A Criptografia Funciona
Como Proteger Sua Privacidade na Era da Vigilância em Massa

Micah Lee
Diretor de Tecnologia

Julho de 2013

FREEDOM
OF THE PRESS
FOUNDATION

Dedicado para todos os cypherpunks que programam.
Suas habilidades são necessárias agora mais do que nunca.

Autor: Micah Lee

Uma publicação da **Fundação da Liberdade de Imprensa**, 2013

Tabela de Conteúdos

Introdução 4

Modelo de Ameaça 4

Sistemas de Criptografia 5

Software que você pode confiar 6

Anonimize sua localização com Tor 9

Off-the-Record (OTR) Chat 10

Provedores de Serviços e Jabber 11

Clientes OTR 11

Sua Chave 11

Sessões 12

Verificação da Impressão Digital do OTR 13

Registros 15

Criptografia de Email “Pretty Good Privacy” (PGP) 16

Par de chaves e chaveiros 16

Frases secretas 17

Software 18

Criptografar, Descriptografar, Assinaturas 18

PGP não é apenas para Email 20

Verificação de Identidade 21

Ataques 23

Tails: O Sistema Amnésico Incógnito Live 24

PGP e Email no Tails 25

Fluxo de Trabalho 27

Uma Chance de Luta 29

A Criptografia Funciona

Como Proteger Sua Privacidade na Era da Vigilância em Massa

> *A criptografia funciona. Os sistemas criptográficos fortes e devidamente implementados são uma das poucas coisas em que você pode confiar. Infelizmente, a segurança na ponta final é tão terrivelmente fraca que a NSA pode frequentemente achar formas de contorná-los.*
>
> - Edward Snowden, respondendo perguntas ao vivo no site do *The Guardian*[1].

A *National Security Agency (*NSA, Agência de Segurança Nacional) é a maior, mais bem financiada agência de espionagem jamais vista. Eles gastam bilhões e bilhões de dólares por ano fazendo tudo o que podem para extrair a comunicação digital da maior parte dos humanos nesse planeta que possuem acesso à Internet e à rede telefônica. E como mostram as matérias recentes no Guardian e Washington Post, nem mesmo as comunicações americanas domésticas estão a salvas de suas interceptações.

Defender-se contra a NSA, ou contra qualquer agência de inteligência do governo, não é simples, e não é algo que pode ser resolvido baixando um aplicativo. No entanto, graças ao trabalho dedicado de criptógrafos civis e à comunidade do software livre e do código aberto, é possível ter privacidade na Internet. E o software necessário para isso está disponível, de forma livre para todos. Usá-lo é especialmente importante para jornalistas que se comunicam online com suas fontes.

Modelo de Ameaça

A NSA é um adversário poderoso. Se for escolhido pela agência como um alvo direto, você vai precisar se esforçar muito para se comunicar em privado. E mesmo pessoas que não são alvos diretos, bilhões usuários inocentes de Internet, são capturados pela rede de arrastão da NSA. A mudança de algumas práticas básicas nos softwares que você usa podem lhe proporcionar uma boa privacidade, ainda que não lhe garanta segurança contra ataques direcionados pelo governo dos Estados Unidos. Esse artigo explora métodos que você pode usar nos dois casos.

As ferramentas e recomendações nesse artigo são focadas na proteção de sua privacidade contra os métodos de coleta de dados da NSA, mas podem ser usadas para ampliar a sua segurança de computador contra qualquer adversário. É importante lembrar que outros governos, inclusive os da China e da Rússia, gastam quantias imensas de dinheiro com seus próprios equipamentos de alta tecnologia de vigilância e são especialmente conhecidos por visar jornalistas e suas fontes. Nos Estados Unidos, a má segurança digital pode custar a liberdade dos denunciantes, mas em outros países isso pode custar a vida do jornalista e das suas fontes. Um exemplo recente da Síria[2] mostra como o pouco cuidado com a segurança digital pode ter resultados trágicos.

Sistemas de Criptografia

Nós fizemos uma descoberta. Nossa única esperança contra o domínio total. Uma esperança que, com coragem, discernimento e solidariedade, poderíamos usar para resistir. Uma estranha propriedade do universo físico no qual vivemos.

O universo acredita na criptografia.

É mais fácil criptografar informações do que descriptografá-las.

- Julian Assange, na introdução de Cypherpunks: Liberdade e o Futuro da Internet

A criptografia é o processo de pegar uma mensagem em texto puro e uma chave gerada aleatoriamente e fazer operações matemáticas com as duas até que tudo que sobra é uma versão cifrada da mensagem embaralhada. Descriptografar é pegar o texto cifrado e a chave correta e fazer mais operações matemáticas até que o texto puro é recuperado. Esse processo é chamado criptografia, ou, resumidamente, cripto. Um algoritmo de criptografia, o que as operações matemáticas fazem e como eles fazem, é chamado de cifra.

Para criptografar alguma coisa você precisa da chave certa. E precisa da chave certa para descriptografar também. Se o software de criptografia for implementado corretamente, se a matemática for sólida, e se as chaves forem seguras, todo o poder computacional da Terra não pode quebrar essa criptografia.

Os sistemas de criptografia que nós construímos dependem de problemas da matemática que nós acreditamos ser difíceis, como a dificuldade de se fatorar números grandes. A menos que novas descobertas na matemática tornem esses problemas mais fáceis – e que a NSA mantenha isso em segredo do resto do mundo –, quebrar a criptografia, da qual a segurança depende, é inviável.

A concepção dos sistemas de criptografia e as cifras devem ser completamente públicas. A única forma de garantir que a própria cifra não possui uma falha crítica é publicar como ela funciona, para que muitos olhos a examinem detalhadamente. E deixar que ela enfrente os ataques no mundo real para poder corrigir seus erros. O funcionamento interno da maior parte da criptografia que usamos diariamente, como HTTPS[3], a tecnologia que torna possível digitar de forma segura os números de cartão de crédito e senhas em formulários de sites, é completamente público. Mesmo que um atacante saiba todos os detalhes como funciona a criptografia ainda assim falhará em quebrá-la se não possuir a chave. Uma criptografia proprietária, desenvolvida com código secreto, não pode ser confiável para ser segura.

Aqui temos uma questão importante para perguntar ao avaliar se um serviço ou um aplicativo que usa criptografia é seguro: “É possível que o próprio provedor de serviço possa burlar a criptografia?”, Se a resposta for sim, não se pode confiar na segurança daquele serviço. Muitos serviços como Skype[4] e Hushmail[5] prometem criptografia de “ponta a ponta”, mas muitas vezes isso significa que o próprio serviço possui a chave para decifrar a conversa. Em uma verdadeira criptografia ponta a ponta, o provedor do serviço não consegue, ainda que queira, espionar sua conversa.

Outro coisa importante a saber é que a criptografia é usada para muito mais coisas além de proteger a privacidade da comunicação. Ela pode ser usada para “assinar digitalmente” as mensagens a fim de comprovar que ela veio, realmente, da pessoa que você esperava. Também pode ser usada para criar moedas digitais como Bitcoin, e para criar redes anônimas como o Tor.

A criptografia pode ser utilizada para impedir as pessoas de instalar aplicativos nos seus próprios Iphone, que não venham da App Store; para impedir que gravem filmes diretamente do Netflix; para impedir de instalar Linux num tablet com o Windows 8. E também pode ser usada para impedir que ataques *man-in-the-middle* (MITM)[6] sejam usados para inserir um um malware em atualizações de software que, sem ele, seriam legítimas.

Resumindo, a criptografia abrange uma série de usos, mas este artigo se concentra em um aspecto: como podemos usá-la para nos comunicar com segurança e privacidade.

Software que você pode confiar

Quando Edward Snowden usa o termo “segurança na ponta final”, ele está se referindo à segurança dos computadores em cada ponta de uma conversa, garantida por chaves de criptografia e descriptografia. Não está falando da segurança das mensagens enquanto trafega pela rede. Se você enviar um e-mail criptografado para um amigo mas ele tiver um *keylogger* em seu computador, este programa gravará a mensagem inteira, assim como a senha que protege suas chaves de criptografia. E aí sua criptografia vale muito pouco.

Depois que os membros do conselho da Fundação de Liberdade de Imprensa Glenn Greenwald e Laura Poitras deram o furo jornalístico sobre a vigilância exercida pela rede de arrastão da NSA, muito mais informações sobre as agências de espionagem dos EUA tornaram-se públicas. Mais especificamente, a Bloomberg escreveu sobre um programa voluntário de compartilhamento de informação entre as empresas e as agências de espionagem dos EUA[7].

Até agora, a revelação mais chocante sobre esses programas de compartilhamento de informações é que a Microsoft adota uma política de entregar informações sobre as vulnerabilidades dos seus programas para o governo dos Estados Unidos antes de liberar as atualizações de segurança para o público. O artigo diz:

> *A Microsoft Corp. (MSFT), maior empresa de programas do mundo, fornece às agências de inteligência, informações sobre* bugs *nos seus populares programas antes do lançar as correções publicamente, segundo duas pessoas que conhecem este processo. Essa informação pode ser usada para proteger os computadores do governo e para acessar computadores de terroristas e inimigos milita*res

Isso significa que é provável que a NSA venha recebendo as chaves de qualquer computador rodando Windows, Office, Skype, ou outro software da Microsoft. Se vocêusar um desses softwares no seu computador, é possível que a NSA comprometa o seu computador, e assim as suas comunicações criptografadas, se você se tornar um alvo da agência.

Também soubemos pelo New York Times[8] que o Skype, software que tem, fora da comunidade de segurança, a reputação de ser uma forma segura de se comunicar, tem fornecido as conversas privadas dos seus usuários para o governo dos Estados Unidos nos últimos cinco anos.

> *Skype, o serviço de telefonia baseado na Internet, criou o seu próprio programa secreto, o Projeto Xadrez, para explorar as questões legais e técnicas para tornar as chamadas Skype rapidamente disponíveis para as agências de inteligência e as autoridades da lei. A informação é de pessoas que conhecem o programa e pediram para não ser nomeadas para evitar problemas com as agências de inteligência.*
>
> *O Projeto Xadrez, nunca havia sido revelado publicamente e um programa pequeno, limitado a um grupo menor que uma dúzia de pessoas no Skype e foi desenvolvido enquanto a empresa tinha diálogo, às vezes controverso, com o governo sobre as questões legais, disse uma das pessoas informada sobre o projeto. O projeto começou por volta de cinco anos atrás, antes da maior parte da empresa ser vendida pelo seu pai, eBay, a investidores externos em 2009. A Microsoft adquiriu o Skype num negocio de $8.5 bilhões, concluída em Outubro de 2011.*
>
> *Um executivo do Skype negou, no ano passado, num post no blog, que as recentes mudanças na operação de serviço foram feitas pela Microsoft para facilitar a bisbilhotagem dos agentes da lei. Parece, no entanto, que o Skype encontrou um jeito de cooperar com as agências de inteligência antes da Microsoft assumir a empresa, segundo os documentos vazados por Edward J. Snowden, ex-analista da N.S.A. Um dos documentos sobre o programa Prism, tornado publico pelo Sr. Snowden, diz que o Skype entrou no Prism em 6 de Fevereiro, 2011.*

O software proprietário, assim como muito do que é produzido pela Microsoft, Apple, e Google, têm um outro problema. É muito mais difícil para os usuários verificarem independentemente que *backdoors* secretos não existem por pedidos clandestinos da vigilância do Estado. Embora as matérias recentes demonstrem que muitas empresas entregaram uma quantidade desconhecida de informação em resposta a solicitações da FISA (Foreign Intelligence Surveillance Act), nenhuma revelou o uso direto de *backdoors* em seus sistemas.

