O GUIA DO P.C.T.


TOR
PONTO A PONTO
CRIPTO GRAFADO


NOVA ESTRU-
TURA DE COMU-
NICAÇÃO PARA
ANARQUISTAS

Fique quieto!

Esta é uma discussão sobre ferramentas digitais para a comunicação segura e privada. Para começar, deve ser enfatizado que uma reunião cara a cara, fora da vista das câmeras e fora do alcance de outras pessoas e dispositivos, é a maneira mais segura de se comunicar. Os anarquistas iam passear para conversar muito antes de existirem textos criptografados, e ainda deveriam fazê-lo agora, sempre que possível.

Dito isto, é inegável que aplicativos e programas para a comunicação digital segura agora fazem parte de nossa infraestrutura anarquista. Talvez muitos de nós confiem mais neles do que deveriam, mas numa certa medida eles se tornaram inevitáveis para coordenar, colaborar e permanecer conectados. Considerando que estas ferramentas são infraestrutura essencial para nós, é crucial que examinemos e reavaliemos constantemente sua segurança e eficiência para nos proteger de nossos adversários.

Na última década ou duas, os anarquistas foram os primeiros a adotar essas ferramentas e técnicas de comunicação seguras, e desempenharam um papel na normalização e disseminação de seu uso dentro de nossas próprias comunidades, bem como, entre outros, engajadas em resistência e luta. O texto a seguir pretende apresentar aos anarquistas novas ferramentas para uma comunicação criptografada segura, e defender que devemos adotá-las a fim de reforçar a resiliência e a autonomia de nossa infraestrutura. Podemos aprender as vantagens dessas novas aplicações - como elas podem ajudar a evitar a vigilância e a repressão - e subsequentemente empregá-las efetivamente em nossos movimentos e ajudar a difundir seu uso de forma mais ampla.

É mais fácil enquadrar uma conversa sobre novos aplicativos de bate-papo seguro, apresentando-os em contraste com o aplicativo de bate-papo seguro que todos conhecem: Signal. O Signal é a infraestrutura de comunicação segura de fato para muitos, pelo menos na América do Norte, e está se tornando rapidamente onipresente fora dos círculos anarquistas. Se você está lendo isto, provavelmente usa o Signal, e há uma boa chance de sua mãe ou colega de trabalho usar o Signal também. O uso do Signal aumentou maciçamente em janeiro de 2021 (tanto que o serviço foi eliminado por 24 horas), atingindo 40 milhões de usuários diários. O Signal permite que os usuários troquem mensagens criptografadas com muita facilidade. Ele surgiu de um projeto anterior chamado TextSecure, que adicionava criptografia às mensagens SMS (mensagens de texto antigas para a leitura dos zoomers). O TextSecure, e mais tarde o Signal, eram ambos de confiança legítima dos anarquistas no início, em grande parte devido à rede de confiança IRL entre o desenvolvedor principal, Moxie Marlinspike, e outros anarquistas.

No início de 2022, o Moxie deixou o Signal, e isso estimulou uma nova onda de conspiração e de medo sobre o Signal. O CEO anarquista do Signal demitiu-se. O Signal foi cancelado. Uma peça intitulada "Aviso de Si(g)nal" publicada no It's Going Down[i] tentou dissipar essas preocupações e teorias da conspiração, e discutiu se os anarquistas ainda podem 'confiar' no Signal (eles podem, com ressalvas como sempre), e reiterou porque o Signal é, na verdade, bastante seguro e confiável (é fortemente auditado e examinado por especialistas em segurança).

Entretanto, o "Aviso de Si(g)nal" sugeriu que a saída de Moxie marcou, no mínimo, um lembrete da necessidade de constante escrutínio e ceticismo com o Signal, e com qualquer ferramenta de terceiros ou software que os anarquistas utilizem.

"Agora, com o verniz removido, nossa capacidade de analisar o Signal e de

avaliar seu uso dentro de nossos contextos pode começar a ocorrer fora de quaisquer distorções que a confiança às vezes pode gerar. Agora temos que olhar o aplicativo e seu protocolo subjacente como eles são, como código rodando dentro de um computador, com todos os benefícios e limitações que isso implica. Isto está longe do fim, e nem mesmo está, neste ponto, indo nessa direção. Mas, como todos os sistemas técnicos, precisamos abordá-los com informações e suspeitas".

O Signal continua a ser amplamente confiável, e ainda não há nada parecido com uma "arma fumegante" em relação à segurança do Signal. O que se segue não é uma chamada para abandonar o Signal - o Signal continua sendo uma excelente ferramenta. Mas, dado seu papel de grande porte na infraestrutura anarquista e interesse renovado em saber se podemos ou devemos confiar no Signal, podemos aproveitar esta oportunidade para examinar de perto o aplicativo, como ele funciona, como o usamos e explorar alternativas.

