.

16.2.3 Em inglês

- **Livros do Bruce Schneier:**
  - Data and Goliath.
- The American Black Chamber.
- The Codebreakers. (2).
- **Livros do James Bamford sobre a NSA.**
  - Puzzle Palace.
  - The Shadow Factory.
- Livros do James Risen.
- This Machine Kills Secrets.
- No Place to Hide.
- Underground. - Hacker Crackdown.
- Cypherpunks.
- The Like Switch: A Former FBI Agent Explains How to Tell When Someone Is Lying to You | Inc.com.
- NSA's Transformation: An Executive Branch Black Eye by Edward Loomis.
- Vigiância Líquida.
- Spies for Hire: The Secret World of Intelligence Outsourcing.
- Exploding the Phone.
- Livros do Jacques Henno.
- The Rise of the Computer State.
- Livros do James Bamford.
- Secret Manoeuvres in the Dark: Corporate Spying on Activists.
- Livros do James Risen.
- Obra de Somerset Maugham.

- Obra de Compton Mackenzie.
- The American Black Chamber.
- The Soul of a New Machine.
- The Codebreakers: The Story of Secret Writing (by David Kahn).
- No Place to Hide.
- This Machine Kills Secrets.
- Takedown (resenha).

16.3 Filmografia

Filmografia sobre segurança, privacidade, vigilância e espionagem.

16.3.1 Não-ficção

- Citizenfour (2014).
- The Gatekeepers.
- The Most Dangerous Man in America: Daniel Ellsberg and the Pentagon Papers.
- The Vula Connection.
- The Internet's Own Boy: The Story of Aaron Swartz.
- VIPs: Histórias Reais de um Mentiroso (2010).
- Collateral Murder (2010).
- Shoshana Zuboff on surveillance capitalism | VPRO Documentary.
- XPloit: Internet sob ataque (websérie 1-6).
- Don't Fuck with Cats (2019).

16.3.2 Ficcionalizados

- A Batalha de Argel (1966).
- Snowden.
- Takedown (2000).
- The Imitation Game (2014).
- Argo (2012).
- The Report (2019).
- Official Secrets (2019).
- Wasp Network (2019).
- The Post (2017).

16.3.3 Ficção

- A Most Wanted Man - Wikipedia.
- Sneakers.
- The Conversation.
- Catch Me If You Can.
- The Lives of Others.
- Brazil.
- 1984.
- The Girl with the Dragon Tattoo (2009).
- Wargames (1984).
- Hackers (1995).
- Tinker Tailor Soldier Spy (2011).
- The Little Drummer Girl (2018).
- Our Kind of Traitor (2016).
- Gattaca.
- J. Edgar (2011).
- The Departed (2006).
- The Night Manager (2016).
- Red Sparrow (2018).
- Atomic Blonde (2017).
- The Constant Gardener (2005).
- Ghost in the shell (2017).

16.3.4 Referências

- Movies for Hackers.

16.4 Legislação

- Esta não é uma lista completa.

16.4.1 Legislação Brasileira

- Guia de Direitos.
- Manual de sobrevivência na selva de bits: evitando as ações judiciais contra publicações na Internet.
- Lei 9453/97 - Retenção de documentos:

```
"§ 2º Quando o documento de identidade for indispensável para a
entrada de pessoa em órgãos públicos ou particulares, serão seus
dados anotados no ato e devolvido o documento imediatamente ao
interessado."
```

- Lei 9.296/96: Interceptação Telefônica (Lei do Grampo).
- Lei 9883/99: Criação da ABIN e do SBI
- Decreto 4376/2002: Funcionamento e organização do SBI
- CF/88 - XII do artigo 5 - Sigilo da correspondência

```
"XII - é inviolável o sigilo da correspondência e das comunicações
      telegráficas, de dados e das comunicações telefônicas, salvo, no último␣
↪caso,
      por ordem judicial, nas hipóteses e na forma que a lei estabelecer para␣
↪fins de
      investigação criminal ou instrução processual penal;"
```

- CF/88 - XXXIII do artigo 5 - Habeas Data

```
"XXXIII - todos têm direito a receber dos órgãos públicos informações
de seu interesse particular, ou de interesse coletivo ou geral, que
serão prestadas no prazo da lei, sob pena de responsabilidade,
ressalvadas aquelas cujo sigilo seja imprescindível à segurança da
sociedade e do Estado"
```

- Lei 9507/97: Alteração do Habeas Data
- Lei Carolina Dieckmann - Cibercrimes.
- Lei Azeredo - Cibercrimes.
- Marco Civil da Internet.
- Lei de Segurança Nacional - LEI Nº 7.170, DE 14 DE DEZEMBRO DE 1983.
- Lei das Organizações Criminosas - LEI Nº 12.850, DE 2 DE AGOSTO DE 2013.