Neste sentido, existe outro software que é mais confiável. O software livre e de código aberto[9] nem sempre é amigável para o usuário e nem sempre é seguro. No entanto, quando seu desenvolvimento é aberto, com controle de bug aberto, listas de e-mail abertas, estruturas de governança abertas, e o código fonte aberto, é muito mais difícil para esses projetos ter uma política de traição a seus usuários -- como a Microsoft tem.

O GNU/Linux é um sistema operacional composto inteiramente de software livre e de código aberto. Exemplos de distribuições GNU/Linux incluem o Ubuntu[10], Debian [11], e o Fedora Core[12]. São as alternativas mais populares de software livre ao Windows e Mac OS X.

Mesmo que seja possível inserir linhas de código mal intencionadas em projetos de software livre (veja o Concurso Underhanded C[13]), a pessoa que está escrevendo o código precisa escondê-las de forma hábil e torcer para que nenhum dos outros desenvolvedores, ou mantenedores do pacote GNU/Linux que preparam e compilam o código fonte dos projetos para incluir na sua distribuição, percebam.

Nos anos 1990, quando a criptografia civil estava começando a se popularizar e o governo dos Estados Unidos estava fazendo de tudo para impedir[14], o movimento "cypherpunk" nasceu. Muitos trechos de software escritos para aproximar a criptografia das pessoas cresceram a partir desse movimento.

> *Cypherpunks escrevem código. Nós sabemos que alguém tem que escrever software para defender a privacidade, e uma vez que nossa privacidade não pode ser garantida a não ser que todos a tenham também, nós vamos escrevê-lo. Nós publicamos o código para que nossos companheiros Cypherpunks o usem e se divirtam com ele. Nosso código é livre para todos usarem, no mundo inteiro. Não nos importamos se você não aprovar o software que escrevemos. Nós sabemos que um software não pode ser destruído e que um sistema amplamente distribuído não pode ser desmantelado.*
>
> – Eric Hughes, em seu Manifesto Cypherpunk, 1993

Esse código, que é aberto e público para que os companheiros cypherpunks pratiquem e se divirtam e que pode ser usado por qualquer pessoa no mundo, forma a base de software e de protocolos na qual podemos confiar: TLS (a criptografia que sustenta o HTTPS), LUKS (criptografia de disco[15] incorporada no GNU/Linux), OpenGPG, Off-the-Record, e Tor.

O Coletivo Tecnologia Tática[16] elaborou um ótimo guia de softwares seguros de código aberto nos quais você pode confiar[17] para manter suas comunicações a salvo da vigilância. É importante lembrar que apenas usando esse software, e mesmo usando-o perfeitamente, não se pode garantir a segurança da sua criptografia. Um exemplo: nós não tínhamos ideia se a Apple cedeu vulnerabilidades de zero dia do iOS para a NSA da mesma forma como a Microsoft fez, segundo reportagens. O ChatSecure, que permite você ter conversas criptografadas nos dispositivos iOS, é tão seguro quanto o sistema operacional no qual está sendo executado.

É importante para lembrar que apenas usar software livre não garante que você não seja hackeado. Pessoas encontram vulnerabilidades de zero dias [18] em softwares livres o tempo todo, e algumas vezes vendem para os governos e outros atacantes maliciosos. Os usuários de software livre ainda baixam anexos maliciosos em seus e-mails e frequentemente possuem serviços mal configurados e facilmente exploráveis em seus computadores. E pior ainda, os malwares geralmente são muito competentes em se esconder. Se um usuário de software livre pegar um malware em seu computador, ele pode ficar ali até o usuário formate seu disco rígido.

O Tails, uma distribuição GNU/Linux em live DVD e live USB que discutirei em detalhes mais abaixo, soluciona muitos desses problemas.

Anonimize sua localização com Tor

O Tor[19] é um serviço de software que permite você usar a Internet e ocultar o seu endereço IP, o que é, em geral, uma indica;'ao muito precisa da sua localização. A rede Tor é formada por mais de 3,600 servidores voluntários, chamados nós. Quando alguém usa a rede Tor para visitar um site, sua conexão é transmitida por três desses nós (um circuito) antes de finalmente sair na Internet normal. Alguém interceptando o seu tráfego pensará que sua localização é o nó final por onde o seu tráfego saiu.

É importante lembrar que somente o fato de sua conexão com a Internet ser anônima, isso não a transforma, de forma mágica, em segura. A EFF fez um grande sistema de visualização[20] de como o Tor e o HTTPS podem trabalhar juntos para proteger sua privacidade.

Como todo bom software de criptografia, o Tor é software livre, com um sistema aberto de monitoramento de bugs, lista de e-mail, e código fonte[21].

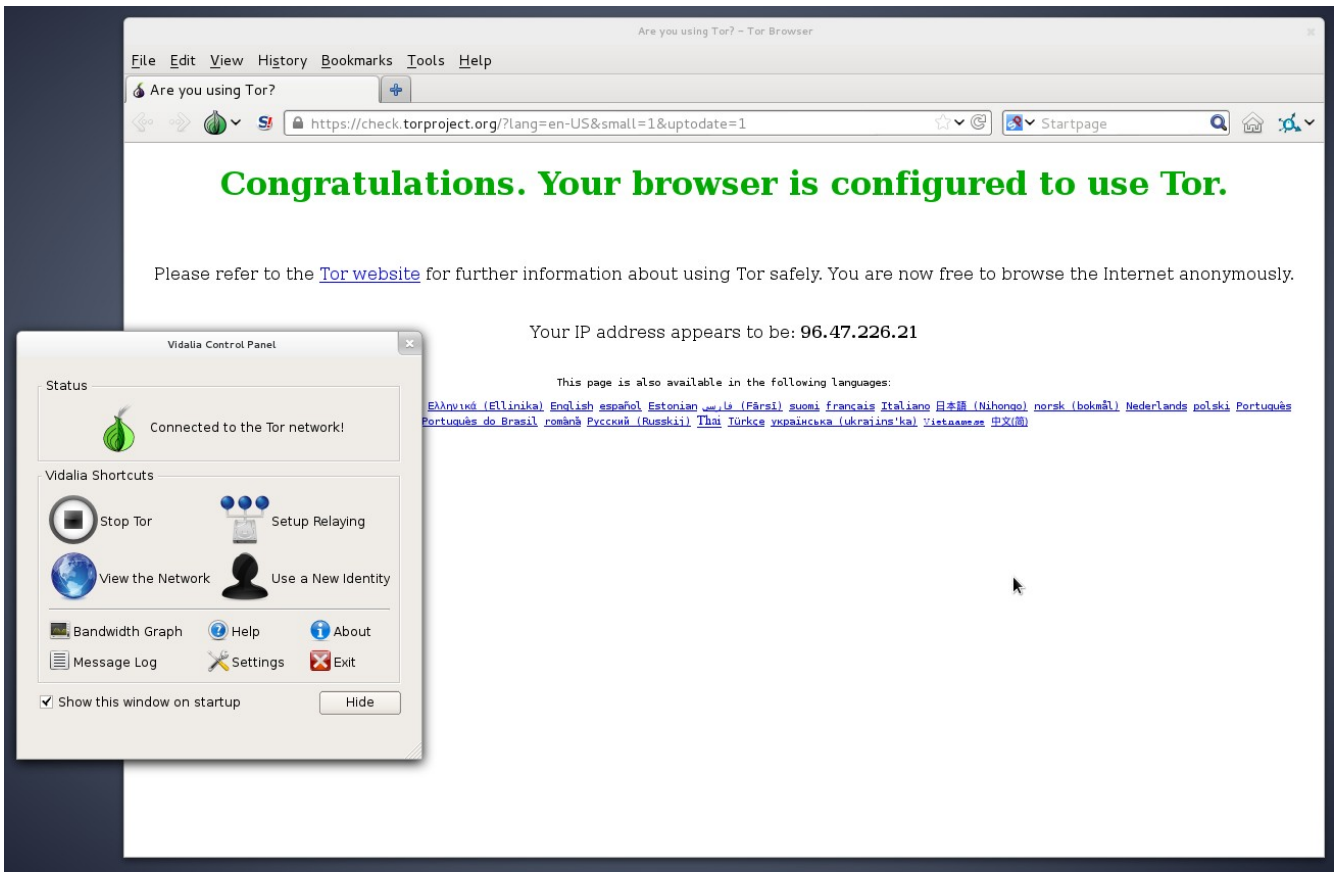
A documentação do Tails, a distribuição GNU/Linux que força todo o tráfego de rede do usuário através da rede Tor, diz o seguinte sobre os adversários globais[22]:

> Um adversário global passivo poderia ser uma pessoa ou uma entidade capaz de monitorar ao mesmo tempo o tráfego entre todos os computadores numa rede. Estudando, por exemplo, o tempo e os padrões de volume de diferentes comunicações através da rede, seria estatisticamente possível identificar os circuitos do Tor e desse modo corresponder os usuários do Tor com os servidores de destino.

Nós ainda não sabemos se a NSA ou a GCHQ contam como um adversário global, mas sabemos que eles monitoram uma grande parte da Internet. É ainda muito cedo, ainda, para saber com certeza com qual facilidade as agências de inteligência podem derrotar o anonimato da rede Tor.

Mesmo se eles poderem, usando Tor ainda nós dá muitas vantagens. Torna o trabalho deles muito mais difícil, e deixamos muitos menos traços identificadores nos servidores que conectamos através da rede Tor. Isso torna muito difícil para ser uma vítima de um ataque MITM na nossa rede local ou no nível do provedor de Internet. E mesmo que alguns circuitos do Tor sejam derrotados por um adversário global, se houver pessoas suficientes com o tráfego roteado pelos mesmos nós do Tor simultaneamente, pode ser difícil para o adversário dizer qual tráfego pertence a qual circuito.

O jeito mais fácil de começar a usar o Tor é baixando e instalando o Tor Browser Bundle[23].



Quando Snowden estava respondendo perguntas no site do Guardian[24] de uma “conexão de Internet segura”, ele estava provavelmente roteando seu tráfego através de uma rede Tor. Ele pode ter também utilizado uma conexão ponte[25] para conectar na rede Tor para tornar o fato de que estava usando Tor através do seu endereço IP menos óbvio para um intruso.

Off-the-Record (OTR) Chat

O Off-the-Record[26] (OTR) é uma camada de criptografia que pode ser adicionada a qualquer sistema existente de mensagem instantânea (bate-papo), desde que você se conecte no sistema de bate-papo usando um cliente de conversa que suporte OTR, como o Pidgin ou o Adium[27]. Com o OTR é possível ter conversas seguras criptografadas ponta-a-ponta sobre serviços como Google Talk e Facebook Chat sem que o Google ou o Facebook tenham acesso aos conteúdos das conversas. Nota: isso é diferente da opção “off-the-record” no Google, a qual não é segura. E lembre-se: enquanto a conexão HTTPS do Google e do Facebook são muito valiosas para proteção da mensagem em trânsito, eles ainda possuem as chaves das suas conversas e podem entregá-las para as autoridades.