O exame minucioso do Signal não revela manipulações secretas, ou vulnerabilidades em aberto. Mas revela uma priorização da experiência do usuário e um desenvolvimento racionalizado em relação às metas de segurança mais robustas. As metas e características mais amplas do projeto Signal agora podem não se encaixar exatamente em nosso modelo de risco. E como causa de como o Signal funciona em um nível estrutural, os anarquistas dependem de um serviço centralizado para a maior parte de suas comunicações online seguras. Isto tem consequências para a segurança.

Mas existem alternativas que foram desenvolvidas em grande parte para tratar especificamente destas questões. **Briar** e **Cwtch** são duas novas aplicações de chat seguro que, como o Signal, também permitem a troca de mensagens criptografadas. Na superfície, eles parecem funcionar muito como o Signal, mas como eles realmente funcionam é bem diferente. Onde o Signal é um serviço de

mensagens criptografadas, ao contrário, Briar e Cwtch são aplicações PCT - são aplicações autônomas que permitem o envio de mensagens Peer-to-peer (ponto a ponto) e Criptografadas por Tor.

Estas aplicações PCT e como elas funcionam serão apresentadas em detalhes. Mas a melhor maneira de realmente explicar suas vantagens (e por que os anarquistas devem se importar até mesmo com outras aplicações de bate-papo seguro quando já temos Signal) é realizar uma análise crítica profunda do Signal.

Modelo de risco e isenção de responsabilidade

Antes de mergulhar, é importante contextualizar esta discussão, definindo o modelo de risco relevante e fornecendo algumas isenções de responsabilidade.

Para os propósitos desta discussão, nossos adversários são a imposição da lei a nível nacional ou local, com algum acesso aos recursos de imposição da lei a nível nacional.

Apesar da criptografia de ponta a ponta esconder o conteúdo das mensagens em trânsito, estes adversários têm muitas capacidades que poderiam ser usadas para descobrir ou interromper nossas atividades, comunicações ou redes para poderem nos reprimir. Em particular, as seguintes capacidades desses adversários serão abordadas:

- Eles têm acesso irrestrito a sites de mídia social e outras informações públicas.

- Em alguns casos, eles podem monitorar todo o tráfego de internet doméstico ou celular para um indivíduo específico.

- Eles podem acessar dados ou metadados "anônimos" de usuários de aplicativos, provedores de telefonia celular, ISPs, etc.

- Eles podem acessar o tráfego de rede registrado coletado em massa a partir de muitos pontos de gargalo na infra-estrutura da Internet.

- Com diferentes graus de sucesso, podem combinar, analisar

e correlacionar tais dados e tráfego de rede para desanonimizar usuários, mapear redes sociais ou revelar outras informações potencialmente incriminatórias sobre indivíduos ou grupos e suas comunicações.

■ Eles podem comprometer a infraestrutura da Internet (ISPs, provedores de serviços, corporações, desenvolvedores de aplicativos) através de coerção ou hacking.[ii]

■ Eles podem interromper o tráfego da Internet em geral ou de maneiras específicas, seja porque controlam a infraestrutura da Internet, seja por meio de ciberataques contra a infraestrutura da Internet.

Este guia preocupa-se em mitigar as capacidades destes adversários, mas há muitos outros que não podem ser abordados aqui:

■ Eles podem infectar remotamente dispositivos de indivíduos visados com registrador de teclado e malware de rastreamento, em casos extremos.

■ Eles podem obter acesso à comunicação criptografada através de informantes confidenciais ou agentes infiltrados.

■ Eles podem exercer grande pressão ou tortura para obrigar indivíduos a desbloquear seu telefone ou computador ou desistir de senhas.

■ Embora eles não possam quebrar uma boa criptografia dentro de qualquer prazo prático, no caso de uma apreensão eles ainda podem ser capazes de obter dados de dispositivos ostensivamente criptografados devido a outras vulnerabilidades (por exemplo, no sistema operacional do dispositivo) ou falhas operacionais de segurança.

Qualquer método de comunicação seguro é altamente dependente das práticas de segurança do usuário ao redor. Não importa que você esteja usando o *aplicativo de bate-papo seguro™ preferido de Edward Snowden* se seu adversário tiver um registrador de teclado instalado em seu telefone, ou se alguém compartilhar capturas de tela de seus textos criptografados no Twitter, ou se seu telefone for

apreendido e não estiver devidamente protegido[iii].

Uma explicação completa da segurança operacional, cultura de segurança e conceitos e melhores práticas relacionadas está fora do escopo deste texto - esta discussão é apenas uma parte da segurança operacional relevante para o modelo de risco operacional. Você deve considerar a cultura geral de segurança para proteger contra a ameaça de infiltrados e informantes, como usar com segurança dispositivos como telefones e laptops para que não possam incriminá-lo se apreendidos, e como construir hábitos para minimizar os dados deixados em dispositivos eletrônicos por completo (encontrar-se pessoalmente e deixar seu telefone em casa!).

A chamada "cibersegurança" é rápida: há uma guerra de atrito entre as ameaças e os desenvolvedores de aplicativos. As informações fornecidas aqui podem estar desatualizadas quando você estiver lendo isto.