São Paulo

- Lei Municipal (São Paulo) Nº 13.541/2003 (ver alterações):

```
Dispõe sobre a colocação de placa informativa sobre filmagem de
ambientes, e dá outras providências
```

16.4.2 Legislação Internacional

Geral

- Mutual legal assistance treaty (MLAT).

EUA

- Privacy Act of 1974.

- Foreign Intelligence Surveillance Act (FISA).
- Executive Order 12333 (substituída pela USSID SP0018).
- CALEA.
- Electronic Communications Privacy Act.
- USA PATRIOT Act (em especial a seção 215).
- National security letter (em especial a seção 702).

Reino Unido

- Regulation of Investigatory Powers Act 2000 (RIPA).

França

- Justiça dos nomes de domínios in Francia.

Estas são referências complementares a este guia, o que não significa que avaliamos, concordamos, ou recomendamos necessariamente o seus conteúdos.

16.5 Guias práticos

16.5.1 Em português

- A Criptografia Funciona - Como Proteger Sua Privacidade na Era da Vigilância em Massa.
- Guia de Protestos.
- Security-in-a-box
- PRISM Break
- Segurança da Informação.
- Dicas de privacidade
- Cultura de Segurança
- Internet Segura do CGI.br.
- Guia prática de estratégias e táticas para a segurança digital feminista.
- Segurança Holística.
- Data Detox Kit.
- Tem boi na linha? » Guia prático de combate à vigilância na internet.
- Oficinas e Ferramentas | Oficina Antivigilância

16.5.2 Em espanhol

- Quema tu móvil.

- Cibermujeres: currícula de seguridad digital con enfoque holístico y perspectiva de género que tiene el fin de brindar experiencias de aprendizaje para defensoras de derechos humanos que trabajan en entornos de alto riesgo..
- Protege.la: espacio abierto para compartir recursos sobre seguridad y privacidad digital.
- Registrando Incidentes de Seguridad Digital como Práctica de Mitigación del Riesgo.

16.5.3 Em inglês

- Organisational Security Wiki.
- Freedom of the Press Foundation - Guides & Training.
- Holistic security.
- Surveillance Self-Defense | Tips, Tools and How-tos for Safer Online Communications.
- Email Self-Defense - a guide to fighting surveillance with GnuPG encryption
- Anonymity/Security: A practical guide to computers for anarchists
- Quick Guide to Alternatives
- Me and my Shadow
- Information Security for Journalists | tcij.org
- Cybersecurity Policy for Human Rights Defenders - Publication | Global Partners Digital
- Complete manual - Gender and Tech Ressources
- Security in Context
- ActivistSecurity collective
- Digital Security and Privacy for Human Rights Defenders.
- Rebel-Alliance-Tech-Manual: Introduction to electronic security for activists and dissidents.
- Security Tips Every Signal User Should Know
- Guia para furar a censura (dicas do Boing Boing)
- Security Culture for Activists da Ruckus Society.
- Integrated security | Integrated security - the Manual.
- Security Culture - A Comprehensive Guide for Activists in Australia.
- OPSEC Resources.
- Privacy Tools.
- Practical Privacy and Security.
- Security Planner.
- Digital Security Readiness Assessment Tool.
- LevelUp.
- Holistic Security.
- Security Education Companion (SEC).
- Helpdesk - Reporters Without Borders.

- Cyberwomen: digital security curriculum with a holistic and gender perspective, aimed at offering trainers with tools to provide in-person learning experiences to human rights defenders and journalists working in high-risk environments.

16.5.4 Noutros idiomas

- Guide d'autodéfense numérique.

16.6 Debian

- Securing Debian Manual.
- Verifying authenticity of Debian CDs (How to tell if the key is safe).

16.7 Análises, discussões e aprofundamentos

- Warren and Brandeis, «The Right to Privacy».
- Why I Wrote PGP.
- The Economics of Mass Surveillance and the Questionable Value of Anonymous Communication.
- O que todo revolucionário deve saber sobre a repressão (1929).
- Cryptography I - Stanford University | Coursera.
- Salta Montes - traduções para o português no tema da segurança digital e guerra psicológica.
- Glossário draft-dkg-hrpc-glossary-00 - Human Rights Protocol Considerations Glossary.

CAPÍTULO 17

Meta

Manual em desenvolvimento por Autodefesa.

17.1 Licençiamento

Não havendo menção contrária, todo o conteúdo é disponível de acordo com

- Creative Commons — Attribution-ShareAlike 3.0 Unported — CC BY-SA 3.0.
- Definition of Free Cultural Works.
- Logo: Karate Girl.

17.2 Baixando o repositório

URL pública, somente leitura:

```
git clone --recursive https://0xacab.org/autodefesa/guia
```

17.3 Contribuindo

Este wiki utiliza o padrão de documentação da Autodefesa.

17.4 Em construção

Este guia sempre estará incompleto e sempre estará em construção!