O OTR é usado para duas coisas: para criptografar o conteúdo em conversas de mensagem instantânea em tempo real e para verificar a identidade da pessoa com quem você está falando. A verificação da identidade é extremamente importante e é algo que

muitos usuários do OTR negligenciam. Ainda que o OTR é muito mais amigável do que outras formas de criptografia de chave pública, se quiser usá-lo seguramente você precisa entender como funciona e quais são os ataques possíveis.

Provedores de Serviço e Jabber

Usar OTR criptografa apenas o conteúdo das suas conversas de batepapo, mas não o metadado relacionado a elas. Esse metadado inclui informações com quem você falou, quando e quantas vezes você falou. Por essa razão, eu recomendo utilizar um serviço que não é de conhecimento público que colabore com as agências de inteligência. Embora isso não vá necessariamente proteger seus metadados, pelo menos você terá uma chance de mantê-los em privado.

Eu também recomendo você usar um serviço de XMPP (também conhecido como Jabber). Assim como o e-mail, Jabber é um protocolo aberto e federado. Usuários do serviço do Jabber do Riseup.net podem conversar com outros usuários do serviço jabber.ccc.de assim como os do serviço jabber.org.

Clientes OTR

Para usar OTR você precisará baixar o software. Se usar Windows, baixe e instale o Pidgin e o plugin OTR separadamente[29]. Se usar GNU/Linux instale os pacotes pidgin e pidgin-otr. Você pode ler, na documentação, como configurar suas contas no pidgin com OTR. Se usar Mac OS X, você pode baixar e instalar o Adium, um cliente de bate-papo em software livre que inclui suporte para OTR. Leia na documentação oficial como configurar a criptografia OTR com o Adium[31].

Há também clientes Jabber e OTR disponíveis para Android, chamados Gibberbot[32], e para iOS, chamado ChatSecure[33].

Seus Chaveiros

Quando você começar a usar o OTR, seu cliente de bate-papo vai gerar uma chave criptográfica e armazená-la num arquivo na pasta pessoal do seu usuário no disco rígido. Se seu computador ou smartphone for perdido, roubado ou infectado por algum malware, é possível que a sua chave OTR seja comprometida. Caso isso aconteça, é possível que um invasor com controle sobre seu servidor Jabber monte um ataque MITM no momento que você estiver conversando com pessoas que você anteriormente verificaram sua identidade.

Sessões

Se você quer usar OTR para falar privadamente com seus amigos, seus amigos também precisam usá-lo. Uma sessão criptografada entre duas pessoas requer duas chaves de criptografia. Por exemplo, se você e seu amigo ambos estiverem logados no bate-papo do Facebook usando Adium ou Pidgin e vocês dois tiverem configurado OTR, vocês podem falar num batepapo privado. No entanto, se você estiver logado no mensageiro instantâneo usando Adium ou Pidgin mas seu amigo estiver conversando diretamente do facebook pelo navegador web, você não consegue criptografar a conversa.

Se você quiser usar os serviços do Facebook ou do Google para conversar com seus amigos, eu recomendo desabilitar o bate-papo da interface web desses serviços e apenas usar o Adium ou o Pidgin para conectar. E encorajar todos seus amigos a fazer a mesma coisa[34].

Quando você começar as sessões criptografadas OTR, seu programa cliente lhe dirá algo parecido com isso:

```
Attempting to start a private conversation with username@jabberservice...
Unverified conversation with username@jabberservice/ChatClient started.
```

Se você já tiver verificado a impressão digital OTR da pessoa com quem estiver falando (mais detalhes abaixo), sua sessão aparecerá assim:

```
Attempting to start a private conversation with username@jabberservice...
Private conversation with username@jabberservice/ChatClient started.
```

Quando você começa uma nova sessão OTR, seu programa OTR e o programa OTR do seu amigo trocam uma séries de mensagens para negociarem uma nova chave de sessão. Essa chave temporária de criptografia, que é apenas conhecida por seu cliente de mensagem instantânea e nunca é enviada pela Internet, é então usada para criptografar e descriptografar as mensagens. Quando a sessão é finalizada ambos clientes esquecem a chave. Se você estiver conversando com a mesma pessoa mais tarde, seus clientes gerarão uma nova chave de sessão.

Desta maneira, mesmo se um atacante estiver grampeando toda sua conversa criptografada com OTR – o que a NSA acredita que é legalmente permitido fazer [35], mesmo se você é um cidadão dos Estados Unidos e eles não possuem mandado ou uma causa provável – e depois comprometer sua chave OTR, ele não pode usá-la para voltar atrás e descriptografar as mensagens das conversas antigas.

Essa propriedade é chamada de *forwared secrecy* (sigilo antecipado), e é uma característica do OTR que o PGP não possui. Se sua chave secreta PGP (mais sobre isso abaixo) for comprometida, e o atacante tiver acesso a todo o conteúdo criptografado das mensagens que você recebeu, eles podem voltar atrás e descriptografar todas elas. Leia mais sobre como funciona a *forward secrecy,* e porque todas as companhias de Internet deveria adotá-la para seus sites[36]. A boa notícia é que o Google já adotou o *forward secrecy,* e Facebook implementará muito em breve[37].

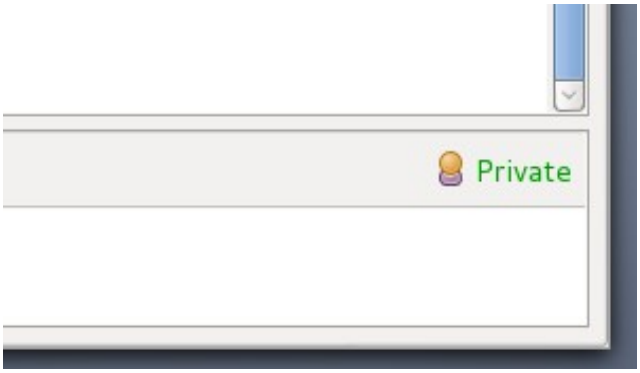
Verificação da impressão digital OTR

Quando você inicia uma nova sessão OTR com alguém, seu software de mensagem instantânea recebe a impressão digital da sua chave de criptografia, e o seu programa OTR grava essa impressão digital. Enquanto alguém usar a mesma chave de criptografia enquanto conversa com você, presumivelmente porque ela está usando provavelmente o mesmo dispositivo, terá a mesma impressão digital. Se a impressão digital mudar, então ou ela está usando uma chave OTR diferente ou você dois são alvos de um ataque MITM.

Sem verificar as chaves você não tem como saber se você está sendo uma vítima de um não detectável e bem sucedido ataque MITM.

Mesmo se a pessoa que você está falando é definitivamente seu amigo real porque ela sabe coisas que apenas ela poderia saber, e você está usando a criptografia OTR, é possível, para um atacante ler sua conversa. Isso porque você talvez tenha uma conversa criptografada com OTR com o atacante, o qual por sua vez está tendo uma conversa criptografada com OTR com seu amigo real e apenas encaminhando suas mensagens de um para o outro. Antes da impressão digital do seu amigo, o seu cliente estaria vendo a impressão digital do atacante. Tudo o que você, como usuário, pode ver é que a conversa é “Não-verificada”.

As próximas capturas de telas mostram as indicações visuais do Pidgin sobre a verificação da impressão digital. Se você tiver verificado sua impressão digital OTR, sua conversa é privada. Se você não tiver, sua conversa é criptografada, mas você pode estar sob ataque. Você não pode ter certeza, a não ser que verifique.



Se você clicar no link “Não-verificado” (no Adium é um ícone de cadeado), você pode escolher “Autenticar amigo”. O protocolo OTR suporta três tipos de verificação: o protocolo socialista milionário [38], um segredo compartilhado[39], e a verificação manual de impressão digital. Todos os clientes de OTR suportam a verificação manual de impressão digital, mas nem todos os clientes suportam outros tipos de verificação. Quando em dúvida, escolha o processo de verificação manual de impressão digital.

Na captura de tela acima, você pode ver as impressões digitais OTR de ambos usuários na sessão. A outra pessoa deve ver as mesmas e exatas impressões digitais. Para ter certeza de que ambas as partes estão vendo corretamente as impressões digitais, vocês dois precisam se encontrar em pessoa, ou falar pelo telefone se você puder reconhecer sua voz, ou encontrar alguma outro método seguro, fora da conversa, para verificar as impressões digitais, como enviar através de um e-mail assinado e criptografado com PGP.

As impressões digitais OTR são 40 caracteres hexadecimal. É estatisticamente impossível gerar duas chave OTR que possuem a mesma impressão digital -- o que chamamos de colisão. Porém, é possível gerar uma chave OTR que não é uma colisão, mas parece uma quando se faz uma inspeção rápida. Por exemplo, os primeiros caracteres e os últimos caracteres podem ser os mesmos com diferentes caracteres no meio. Por essa razão, é importante comparar cada um dos 40 caracteres para ter certeza que você tem a chave OTR correta.

Como você geralmente configura uma nova chave OTR a cada vez que você configura um novo dispositivo (por exemplo, se quiser usar a mesma conta Jabber para conversar do seu celular Android com Gibberbot enquanto você usa seu PC Windows com Pidgin), frequentemente termina com múltiplas chaves, e portanto múltiplas impressões digitais. É importante repetir o passo do processo de verificação em cada dispositivo e com cada

contato com quem você fala.

É uma melhor prática usar o OTR sem verificação de impressão digital do que não usar OTR. Um atacante que tenta um ataque MITM contra uma sessão OTR corre um alto risco de ser pego, então provavelmente essa forma de ataque será usada com muita cautela.

Logs

Aqui há um trecho dos logs de bate-papo, publicados pela Wired[40], da conversa entre Bradley Manning e Adrian Lamo, que o entregou às autoridades:

> *(1:40:51 PM) bradass87 has not been authenticated yet. You should authenticate this buddy.*
>
> *(1:40:51 PM) Unverified conversation with bradass87 started.*
>
> *(1:41:12 PM) bradass87: oi*
>
> *(1:44:04 PM) bradass87: como vai?*
>
> *(1:47:01 PM) bradass87: eu sou um analista da inteligência do exército, enviado para o leste de Bagdad, aguardando dispensa por um "transtorno de adaptação" em vez de "transtorno de identidade de gênero"*
>
> *(1:56:24 PM) bradass87: eu tenho certeza que você está muito ocupado...*
>
> *(1:58:31 PM) bradass87: se você tivesse um acesso sem precedentes a redes secretas 14 horas por dia, 7 dias por semana, durante + 8 meses +, o que você faria?*
>
> *(1:58:31 PM) info@adrianlamo.com : Cansado de estar cansado*
>
> *(2:17:29 PM) bradass87: ?*
>
> *(6:07:29 PM) info@adrianlamo.com: Qual é a sua Especialidade Ocupacional Militar?*

Como você pode ver em "Unverified conversation with bradass87 started,", eles estavam usando OTR para criptografar a conversa. Mesmo assim, o diálogo terminou sendo publicado no site da Wired e usado como evidência contra Bradley Manning. Ainda que seja possível que a conversa deles estivesse sob um ataque MITM, mas isso é muito improvável. Mas tanto o cliente OTR de Bradley Manning como o de Adrian Lamo estavam gravando uma cópia das conversas em seus discos rígidos, não criptografados.