As características da aplicação ou implementações podem mudar, invalidando parcialmente alguns dos argumentos aqui apresentados (ou reforçando-os). Se a segurança de suas comunicações eletrônicas for crucial para sua segurança, você não deve confiar em nenhuma recomendação dada aqui ou em qualquer outro lugar pelo seu valor nominal.

Perda de Si(g)nal

Como começou, como está agora

Você provavelmente usou o Signal hoje. E não há nada realmente *tão* errado com o Signal. É importante afirmar que, apesar das críticas a seguir, o objetivo aqui não é incitar o pânico sobre o uso do Signal. Seu objetivo não deve ser apagar imediatamente o Signal, queimar seu

telefone e correr para o mato. Talvez você deva fazer isso de qualquer forma para sua própria saúde mental, mas não apenas por causa deste guia. Considere fazer uma caminhada primeiro, pelo menos.

Uma tangente para lidar com algumas teorias conspiratórias

Uma busca rápida no DuckDuckGo por "Signal CIA" (ou talvez uma busca no Twitter? Eu não saberia dizer) trará muita desinformação e teorias conspiratórias sobre o "Signal". Dada a natureza já crítica deste guia e a importância da nuance, por favor, permita uma reclamação sobre estas teorias conspiratórias.
A teoria de conspiração mais comum sobre o Signal é que ela foi secretamente desenvolvida pela CIA e, portanto, está "manipulado". Consequentemente, a CIA (ou às vezes a NSA) tem a capacidade de acessar facilmente tudo o que você diz no Signal, entrando pela porta secreta dos fundos.[iv]

A centelha da verdade que acendeu esta teoria é a seguinte:

Entre 2013 e 2016, os desenvolvedores da Signal receberam pouco menos de 3 milhões de usd em financiamento do Open Technology Fund. Originalmente, o of era um programa da Rádio Ásia Livre que é supervisionado pelo U.S. Agency for Global Media (desde 2019, o otf é diretamente administrado pelo usagm). A usagm é uma "agência independente do governo dos Estados Unidos", que promove os interesses nacionais dos Estados Unidos internacionalmente e é financiada e administrada diretamente pelo governo dos Estados Unidos. O governo dos EUA administra e financia a usagm/Radio Free Asia, que financia a otf, que financiou o desenvolvimento do Signal (e Hilary Clinton era secretária de Estado na época!!!) - assim, a CIA criou o Signal.

A UsAGM (e todos os seus projetos como a Radio Free Asia e a OTF) promove os interesses nacionais dos EUA, minando ou perturbando os governos com os quais os EUA estão em concorrência ou em conflito. Além de promover narrativas contrárias da mídia (através do apoio a uma "imprensa livre e independente" nesses países), isso também envolve a produção de ferramentas que podem ser utilizadas para contornar a censura e resistir a regimes opressivos.

Os beneficiários da OTF são divulgados de forma transparente[v] e não é segredo que o objetivo da OTF é criar ferramentas para

subverter o poder de regimes que dependem fortemente da repressão aberta on-line, da vigilância em massa e da forte censura da Internet para manter seu poder (e que esses regimes são aqueles dos quais o governo dos Estados Unidos não é fã). Como e por que isto acontece em relação a projetos como o Signal é claramente relatado pelos principais pontos de venda como o Wall Street Journal[vi]. Esta informação também é relatada por órgãos como a RT sem contexto e com embelezamentos sensacionais[vii] que levam a estas teorias conspiratórias.

O jornalista Kit Klarenberg gosta de produzir artigos idiotas sobre o Signal para emissoras como RT

O Signal é de código aberto, o que significa que todo o seu código é auditado e examinado por especialistas. É o único lugar onde todos estão procurando uma manipulação da CIA. Em termos de vigilância de massa, é mais fácil e mais eficaz para nossos adversários inserir secretamente a vigilância em aplicações e infraestrutura de Internet de código fechado amplamente utilizadas, com a cooperação de corporações cúmplices.[viii] Em termos de vigilância direcionada, é mais fácil instalar malware em seu telefone[ix].

Muitos projetos de software de código aberto, como o Signal, têm recebido financiamento de fontes semelhantes. A OTF também financia ou já financiou inúmeros outros projetos dos quais você pode ter ouvido falar: Tor (sobre os quais existem teorias de conspiração semelhantes), K-9 Mail, NoScript, F-Droid, Certbot e Tails (cujos desenvolvedores são anarquistas).

Este financiamento é sempre divulgado de forma transparente. Basta verificar a página de patrocinadores da Tails[x] onde você pode ver a OTF listada como um patrocinador passado (e que seu principal patrocinador atual é... o Departamento de Estado dos

EUA!). Ambos os aplicativos PCT discutidos neste guia são parcialmente financiados por fontes similares.