Algumas vezes pode ser útil manter os registros das conversas, mass isso pode comprometer muito sua privacidade. Se o Pidgin e o Adium não gravassem as conversas OTR por padrão, é possível que esses registros de conversas nunca tivessem virado parte de um registro público.

Com o lançamento do OTR 4.0 em Setembro de 2012, o Pidgin parou de gravar as conversas com OTR por padrão. O Adium ainda grava as conversas com OTR por padrão, então você mesmo deve manualmente desabilitar a gravação, que é um bug no Adium[41].

Criptografia de Email: “Pretty Good Privacy” (PGP)

Em 1991, Phil Zimmermann desenvolveu um software de criptografia de e-mail chamado Pretty Good Privacy [42], ou PGP. Ele concebeu o software para ser usado ativistas pela paz na organização do movimento anti-nuclear.

Hoje, o PGP é uma empresa que vende programa proprietário de criptografia com o mesmo nome. OpenPGP[43] é o protocolo aberto que define como a criptografia PGP funciona, e GnuPG[44] (GPG, abreviado) é um software livre, 100% compatível com a versão proprietária. O GPG é muito mais popular que o PGP porque é livre para todo mundo baixar, e os cypherpunks confiam mais nele porque é código aberto. Os termos PGP e GPG são usados frequentemente como sinônimos.

Infelizmente, o PGP é conhecido por sua dificuldade de usar. Um exemplo disso é Greenwald explicando como foi difícil ele iniciar uma conversa inicialmente com Edward Snowden porque era muito difícil de configurar[46].

Par de Chaves e Chaveiros

Assim como no OTR, cada pessoa que deseje enviar ou receber um e-mail criptografado necessita gerar sua própria chave PGP, chamada de par de chaves. O par de chaves PGP é dividido em duas partes, uma chave pública e uma chave secreta.

Se você têm a chave pública de alguém, você pode fazer duas coisas: **criptografar mensagens** que só podem ser descriptografadas com sua chave secreta, e pode **verificar assinaturas** que são geradas com sua chave secreta. É seguro dar sua chave pública para qualquer pessoa que quiser. A pior coisa que alguém pode fazer é criptografar mensagens que só você pode descriptografar.

Com sua chave secreta você pode fazer duas coisas: **descriptografar mensagens** que são criptografadas usando sua chave pública, e **assinar digitalmente mensagens**. É importante manter sua chave secreta segura. Com ela, um atacante pode descriptografar as mensagens destinadas somente a você e pode forjar mensagens em seu nome. Chaves privadas são geralmente criptografadas com uma frase secreta. Então, mesmo que seu computador for comprometido e sua chave for roubada, o atacante ainda precisaria descobrir sua chave secreta antes para conseguir acessar sua chave. Diferente do OTR, o PGP não possui *forward secrecy* (sigilo antecipado). Se sua chave secreta PGP for comprometida e o atacante possuir cópias de qualquer e-mail criptografado que você recebeu, ele descriptografar retroativamente todos as mensagens.

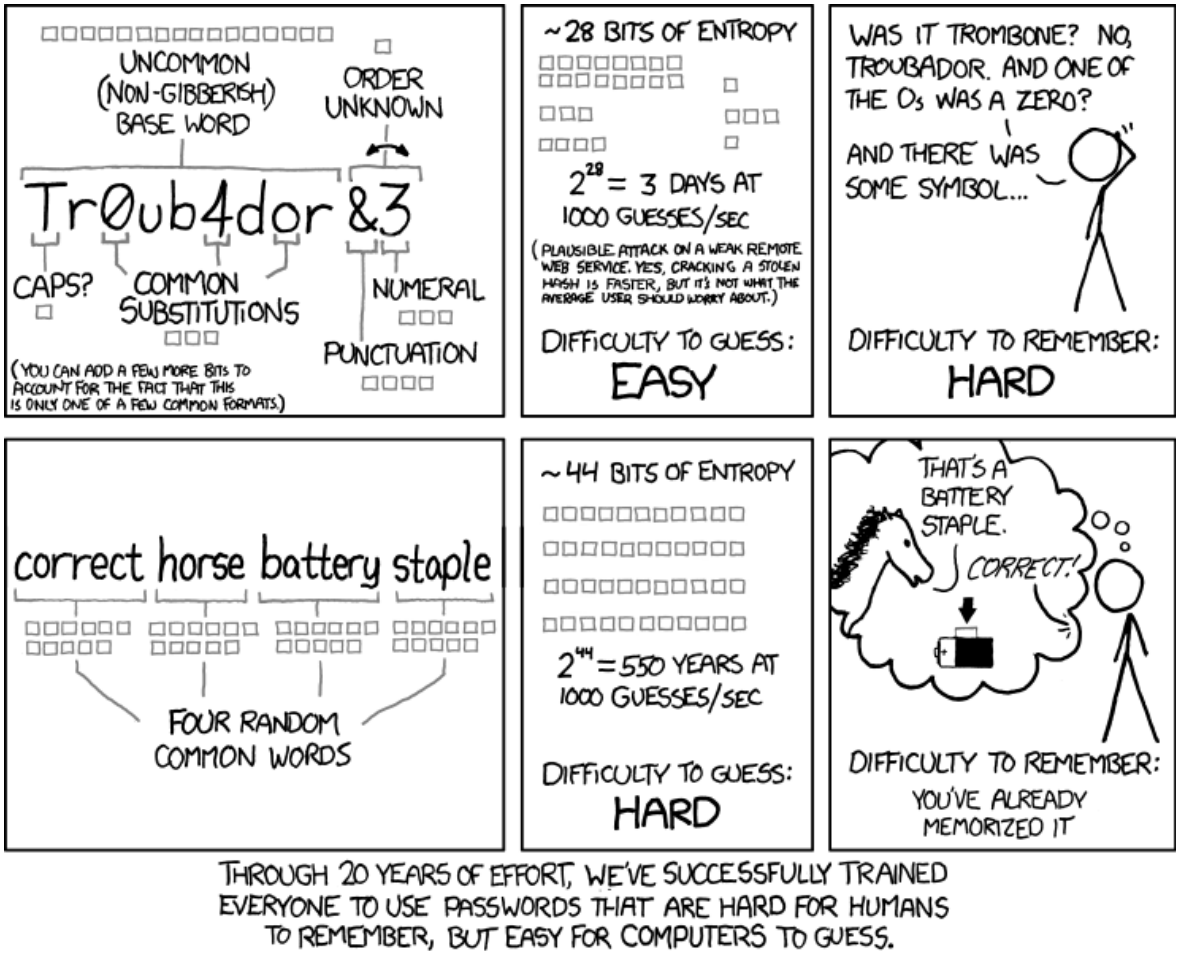
Como você precisa da chave pública de outras pessoas para criptografar suas mensagens para eles, o software PGP permite que você gerencie um chaveiro com sua chave secreta, sua chave pública, e todas as chaves públicas das pessoas com quem você se comunica.

Usar o PGP para criptografia de e-mail pode ser muito inconveniente. Por exemplo, se você configurar o PGP no seu computador mas tiver recebido um e-mail criptografado no celular, você não será capaz de descriptografá-lo para ler até acessar do seu computador.

Assim como o OTR, cada chave PGP tem uma única impressão digital. Você pode encontrar uma cópia da minha chave pública no site da Fundação da Liberdade de Imprensa[46], e minha impressão digital é 5C17 6163 61BD 9F92 422A C08B B4D2 5A1E 9999 9697. Se você olhar para minha chave pública você vai ver que ela é bastante longa e que seria difícil de ler por telefone. Uma impressão digital é um meio curto e mais conveniente para representar de forma única uma chave. Com minha chave pública você pode criptografar mensagens que só eu poderei descriptografar, desde que a minha chave secreta não esteja comprometida.

Frase secreta

A segurança da criptografia muitas vezes depende da segurança de uma senha. Uma vez que as senhas são facilmente descobertas por computadores, criptógrafos preferem o termo frase secreta[47] para encorajar os usuários para fazer suas senhas muito longas e seguras.



Cortesia do XKCD, https://xkcd.com/936/

Para dicas de como escolher boas frases secretas, leia a seção “Frase Secreta” do guia “Defendendo a Privacidade” da Electronic Front Foundation (EFF) no documento oficial “U.S. Border: Um Guia para Viajantes Carregando Dispositivos Digitais”[48], e também Diceware Passphrase Home Page[49].

Além disso, para proteger sua chave secreta PGP, você também precisa escolher boas frases secretas para o seu disco rígido criptografado e para o gerenciador de senhas[50].

Software

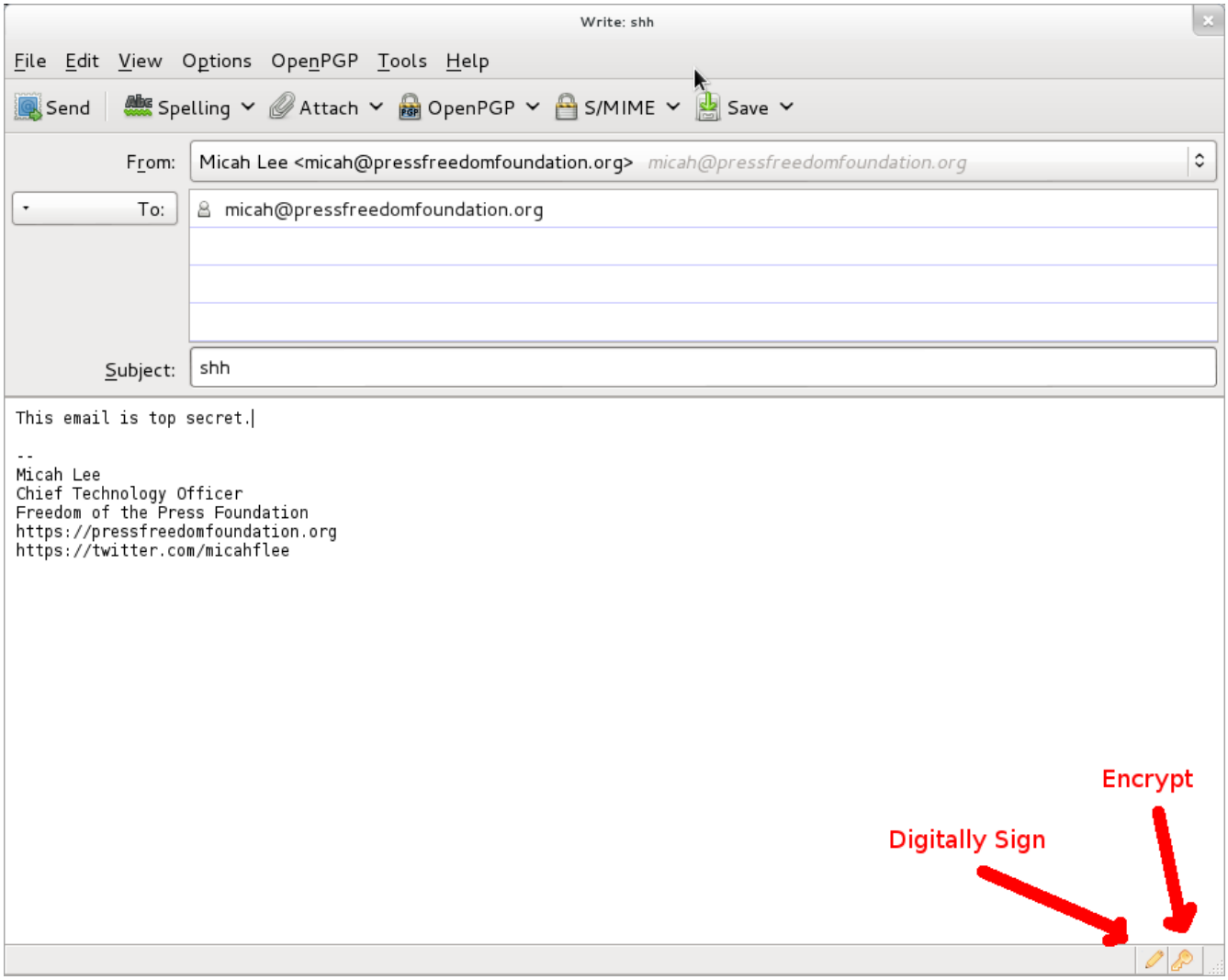
Para instalar o GPG, os usuários do Windows pode baixar o Gpg4win[51] e usuários do Mac OS X pode baixar o GPGTools[52]. Se você roda GNU/Linux já deve ter o GPG instalado. O GPG é um programa de linha de comando, mas há softwares com interfaces com os clientes de e-mail que facilitam o seu uso.

Você deverá fazer o download de um cliente de e-mail para usar o PGP corretamente. Um cliente de e-mail é um programa em seu computador que você abre para checar os e-mails, ao invés de usar o seu navegador de Internet. A instalação mais popular do PGP é o cliente de e-mail Thunderbird com o complemento Enigmail[53]. Thunderbird e Enigmail são softwares livres e rodam no Windows, Mac e GNU/Linux.

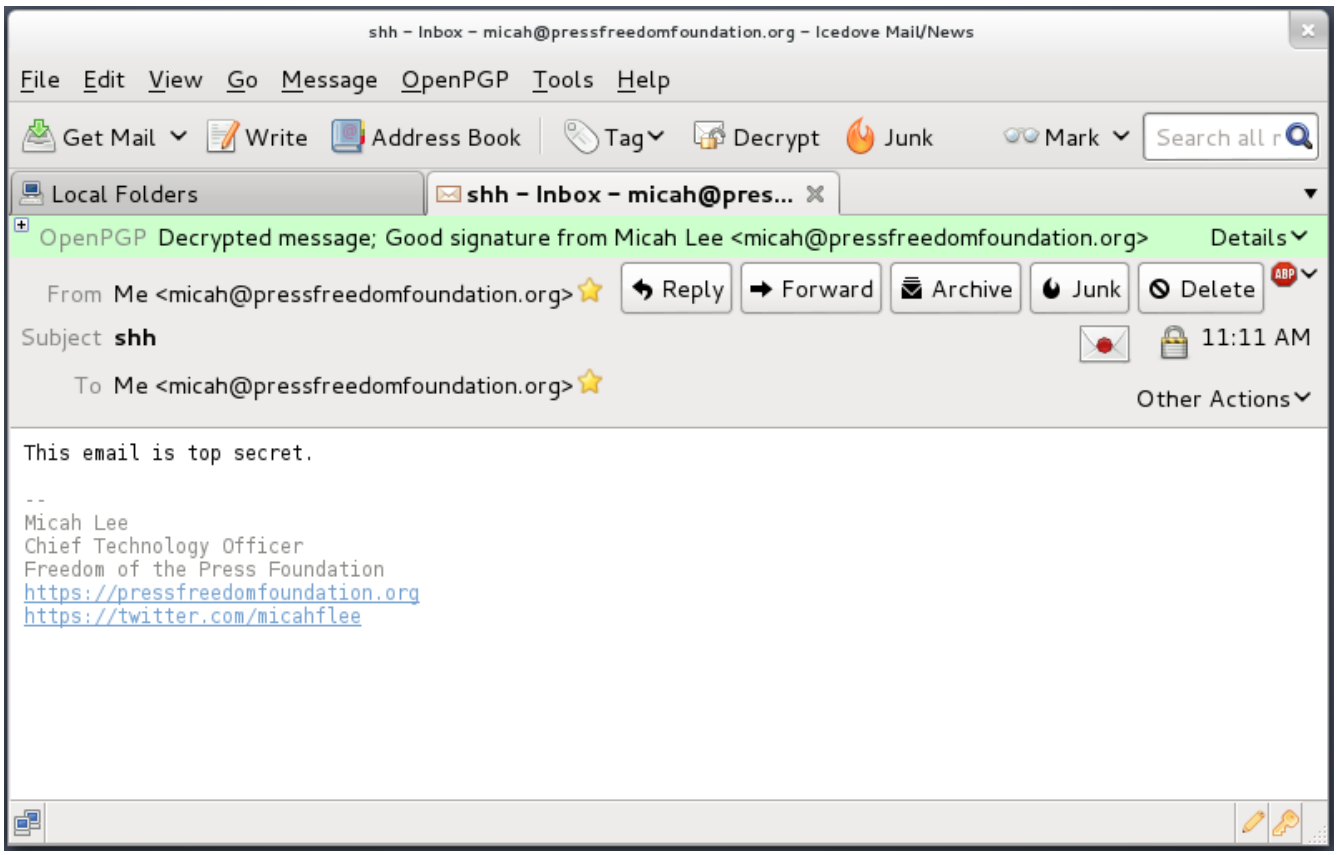
Ainda é muito difícil usar o PGP com segurança através do navegador de Internet. Existem algumas extensões do navegador para ajudar nisso, mas eu recomendo usar o cliente de e-mail para desktop até que a criptografia nos navegadores amadureça. É possível usar a criptografia do PGP com o Gmail, mas o jeito mais fácil é configurar um cliente de e-mail como o Thunderbird e rodar sua conta do Gmail através dele.

Criptografar, Descriptografar, e Assinaturas

Você pode mandar e-mails criptografados e assiná-los digitalmente usando uma interface gráfica disponibilizada pelo Thuderbird ou pelo Enigmail. Aqui está um exemplo de um e-mail criptografado que vou mandar para mim mesmo. Quando eu clicar em enviar, meu software pegará o corpo da mensagem e criptografará com a minha chave pública, tornando o conteúdo ininteligível para intrusos, e, certamente, também para o meu provedor de e-mail.



Quando abri esse e-mail fui solicitado a digitar minha frase secreta da criptografia para poder descriptografá-lo. Como criptografei usando a minha chave pública, a única forma de descriptografar é com a minha chave secreta. Minha chave secreta é protegida com uma frase secreta, então precisei digitar minha frase secreta para temporariamente descriptografar minha chave secreta e poder usá-la para descriptografar a mensagem.



PGP não é apenas para e-mail

O PGP é frequentemente usado para criptografia de e-mail, mas nada impede você de utilizá-lo para criptografar qualquer coisa e publicá-la em qualquer meio. Você pode postar uma mensagem criptografada com PGP em blogs, redes sociais e em fóruns.

Kevin Poulsen publicou uma mensagem criptografada com PGP no site da Wired[54] querendo que Edward Snowden lesse. A Wired possui uma cópia da chave pública real de Edward Snowden. Assim, apenas alguém com a posse da chave secreta de Snowden pode descriptografar essa mensagem. Nós não sabemos como a Wired conseguiu uma cópia da chave pública de Snowden.

Aqui está a mensagem que foi criptografada com a minha chave pública. Sem ter acesso para a minha chave secreta associada, a NSA não deveria ser capaz de quebrar a criptografia. (NSA, por favor me avise se entendeu essa).

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.12 (GNU/Linux)

hQIMA86M3VXog5+ZAQ//Wep9ZiiCMSmLk/Pt54d2wQk07fjxI4c1rw+jfkKQAi4n
6HzrX9YIbgTukuv/0Bjl+yp3qcm22n6B/mk+P/3Cbxo+bW3gsq5OLFNenQO3RMNM
i9RC+qJ82sgPXX6i9V/KszNxAyfegbMseoW9FcFwViD14giBQwA7NDw3ICm89PTj
y+YBMA50iRqdErmACz0fHfA/Ed5yu5cOVVa8DD12/upTzx7i0mmkAxwsKiktEaKQ
vg8i1gvzqeymWYnckGony08eCCIZFc78CeuhODy0+MXyrnBRP9p++fcQE7/GspKo
SbxVT3evwT2UkebezQT2+AL57NEnRsJzsgQM4R0sMgvZI7I6kfWKerhFMt3imSt1
QGphXmKZPRvKqib59U57GsZU1/2CMIlYBVMTZIpYKRh6NgE8ityaa4gehJDl16xa
```