Há uma infinita discussão a ser feita sobre fontes de financiamento de projetos de código aberto que facilitam a privacidade ou a resistência à vigilância: conflitos de interesse, ética, confiabilidade, tais ferramentas sendo desenvolvidas no contexto da geopolítica neoliberal... É bom ter um ceticismo saudável e críticas sobre como os projetos são financiados, mas isso não deve nos levar a teorias conspiratórias que obscurecem as discussões sobre sua real segurança e segurança na prática. O Signal tem recebido financiamento de muitas fontes "duvidosas" deste tipo: O desenvolvimento inicial do Signal foi financiado pela venda de seu projeto precursor, TextSecure, para o Twitter por uma quantia desconhecida. Mais recentemente, o Signal recebeu um empréstimo de US$ 50 milhões, com juros de 0%, do fundador da WhatsApp, que agora é o CEO da Signal Foundation. Há muitas provas válidas que explicam por que e como o Signal foi financiado por uma iniciativa dos Estados Unidos em prol do domínio global que não sugere nem implica de forma alguma a existência de um mecanismo de manipulação da CIA impossível de esconder e destinado a atingir os usuários do Signal.

O Signal é bom mesmo?

Portanto, se o Signal não é uma operação da CIA, então está tudo bem? Os protocolos de criptografia do Signal são amplamente considerados seguros, e o Signal tem um grande histórico de melhoria de suas características e de endereçamento de vulnerabilidades de forma oportuna e transparente. O Signal conseguiu tornar o bate-papo criptografado de ponta a ponta fácil o suficiente para realmente se tornar popular. A adoção generalizada do Signal é quase certamente uma coisa boa.

Mas, à parte as teorias da conspiração, há boas razões para os anarquistas serem céticos em relação ao Signal. O Moxie tinha uma abordagem um tanto dogmática para muitas escolhas estruturais e de engenharia de software feitas no desenvolvimento do Signal. Essas decisões foram tomadas intencionalmente (como explicado em posts de blogs, palestras e em vários tópicos arcanos de GitHub) para facilitar a ampla adoção do Signal Messenger entre os usuários menos experientes em tecnologia, facilitar o crescimento a longo prazo do

projeto e permitir a evolução do fluxo e a adição de novas características.

Há muito tempo que os técnicos de segurança cibernética online criticam estas decisões como concessões que sacrificam melhor segurança, privacidade ou anonimato do usuário no interesse dos próprios objetivos da Moxie para o Signal. Aprofundar demais nisto corre o risco de entrar no território de debate dominado por pedantes FOSSbros (se ainda não estivermos lá). Para mantê-lo extremamente breve, as justificativas de Moxie podem ser resumidas para manter o Signal competitivo no ecossistema capitalista do Vale do Silício, movido pelo lucro. Debates sobre estratégias de desenvolvimento de software sob o capitalismo tardio à parte, os aspectos de detalhe do Signal mais comumente criticados são os seguintes:

1. O Signal depende de uma infraestrutura de servidor centralizada
2. O Signal exige que cada conta esteja vinculada a um número de telefone
3. O Signal tem um sistema de pagamento em moeda criptográfica incorporado.

Talvez Moxie tivesse razão e suas concessões valessem a pena: hoje, o Signal é muito popular, o aplicativo escalou maciçamente com o mínimo de dores de crescimento, inúmeras novas características (tanto para usabilidade quanto para segurança) foram facilmente introduzidas, e parece ser sustentável para o futuro previsível.[xi]

Mas a onipresença do Signal na infraestrutura anarquista exige um exame cuidadoso dessas críticas, especialmente porque elas se aplicam a nossos casos de uso e modelo de risco em um mundo em mudança. O exame destas críticas do Signal ajudará a explicar como aplicações PCT como **Briar** e **Cwtch**, que usam um modelo completamente diferente para uma comunicação segura, pode potencialmente nos proporcionar mais resiliência e segurança.

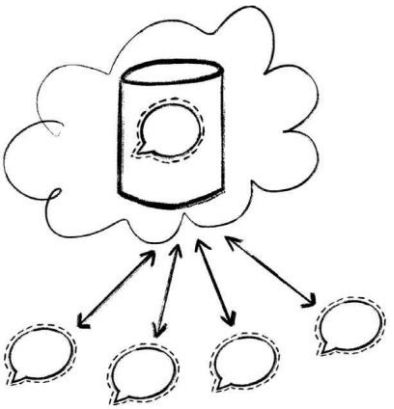
Signal como serviço centralizado

O Signal é na verdade menos do que um aplicativo e mais do que um serviço. Signal (Open Whisper Systems/The Signal Foundation)

fornece o aplicativo Signal (que você pode baixar e executar em seu telefone ou computador) e opera o Servidor de Signal[xii]. O Aplicativo Signal, por si só, não pode fazer nada. O Servidor de Signal fornece o serviço subjacente, manuseando e repassando todas as mensagens enviadas e recebidas com o Signal.

É assim que funciona a maioria dos aplicativos de bate-papo. Discord, WhatsApp, iMessage, Instagram/Facebook Messenger e Twitter DMs são todos serviços de comunicação centralizados, em que você executa um aplicativo em seu dispositivo e um servidor centralizado operado por alguns retransmissores terceiros de mensagens entre indivíduos.