```
pZ8z3DMNt3CRF8hqWmJNUfDwUvXBEk8d/8Lkh39/IFHbWqNJh6cgq3+CipXH5HjL
iVh7tzGPfB6yn+RETzcZjesZHtz4hFudOxTMV0YnTIv0FGtfxsfEQe7ZVmmfqGNG
glxE0EfbXt0psLXngFMneZYBJqXGFsK3r5bHjRm6wpC9EDAzXp+Tb+jQgs8t5eWV
xiQdBpNZnjnGiIOASOxJrIRuzbTjo389683NfLvPRY8eX1iEw58ebjLvDhvDZ2jS
pwGuWuJ/8QNZou1RfU5QL0M0SEe3ACm4wP5zfUGnW8o1vKY9rK5/9evIiA/DMAJ+
gF20Y6WzGg4llG9qCAnBkc3GgC7K1zkXU5N1VD50Y0qLoNsKy6eengXvmiL5EkFK
RnLtP45kD2rn6iZq3/Pnj1IfPonsdaNttb+2fhpFWa/r1sUyYadWeHs72vH83MgB
I6h3Ae9ilF5tYLs2m6u8rKFM8zZhixSh
=a8FR
-----END PGP MESSAGE-----
```

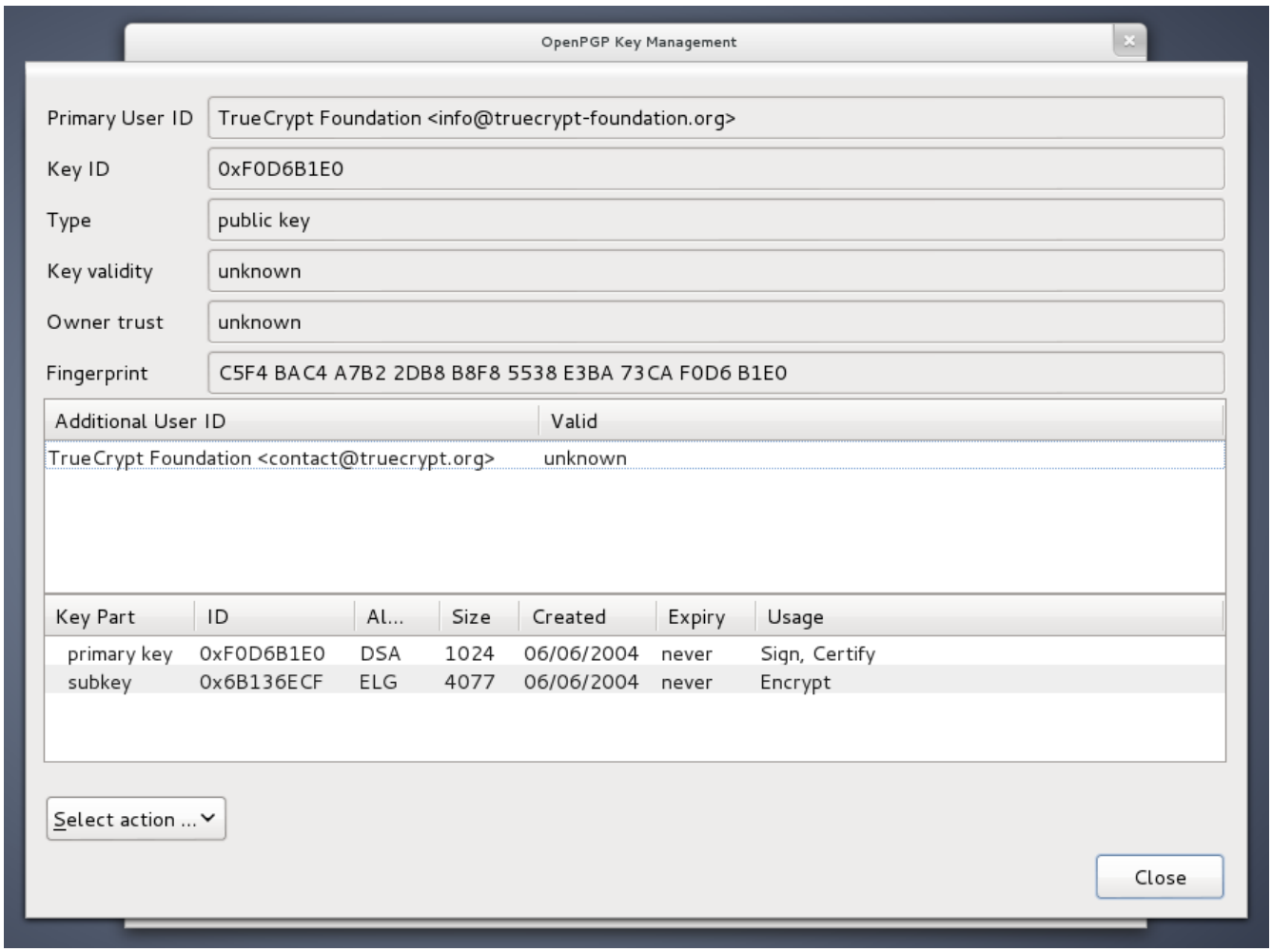
Verificação de identidade

Assim como o OTR, é importante que você verifique a chave PGP das pessoas com quem você se comunica. No PGP você faz isso usando sua chave secreta para assinar digitalmente a chave pública de alguma outra pessoa.

No Thunderbird você pode clicar no menu OpenPGP e abrir o Gerenciamneto de Chave. Você pode checar a caixa “Mostrar todas as chaves por padrão” para ver todas as chaves no seu chaveiro. A partir daí você pode importar chaves de arquivos, da sua área de transferência ou de outros servidores de chaves. Você também pode gerar novos pares de chaves e ver os detalhes de todas as chaves no seu chaveiro.

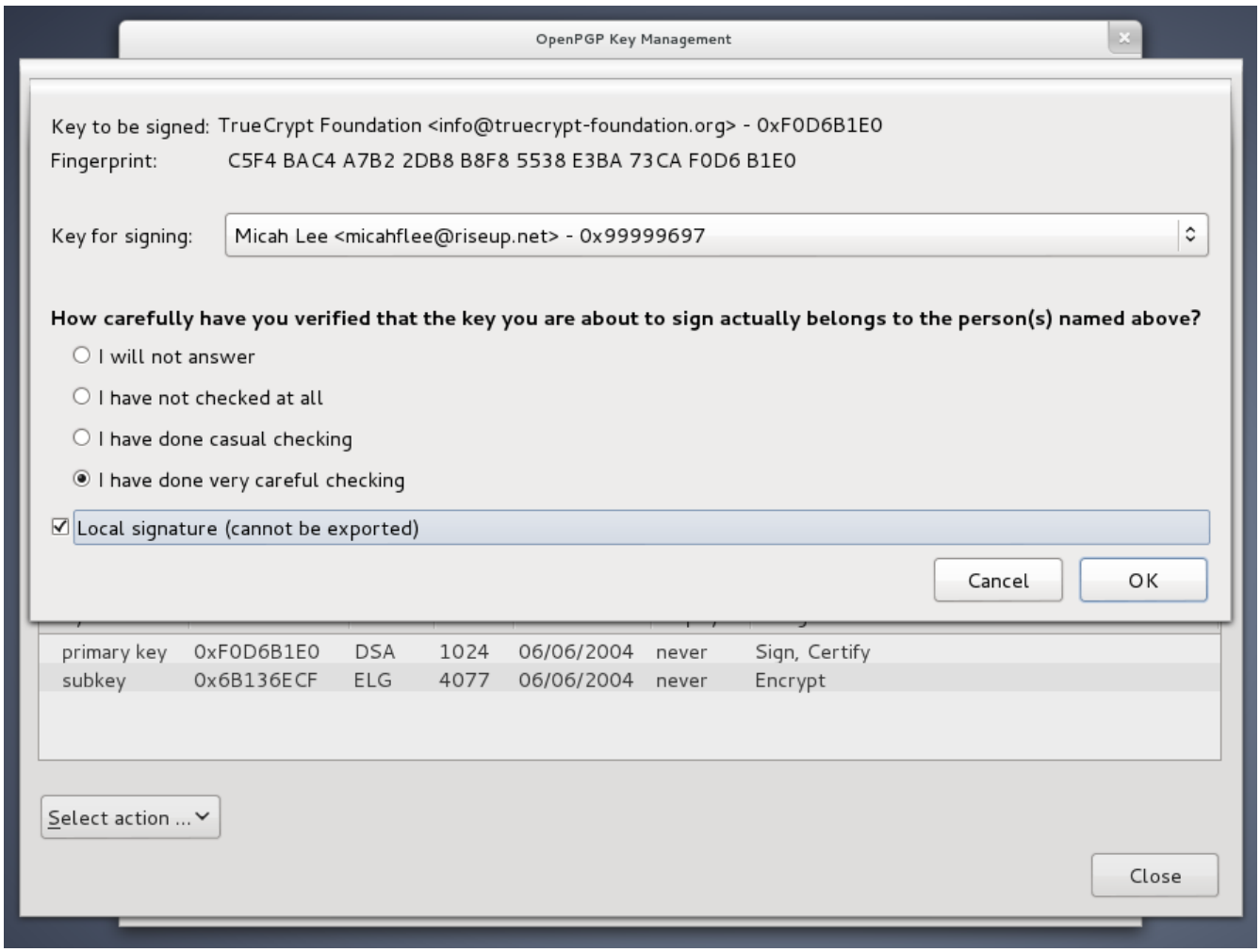
Assim como as chaves OTR, cada chave PGP tem uma única impressão digital. E assim como o OTR, você precisa ler toda a impressão digital para ter certeza que a chave pública que você está olhando realmente pertence a pessoa que você acredita que pertence.

Você pode dar um clique com o botão direito na chave na lista e escolher “Ver Detalhes” para ver sua impressão digital. Aqui estão os detalhes da chave PGP que o software TrueCrypt[55] de criptografia de disco utiliza para assinar digitalmente as atualizações do software.



Assim como o OTR, você precisa encontrar pessoalmente, falar com ela por telefone ou usar uma sessão do OTR já verificada para comparar cada caractere da impressão digital.

Após você tiver verificado que a chave pública que você têm pertence a pessoa que você pensa que é, você pode clicar em “Selecione ação” e escolher “Assinar Chave”.



Na captura de tela acima, eu selecionei a caixa “Assinatura local (não pode ser exportada)”. Desta maneira, você pode assinar a chave PGP, que é necessário para o Enigmail e outros softwares PGP mostrarem mensagens de segurança que façam sentido, mas faz você não correr o risco de acidentalmente publicar com quem você se comunica para o seu servidor de chave PGP[56].

Se você receber um e-mail criptografado de um alguém que você conhece mas o e-mail não estiver assinado digitalmente, você não pode estar completamente certo que foi realmente escrito por esta pessoa. É possível que seja alguém que falsificou seu e-mail ou invadiu a conta de e-mail.

Se seu conhecido lhe disser, por este e-mail, que gerou uma nova chave, você precisa encontrá-lo pessoalmente ou falar com ele por telefone e ler sua impressão digital para ter certeza de que você não está sob ataque.

Ataques

Se você não verificar identidades, não tem como saber se está sendo vítima de um ataque MITM.

O jornalista do Washington Post Barton Gellman, a quem Edward Snowden confiou as informações sobre o programa Prism da NSA, escreveu sobre a experiência dele usando PGP[57].

> *Na quinta-feira, antes do The Post publicar sua primeira história, eu entrei em contato por*

um novo canal. Ele não estava me esperando lá e respondeu alarmado.

“Eu te conheço?” ele escreveu.

Eu enviei para ele uma nota no outro canal para verificar minha impressão “digital”, uma precaução que nós temos usados por algum tempo. Cansado, enviei uma errada. “Essa não é a impressão digital correta”, ele escreveu, preparando para desligar. “Você está sendo interceptado por um ataque MITM.” Ele estava falando sobre um ataque “homem no meio”, uma técnica padrão da NSA para burlar a criptografia. Eu apresadamente corrigi meu erro.

Snowden estava certo em ser cauteloso e em insistir que ele cheque a nova impressão digital PGP de Gellman. O PGP, se usado direito, fornece as ferramentas necessárias para prevenir de um ataque MITM. Mas essas ferramentas funcionam apenas se os usuários estão alertas e fazem a verificação de identidade.

Tails: O Sistema Live Amnésico Incógnito

Usar “sistemas criptográficos fortes e propriamente implementados” tem uma enorme curva de aprendizagem e requer usuários dedicados, dispostos a ter um trabalho extra para controlar sua própria privacidade. Esta é a principal razão pela qual o OTR e o PGP não são usados, atualmente, em larga escala. Mas mesmo quando você usa essas ferramentas, como você pode ter certeza da “segurança no ponto final” quando não necessariamente pode confiar no seu sistema operacional ou em outro software que você depende todos os dias?

Quando você possui uma séria neessidade de privacidade, a solução é usar um sistema operacional completamente comprometido com a ideia de “software que você pode confiar”. Tails [58] ajuda você resolver esse problema.

Tails é um sistema operacional cujo objetivo é preservar sua privacidade e anonimato. Ele ajuda você usar a Internet anonimamente quase de qualquer lugar e de qualquer computador e não deixa nenhum traço de uso ao menos que você solicite explicitamente.

É um sistema operacional completo, desenvolvido para ser usado a partir de um DVD ou pendrive, independente do sistema operacional original do computador. É um Software Livre baseado no Debian GNU/Linux.

Tails vem com diversas aplicações pré-configuradas com o objetivo de garantir a segurança: navegador web, cliente de mensagens instantâneas, suíte de escritório, editor de som e de imagem, etc.

Tails não é para todos. Ele é difícil de usar se comparado com sistemas operacionais normais. É lento, não possui todos os softwares que talvez você queira. Mas o Tails tem todas essas propriedades porque é especialmente projetado para ser difícil dos usuários bagunçarem com a segurança de ponto final. Se você está na posição onde você pensa que a NSA, ou qualquer outro atacante potencial, pode querer atingir você e seus colegas (o relacionamento entre jornalista/denunciante vêm a mente) é uma das melhores ferramentas disponíveis.

Como o Tails não é prático para o uso cotidiano no computador é bom se habituar a usar o OTR e o PGP no seu sistema operacional normal. O Tails, por si só, não ajuda a mitigar os efeitos da rede de arrastão de vigilância, o que ajuda é criptografar o máximo de coisas que pudermos em nosso dia a dia.

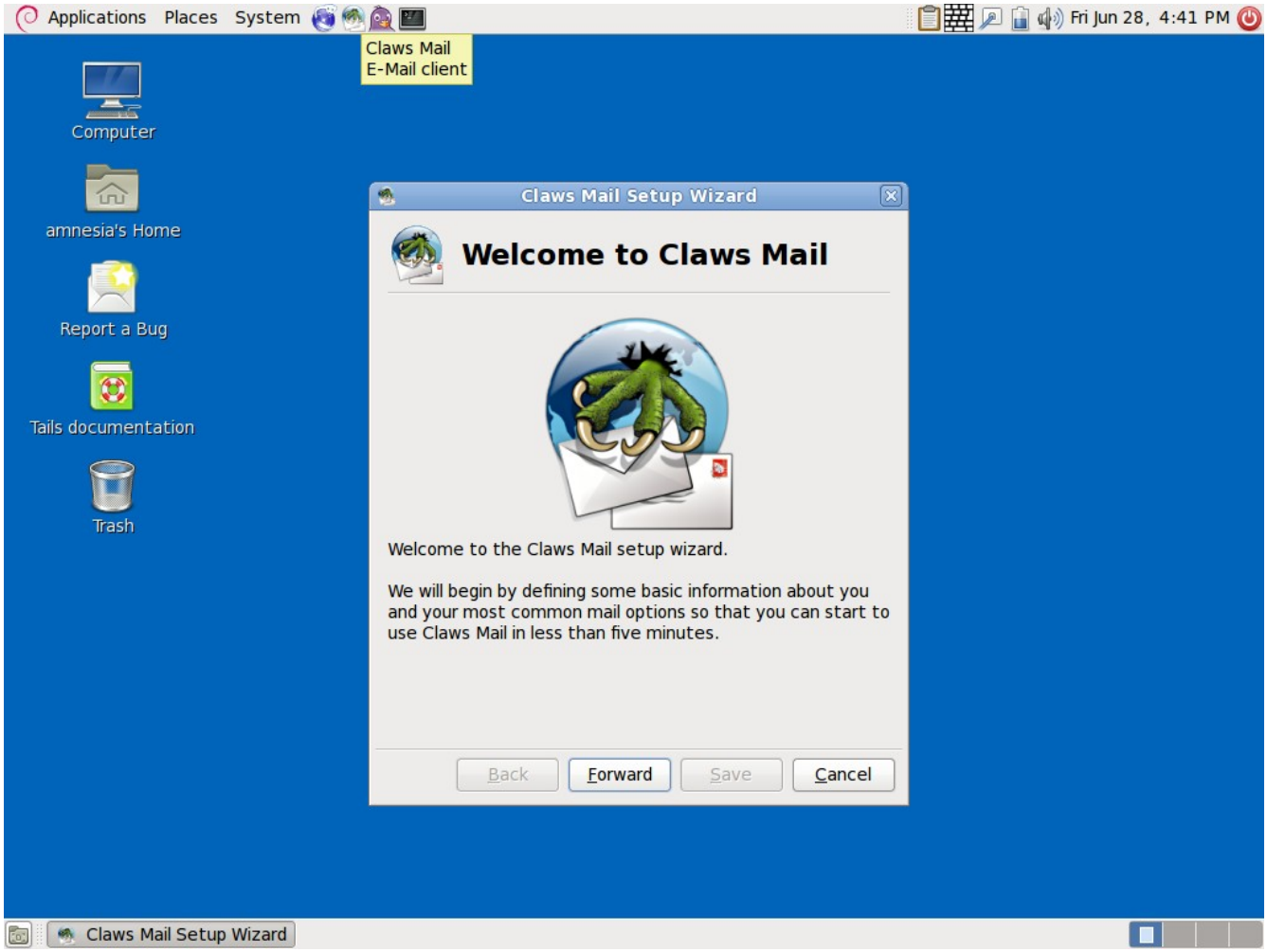
Toda vez que você inicializa o Tails é como começar do zero. Qualquer coisa que você tenha feito na sessão anterior é apagada e o sistema se reconfigura para as configurações padrões. Isso significa que mesmo se você for infectado por um malware enquanto usa o Tails, na próxima vez que você inicializar, o malware terá ido embora.

Você pode começar com o Tails baixando[59] a imagem do DVD e queimando um DVD. E usar esse DVD para inicializar. Esse passo é diferente dependendo de qual modelo de computador você tem, mas frequentemente envolve entrar na sua BIOS e mudar a ordem de inicialização (boot order). Assim seu computador tentará inicializar do DVD antes de tentar pelo disco rígido. Em computadores mais novos você talvez precise também desabilitar o “secure boot” da UEFI na BIOS, a qual é uma criptografia usada para ter certeza que seu computador apenas inicialize nas versões assinadas digitalmente do Windows (o que torna mais difícil para as pessoas inicializarem sistemas operacionais não-Windows). O site do Tails tem mais informação sobre ferramentas de inicialização para DVD ou pendrive[61].

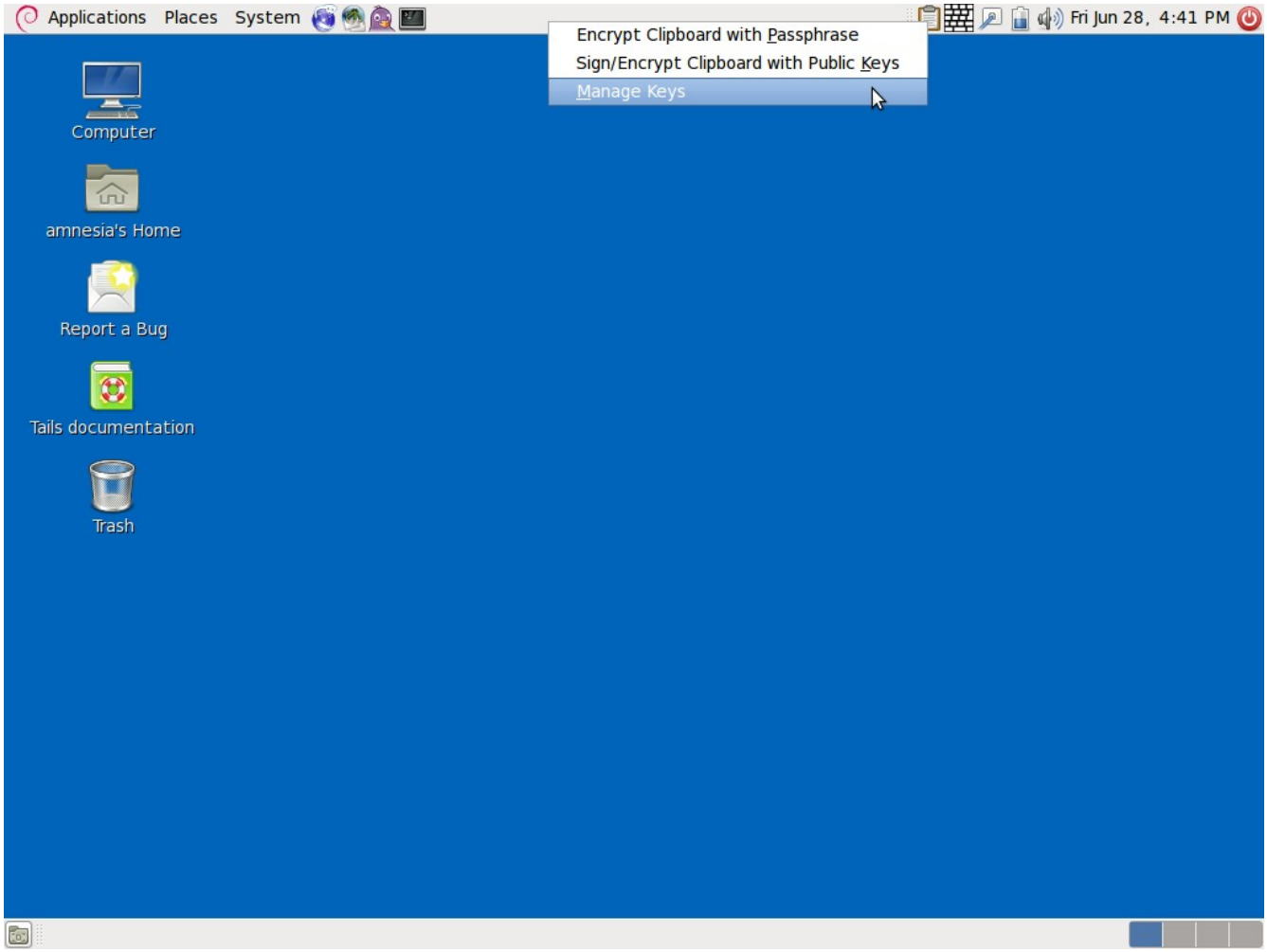
Depois de inicializar o DVD você têm a opção de instalar o Tails num pendrive, o que é especialmente útil porque permite você configurar um volume persistente[62], uma seção criptografada no seu pendrive para armazenar seus dados. Apesar de iniciar de forma zerada cada vez que ligado, é importante que você acesse sua chave OTR ou PGP, seu cliente de e-mail Claws Mail (leia abaixo) e as configurações do Pidgin, e qualquer documento que você está trabalhando. Com seu volume persistente você consegue fazer isso.

PGP e Email no Tails

Eu abordei usando o Thunderbird com o complemento Enigmail para acessar seu e-mail e usar o PGP. Mas esse software não vêm com o Tails. Tails vem com o Claws Mail[63], que inclui o plugin PGP.



Em vez de usar a interface gráfica de usuário do gerenciador de chaves PGP do Enigmail para importar, exportar, gerar, ver os detalhes e assinar as chaves, você pode clicar no ícone da área de transferência no canto superior direito da tela e escolher Gerenciar Chaves para abrir o Seahorse[64], que oferece os mesmos recursos.



Fluxo de trabalho

Para começar a se comunicar com seus amigos e colegas em privacidade e com uma alta segurança na ponta final, aqui vão os passos que você precisa seguir.

- Encontre com seus amigos pessoalmente. Cada pessoa deve trazer seu próprio laptop e pendrive.
- Baixe e queime um DVD do Tails. Inicialize pelo Tails e crie um pendrive com Tails para cada pessoa.
- Quando todos tiverem o pendrive com Tails, cada pessoa deverá inicializar o Tails no seu laptop e configurar um volume persistente no seu pendrive. Uma vez que o volume é criptografado, cada pessoa deve fazer sua própria frase secreta, que precisará ser digitada toda vez que ela inicializar o Tails. Todos devem reiniciar seus laptops no Tails de novo e nesse momento montar o volume persistente.
- Cada pessoa deve criar uma nova conta Jabber com pseudônimo. Um jeito de fazer isso é entrando em http://register.jabber.org/ no Iceweasel. Já que o Tails força todo o tráfego da Internet para passar pelo Tor, isso é suficiente para se fazer uma conta Jabber anônima.
- Cada pessoa deve abrir o Pidgin e configurá-lo para usar suas novas contas Jabber e criar uma nova chave OTR. Todos devem se adicionar na lista de amigos e iniciar sessões OTR com cada um. Já que todos estão na mesma sala, esse é o momento perfeito para comparar as impressões digitais e verificar a identidade de todos os presentes, assim vocês serão capazes de se comunicar seguramente pela Internet no futuro.

- Cada pessoa deve criar um novo endereço de e-mail com pseudônimo também. Alguns provedores de e-mail, como o Gmail, tornam muito difícil criar novas contas durante o uso do Tor e ficar anônimo. Então procure outro provedor de e-mail para usar no lugar. Confirme se esse provedor de e-mail suporta IMAP (assim você pode usar cliente de e-mail) com SSL (assim seu cliente de e-mail usa criptografia quando se comunicar com o servidor de e-mail). Se todo mundo escolher o mesmo provedor de e-mail, o envio de e-mail entre as conta nunca sairá do servidor, reduzindo assim os metadados sobre o uso do seu e-mail, disponíveis para qualquer um controlando a rede de arrastão de vigilância da Internet.
- Cada pessoa deve gerar uma nova chave PGP para seus endereços de e-mail. Assim como criptografia de disco, é importante escolher uma frase secreta forte quando gerar uma chave PGP.
- O cliente de e-mail com PGP ativado que vêm com o Tails é chamado Claws Mail. Cada pessoa deve configurar o Claws Mails para usar seu novo endereço de e-mail e enviar por e-mail uma copia da chave pública para todas as pessoas na sala.
- Cada pessoa deve importar a chave pública de todos os outros em seu chaveiro, e deve manualmente verificar as impressões digitais PGP. Não pule esse passo. No final, cada pessoa deve ter um chaveiro contendo as chaves assinadas de cada um dos outros.

Se um invasor mal intencionado atacar fisicamente e roubar seu pendrive Tails, modificá-lo, e colocá-lo de volta, ele poderá comprometer toda a segurança do Tails. Por essa razão, é importante manter seu pendrive com você todo o tempo.

Se o Diretor da CIA e general de quatro estrelas aposentado David Petraeus e sua biógrafa Paula Broadwell tivessem usado o Tails, Tor, OTR, e PGP, seu relacionamento extraconjungal [65] provavelmente teria permanecido secreto.

Uma chance de lutar

Proteger sua privacidade numa era de vigilância onipresente da NSA é uma coisa incrivelmente complexa. Muito menos do que usar o software disponível, chegar a uma compreensão básica dos conceitos envolvidos exige uma curva enorme de aprendizagem.

Mas mesmo com o acesso direto a todos os dados trafegando na velocidade da luz através dos cabos de fibra de ótica dos backbones da Internet[66], mesmo com a cooperação das maiores companhias de tecnologia dos Estados Unidos[67] (que são extremamente difíceis de boicotar), o maior, mais poderoso e melhor financiado aparato de vigilância que a humanidade já viu não pode derrotar a matemática.

O desafio do novo movimento cypherpunk é fazer a criptografia de ponta a ponta, segura e verificável, ser acessível para todo mundo, e ativada por padrão.

Notas

[1] Edward Snowden: NSA whistleblower answers reader questions, http://www.guardian.co.uk/world/2013/jun/17/edward-snowden-nsa-files-whistleblower

[2] The spy who came in from the code,
http://www.cjr.org/feature/the_spy_who_came_in_from_the_c.php?page=all

[3] HTTP Secure, https://en.wikipedia.org/wiki/Https