Uma centralização como esta proporciona muitos benefícios para você como usuário. Você pode sincronizar suas mensagens e seu perfil sobre o servidor para acessá-las em diferentes dispositivos. Você pode enviar uma mensagem a seu amigo mesmo quando ele está offline e o servidor irá armazenar a mensagem até que seu amigo faça o login e a recupere. As conversas em grupo entre muitos usuários funcionam sem falhas, mesmo que os usuários possam estar ligados ou desligados em horários diferentes.



O Signal utiliza criptografia de ponta a ponta, o que significa que o Servidor de Signal não pode ler nenhuma de suas mensagens. Mas sendo um serviço de comunicação centralizado tem muitas repercussões importantes para a segurança e confiabilidade.

Os Correios do Signal

O Signal pode ser comparado a um serviço postal. É um serviço postal muito bom, como talvez tenham em algum lugar da Europa. Neste exemplo, o Servidor de Signal é como um posto dos correios. Você escreve uma carta para seu amigo e a sela em um envelope endereçado (digamos que ninguém além de seu amigo pode abrir o envelope - isso é a criptografia). Quando lhe for conveniente, você entrega todas as cartas que está enviando no Correio do Signal, onde elas são classificadas e enviadas para os vários amigos a quem são endereçadas. Se um amigo não estiver em casa, não há problema!

Os Correios do Signal guardarão a carta até que encontrem seu amigo em casa, ou seu amigo pode simplesmente pegá-la no Correio do Signal local dele. Os Correios do Signal são realmente bons (Europa, certo?) e até permitem que você encaminhe sua correspondência para qualquer lugar que você queira recebê-la.

Talvez você possa identificar o potencial problema de segurança confiando nos Correios do Signal para lidar com todo o seu correio. Envelopes selados significa que nenhum dos

transportadores de correio ou funcionários dos Correios do Signal pode ler qualquer uma de suas cartas (criptografia = eles não podem abrir os envelopes). Mas qualquer pessoa que tenha um correio sabe que eles ainda podem aprender muito sobre você apenas manuseando toda a sua posta. Eles sabem de quem você está recebendo cartas, todas as suas assinaturas de revistas, quando você está em casa ou não, todos os diferentes lugares para onde você encaminha sua correspondência e todas as merdas embaraçosas que você encomenda on-line. Este é o problema potencial de um serviço centralizado que lide com todo o seu correio - quero dizer, mensagens!

Metadados são para sempre

As informações que todos nos Correios do Signal conhecem sobre você e seu correio são metadados. Metadados são os dados sobre dados. Isto pode incluir coisas como o remetente e destinatário de uma mensagem, a hora em que ela foi enviada e onde ela foi entregue. Todo o tráfego na Internet gera inerentemente este tipo de metadados. Os servidores centralizados fornecem um ponto fácil onde todos esses metadados podem ser observados ou coletados, já que todas as mensagens passam por um único ponto.

Deve ser enfatizado que o exemplo acima sobre os Correios do Signal é apenas metafórico e serve para ilustrar o que são metadados e porque é uma preocupação relevante para os serviços de comunicação centralizada. O Signal é na verdade extremamente bom em minimizar ou obscurecer metadados. Graças à magia negra criptográfica e ao design inteligente do software, há muito poucos metadados que o Servidor do Signal pode acessar facilmente. Nas próprias palavras do Signal:

"As coisas que não temos armazenadas incluem qualquer coisa sobre os contatos de um usuário (como os próprios contatos, um hash dos contatos, qualquer outra informação de contato derivada), qualquer coisa sobre os grupos de um usuário (como quantos grupos um usuário está, em quais grupos um usuário está, as listas de membros dos grupos de um usuário), ou qualquer registro de com quem um usuário tem se comunicado."[xiii]

Existem apenas dois pedaços de metadados que são conhecidos por serem persistentemente armazenados:

- se um determinado número de telefone está registrado em

uma conta Signal

- a última vez que uma determinada conta Signal foi conectada ao servidor

Ainda bem! Em teoria, isso é tudo que qualquer funcionário curioso dos Correios do Signal pode saber sobre você. Mas isto se deve, em parte, à abordagem "Eu não vejo" do próprio Servidor do Signal. Até certo ponto, devemos confiar que o Servidor do Signal está fazendo o que diz...

Não há outra escolha que acreditar

Como o aplicativo Signal em seu telefone ou computador, o Servidor do Signal também é baseado (principalmente)[xiv] em código aberto e, portanto, é submetido ao mesmo exame e auditorias por especialistas em segurança.

Entretanto, há uma realidade importante e inevitável a considerar sobre o Servidor do Signal: somos forçados a confiar que o Servidor do Signal está realmente rodando o mesmo código de fonte aberta que é compartilhado conosco. Este é um problema fundamental ao confiar em qualquer servidor centralizado executado por um terceiro.

"Não coletamos ou armazenamos nenhuma informação sensível sobre nossos usuários, e isso não mudará nunca."[xv]

Como um grande órgão público sem fins lucrativos, a Signal não está em posição de recusar de forma sustentável o cumprimento de garantias ou intimações para dados de usuários. O Signal tem até mesmo uma página em seu site[xvi] que lista várias intimações que recebeu e suas respostas.
Lembre-se das duas partes de metadados que o Servidor do Signal armazena que podem ser divulgadas:

Account	Responsive Information in Signal's Possession
[redacted]	Last connection date: 1634169600000 (unix millis) Account created: 1606866784432 (unix millis)

Resposta do Signal para solicitação de dados mostrando um número de telefone [ocultado], data de criação da conta, e última vez que foi visto.

No momento de escrever, não há razão para duvidar do que foi divulgado, mas deve ser observado que o Signal também se comunica com mandados de advertência que os impedem de revelar que eles receberam até mesmo uma intimação ou mandado[xvii]. Historicamente, o Signal luta contra esses mandados de advertência, mas não sabemos o que não sabemos, e o Signal não emprega um "mandado de autorização" para alertar os usuários sobre quaisquer intimações ou mandados que ainda não foram divulgados. Não há razão firme para acreditar que o Signal tenha cooperado com a aplicação da lei com mais frequência ou em maior grau do que eles alegam, mas há três cenários a considerar:

1. Mudanças na lei poderiam resultar na obrigação do Signal de coletar e divulgar mais informações sobre seus usuários mediante solicitação, e isto poderia acontecer sem o conhecimento público.
2. O Signal poderia ser convencido por argumentos éticos, morais, políticos ou patrióticos a cooperar secretamente com os adversários.
3. O Signal poderia ser infiltrado ou invadido pelos adversários para coletar mais dados dos usuários em segredo, ou de outra forma informar quais são os poucos metadados existentes mais prontamente para os adversários.

Todos estes cenários são concebíveis e têm precedentes históricos em outros lugares, mas não são necessariamente prováveis ou possíveis. Devido à "magia negra criptográfica" acima mencionada e às complexidades dos protocolos de rede, mesmo que o Servidor do Signal tenha sido modificado para ser mal-intencionado, ainda há um limite para a quantidade de metadados que poderiam ser coletados sem que fossem percebidos pelos usuários ou observadores. Não seria equivalente, digamos, ao fato que os Correios do Signal deixassem entrar um espião (através de uma "manipulação" literal da CIA!) que lesse e registasse todos os metadados de cada carta que passasse. Mudanças nas políticas e códigos do Signal poderiam resultar em pequenas, mas crescentes quantidades de metadados, ou outras informações, prontamente disponíveis aos adversários, e isto poderia acontecer com ou sem nosso conhecimento. Não há razão particular para desconfiar do Servidor do Signal neste ponto, mas os anarquistas devem pesar quanta confiança estão depositando em um terceiro, mesmo um

tão historicamente confiável como o Signal.

Comunidade de Informação Global
Centro de Dados de Iniciativa Nacional no Utah

Big Data

Muitos adversários poderosos são capazes de capturar e armazenar grandes quantidades de tráfego na Internet[xviii]. Isto pode incluir conteúdos de mensagens reais para tráfego não criptografado, mas com o uso generalizado da criptografia, agora são principalmente metadados sobre o tráfego e a atividade de todos na Internet que são capturados e armazenados.

Podemos escolher confiar que o Signal não está ajudando ativamente nossos adversários na coleta de metadados sobre as comunicações dos usuários do Signal, mas nossos adversários têm muitas outras formas de coletar esses dados: seja com a cooperação de empresas de hospedagem como a Amazon ou Google (o Signal é atualmente hospedado pela Amazon Web Services), visando tais empresas de hospedagem sem sua cooperação[xix], ou simplesmente monitorando o tráfego da Internet em escala de massa[xx].

Metadados sobre as atividades de todos on-line também estão cada vez mais disponíveis para adversários menos poderosos, que podem comprá-los de forma bruta ou analisada de corretores de dados, que por sua vez os compram ou adquirem de entidades como desenvolvedores de aplicativos ou provedores de telefonia celular.[xxi]

Os metadados coletados desta forma resultam em grandes conjuntos de dados de difícil análise. Mas cada vez mais nossos adversários (e até mesmo corporações ou jornalistas) podem pegar esses enormes conjuntos de dados, combiná-los e aplicar poderosas ferramentas de análise algorítmica para produzir correlações úteis sobre indivíduos ou grupos de pessoas (isto é frequentemente referido como " Big Data"). Mesmo o acesso a pequenas quantidades destes dados e técnicas de análise grosseiras pode desanonimizar indivíduos e produzir resultados úteis[xxii].

Tommy, o mensageiro

Este é um exemplo hipotético para demonstrar como a análise de tráfego e a correlação de metadados podem desanonimizar um usuário do Signal.