[4] Think your Skype messages get end-to-end encryption? Think again,
http://arstechnica.com/security/2013/05/think-your-skype-messages-get-end-to-end-encryption-think-again/

[5] Hushmail To Warn Users of Law Enforcement Backdoor,
http://www.wired.com/threatlevel/2007/11/hushmail-to-war/

[6] Man-in-the-middle attack,
https://en.wikipedia.org/wiki/Man-in-the-middle_attack

[7] U.S. Agencies Said to Swap Data With Thousands of Firms,
http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html

[8] Web's Reach Binds N.S.A. and Silicon Valley Leaders,
http://www.nytimes.com/2013/06/20/technology/silicon-valley-and-spy-agency-bound-by-strengthening-web.html

[9] Free Software Foundation, https://www.fsf.org/about/what-is-free-software

[10] Ubuntu, http://www.ubuntu.com/

[11] Debian, http://www.debian.org/

[12] Fedora Core, https://fedoraproject.org/

[13] The Underhanded C Contest, http://underhanded.xcott.com/

[14] See Phil Zimmermann's criminal investigation,
https://en.wikipedia.org/wiki/Phil_Zimmermann#Criminal_investigation and Clipper chip, https://en.wikipedia.org/wiki/Clipper_chip

[15] Disk encryption, https://en.wikipedia.org/wiki/Disk_encryption

[16] Tactical Technology Collective, https://tacticaltech.org/
[17] Worried about surveillance online? A collection of our tips and how to's on alternatives, https://alternatives.tacticaltech.org/

[18] Zero-day attack, https://en.wikipedia.org/wiki/Zero-Day_Attack

[19] The Tor Project, https://www.torproject.org/

[20] Tor and HTTPS, https://www.eff.org/pages/tor-and-https

[21] Tor's bug tracker: https://trac.torproject.org/projects/tor; mailing list: https://www.torproject.org/docs/documentation#MailingLists; and source code: https://gitweb.torproject.org/tor.git?a=tree;hb=HEAD

[22] Tor doesn't protect you from a global adversary, https://tails.boum.org/doc/about/warning/index.en.html#index7h1

[23] Download the Tor Browser Bundle, https://www.torproject.org/download/download-easy.html.en

[24] Edward Sonwden: NSA whistleblower answera reader questions, http://www.guardian.co.uk/world/2013/jun/17/edward-snowden-nsa-files-whistleblower

[25] BridgeDB, https://bridges.torproject.org/

[26] Off-the-Record Messaging, http://www.cypherpunks.ca/otr/

[27] Pidgin, https://pidgin.im/; Adium, http://adium.im/

[28] Find information about these free Jabber services here: https://www.riseup.net/en/chat, https://web.jabber.ccc.de/, http://www.jabber.org/

[29] After downloading and installing Pidgin from https://pidgin.im/ you must download and install the OTR plugin from http://www.cypherpunks.ca/otr/

[30] Documentation for using Pidgin with OTR, http://www.cypherpunks.ca/otr/index.php#docs

[31] Adium, which you can download at http://adium.im/, comes with OTR. You can find documentation for it at http://adium.im/help/pgs/AdvancedFeatures-OTREncryption.html.

[32] Gibberbot, OTR Jabber client for Android, https://guardianproject.info/apps/gibber/

[33] ChatSecure, OTR Jabber client for iOS, http://chrisballinger.info/apps/chatsecure/

[34] You can find instructions for doing so for Facebook at https://www.facebook.com/help/215888465102253/, and for Google at https://support.google.com/chat/bin/answer.py?hl=en&answer=161823

[35] In Depth Review: New NSA Documents Expose How Americans Can Be Spied on Without A Warrant, https://www.eff.org/deeplinks/2013/06/depth-review-new-nsa-documents-expose-how-americans-can-be-spied-without-warrant

[36] Long Term Privacy with Forward Secrecy, https://www.eff.org/deeplinks/2011/11/long-term-privacy-forward-secrecy

[37] Perfect forward secrecy, https://www.facebook.com/pages/Perfect-forward-secrecy/101895216519655

[38] Socialist millionaire, https://en.wikipedia.org/wiki/Socialist_millionaire

[39] Shared secret, https://en.wikipedia.org/wiki/Shared_secret

[40] Manning-Lamo Chat Logs Revealed, http://www.wired.com/threatlevel/2011/07/manning-lamo-logs

[41] Because Adium is free software with an open bug tracker, you can follow and contribute to the conversations about fixing this bug https://trac.adium.im/ticket/15722 and https://trac.adium.im/ticket/15729

[42] Pretty Good Privacy, https://en.wikipedia.org/wiki/Pretty_Good_Privacy

[43] The OpenPGP Alliance, http://openpgp.org/

[44] GNU Privacy Guard, http://www.gnupg.org/

[45] How Glenn Greenwald Began Communicating With NSA Whistleblower Edward Snowden, http://www.huffingtonpost.com/2013/06/10/edward-snowden-glenn-greenwald_n_3416978.html?1370895818

[46] It's too long to publish in print: https://pressfreedomfoundation.org/keys/micah.asc

[47] Passphrase, https://en.wikipedia.org/wiki/Passphrase

[48] https://www.eff.org/wp/defending-privacy-us-border-guide-travelers-carrying-digital-devices#passphrase

[49] The Diceware Passphrase Home Page, http://world.std.com/~reinhold/diceware.html

[50] Password manager, https://en.wikipedia.org/wiki/Password_manager

[51] Gpg4win, http://www.gpg4win.org/

[52] GPGTools, https://gpgtools.org/

[53] You can download Thunderbird at https://www.mozilla.org/en-US/thunderbird and Enigmail at http://enigmail.net/home/index.php

[54] Our Top-Secret Message to NSA Whistleblower Edward Snowden, http://www.wired.com/threatlevel/2013/06/signed-bda0df3c/

[55] TrueCrypt, http://www.truecrypt.org/

[56] Privacy concerns of key servers, https://en.wikipedia.org/wiki/Key_server_%28cryptographic%29#Privacy_concerns

[57] Code name ‘Verax’: Snowden, in exchanges with Post reporter, made clear he knew risks, http://www.washingtonpost.com/world/national-security/code-name-verax-snowden-in-exchanges-with-post-reporter-made-clear-he-knew-risks/2013/06/09/c9a25b54-d14c-11e2-9f1a-1a7cdee20287_story.html

[58] Tails: The Amnesic Incognito Live System, https://tails.boum.org/about/index.en.html

[59] Download Tails from https://tails.boum.org/download/index.en.html, and be sure to verify the PGP signature

[60] Unified Extensible Firmware Interface, Booting, https://en.wikipedia.org/wiki/Unified_Extensible_Firmware_Interface#Booting

[61] Start Tails!, https://tails.boum.org/download/index.en.html#start

[62] Persistence in Tails, https://tails.boum.org/doc/first_steps/persistence/index.en.html

[63] Claws Mail, http://www.claws-mail.org/

[64] Seahorse, https://wiki.gnome.org/Seahorse

[65] Petraeus scandal, https://en.wikipedia.org/wiki/Petraeus_scandal

[66] GCHQ taps fibre-optic cables for secret access to world's communications, http://www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa

[67] NSA slides explain the PRISM data-collection program, http://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/