Imagine um espectador frequente, mas mal comportado, chamado Tommy, que está sempre enviando mensagens de texto no Signal durante o filme. O brilho da tela de seu telefone (Tommy não usa o modo escuro) incomoda a todos no cinema. Mas, de outra forma, é muito escuro no cinema para Tanner, o gerente intrometido, para descobrir exatamente quem está sempre mandando mensagens. Tanner começa a coletar todos os dados que passam pelo Wi-Fi do cinema procurando por conexões com o Servidor do Signal. As frequentes conexões de Tommy com o Servidor do Signal se destacam de imediato. Tanner é capaz de registrar o endereço MAC (um identificador único associado a cada telefone) e confirmar que o mesmo dispositivo está usando frequentemente o Signal no Wi-Fi do cinema durante o espetáculo. Tanner é então capaz de correlacionar isto com registros de transações de cartão de crédito de sua bilheteria e descobrir um cartão de crédito que sempre compra ingressos para filmes ao mesmo tempo em que o dispositivo de uso frequente do Signal está ativo (o nome do portador do cartão também é revelado: Tommy). Tendo determinado o endereço MAC, nome e cartão de crédito do telefone de Tommy, Tanner pode fornecer esta informação a um investigador privado sombrio, que comprará acesso a grandes conjuntos de dados coletados por corretores de dados (de provedores de telefones celulares e aplicativos móveis), e determinará um local onde o mesmo telefone celular é mais frequentemente utilizado. Além da sala de cinema, esta é a casa de Tommy. Tanner vai à casa de Tommy à noite e lança bombas de incêndio em seu carro (a sala de cinema é uma fachada para os Hell's Angels).

Metadados armados

"Matamos as pessoas em função dos metadados..."

– General Michael Hayden, ex-diretor da NSA 1999-2005 e diretor da CIA 2006-2009

"... mas não é isso que fazemos com esses metadados!" (sorrisos deliberados, risadas do público surgem do público).[xxiii]

Em uma Internet onde os adversários têm estas capacidades de coletar e analisar enormes quantidades de metadados e tráfego, o uso de servidores centralizados pode ser uma responsabilidade. Os adversários podem mais facilmente direcionar os dispositivos para o Servidor do Signal, seja monitorando o tráfego na Internet em geral, no nível do ISP, ou potencialmente em pontos de conexão com o próprio Servidor do Signal.
Eles podem então tentar empregar técnicas de análise para revelar coisas específicas sobre usuários individuais ou suas comunicações por meio do Signal.

Na prática, isto pode ser difícil. Você pode se perguntar se um adversário observando todo o tráfego que entra e sai do Servidor do Signal poderia determinar que você e seu amigo troquem mensagens observando que uma mensagem foi enviada de seu endereço IP para o Servidor do Signal às 14:01 e depois o Servidor do Signal enviou uma mensagem do mesmo tamanho para o endereço IP de seu amigo às 14:02. Felizmente, uma análise correlacional muito simples como esta não é possível devido à quantidade de tráfego que entra e sai do Servidor do Signal o tempo todo e como exatamente esse tráfego é tratado a esse nível. Isto é menos verdadeiro para chamadas de vídeo/voz onde os protocolos de Internet em uso fazem análise correlacional do tráfego para descobrir quem chamou quem mais plausível[xxiv]. Ainda assim, um adversário observando todo o tráfego que entra e sai do Servidor do Signal e tentando determinar quem está falando com quem tem uma tarefa muito difícil. Talvez impossível, até agora.

E ainda assim, as técnicas de coleta de dados e as ferramentas de análise algorítmica comumente chamadas de " Big Data " estão se tornando mais poderosas a cada dia. Nossos adversários estão na vanguarda disto. O uso generalizado da criptografia de todas as telecomunicações tornou a escuta tradicional muito menos eficaz e, consequentemente, nossos adversários estão fortemente motivados a aumentar sua capacidade de reunir e analisar de forma útil metadados. Eles o dizem claramente: "*se você tem metadados suficientes, você não precisa realmente de conteúdo* "[xxv]. Eles matam

pessoas em função dos metadados.

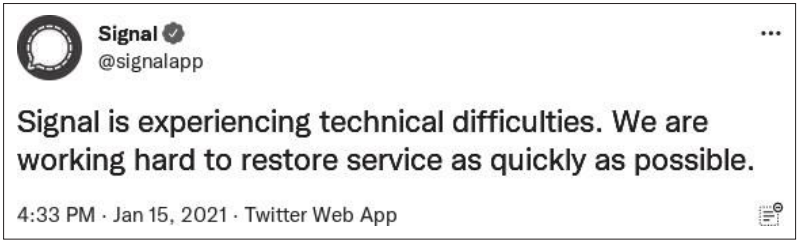
Portanto, embora talvez não seja possível determinar com certeza algo tão preciso quanto quem falou com quem em um determinado momento, nossos adversários ainda estão melhorando rapidamente sua capacidade de determinar qualquer informação incriminatória que possam a partir de metadados. Eles são rotineiramente revelados através de vazamentos por terem estado na posse de capacidades de vigilância mais poderosas ou invasivas do que se pensava anteriormente - não é descabido projetar que suas capacidades são mais avançadas do que sabemos.

O Signal é mais vulnerável a este tipo de vigilância e análise, pois é um serviço centralizado. O tráfego do Signal na Internet não é difícil de detectar, e o Servidor do Signal fornece um ponto central fácil para observar ou coletar metadados sobre os usuários do Signal e suas atividades. Os potenciais compromissos do Signal, ou mudanças em suas políticas ou na lei, podem render uma coleta ainda mais fácil do tráfego do Signal e metadados para nossos adversários analisarem.

Os usuários individuais podem empregar algumas atenuações contra isto, como a execução do Signal através do Tor ou de uma VPN, mas isto pode ser tecnicamente desafiador para implementar e propenso a erros do usuário. Qualquer esforço para tornar mais difícil ligar um usuário do Signal a um indivíduo específico também é complicado pelo fato de que o Signal requer que cada conta seja ligada a um número de telefone (mais sobre isso mais adiante).

Dependência e pontos únicos de falha

Um serviço centralizado significa não só que existe um ponto central de observação, mas também um único ponto de falha - o Signal não funciona se o Servidor do Signal estiver desligado. É fácil esquecer que este é o caso até o dia em que isso acontece. O Signal pode cometer um erro de configuração ou ser atingido com uma enchente de novos usuários por causa de um Tweet viral e, de repente, o Signal simplesmente não funciona.

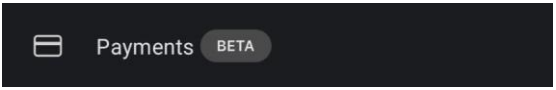

Signal
@signalapp
Signal is experiencing technical difficulties. We are working hard to restore service as quickly as possible.
4:33 PM · Jan 15, 2021 · Twitter Web App

O Signal também pode cair por causa de ações intencionais tomadas por um adversário. Imagine um ataque de Negação de Serviço Distribuído (ou outro ataque cibernético) destinado a interromper a função do Signal durante uma rebelião de massa. Os provedores de serviços que realmente hospedam o Servidor do Signal também poderiam optar por derrubar o Servidor do Signal sem aviso prévio por uma variedade de razões: compelidos pela pressão de um adversário, por pressão política, pela opinião pública, ou por razões financeiras.

Um serviço centralizado também é mais fácil de interromper pelos adversários que controlam diretamente sua infraestrutura local de Internet[xxvi]. Quando isto acontece em certos lugares, o Signal geralmente é rápido para responder, implementando ativamente mudanças ou soluções criativas, resultando em um jogo de gato e rato entre o Signal e qualquer Nação-Estado que esteja tentando bloquear o Signal dentro de sua área de controle. Mais uma vez, é uma questão de confiar que os interesses do Signal sempre se alinharão aos nossos quando um adversário estiver tentando interromper o Signal desta forma em uma determinada região.

Criptocontrovérsia

Em 2021, o Signal começou a integrar um sistema de pagamento ao aplicativo utilizando a moeda criptográfica MobileCoin. Se você não tinha ideia, provavelmente não está sozinho, mas está bem ali, na tela de configurações.



MobileCoin é uma moeda criptográfica pouco conhecida, focada na privacidade, que o Moxie também ajudou a desenvolver. Debates sobre esquemas de pirâmide de moedas criptográficas à parte, a preocupação aqui é que ao incluir pagamentos em moeda criptográfica dentro do aplicativo, o Signal está se abrindo para um monitoramento jurídico muito maior por parte das autoridades policiais. As moedas criptográficas são boas para o crime e fraudes, e o governo dos Estados Unidos está cada vez mais preocupado em regular seu uso. O Signal não é um bando de

piratas - eles são uma organização sem fins lucrativos de alto nível, e não podem resistir de forma sustentável a quaisquer novas leis que o governo dos EUA possa aprovar para regulamentar as moedas criptográficas.

Se os milhões de usuários do Signal estivessem de fato usando MobileCoin para transações diárias, não é difícil imaginar o Signal enfrentando um maior escrutínio da missão da Comissão de Valores Mobiliários dos EUA, ou de outros órgãos reguladores. O governo não gosta de criptografia, mas realmente não gosta que pessoas comuns paguem por drogas ou soneguem impostos. Imagine um cenário em que criminosos cibernéticos confiam no Signal e no MobileCoin para aceitar pagamentos de vítimas de resgate. Isso poderia realmente trazer problemas, e isso poderia ser muito perturbador para o Signal como ferramenta de comunicação confiável e segura.

Informante 514-U

Esta frustração já deveria ser familiar aos anarquistas que usam o Signal: as contas do Signal requerem um número de telefone. Qualquer que seja o número de telefone a que uma conta esteja ligada, também é revelado a qualquer pessoa com quem você se conecte no Signal. Além disso, determinar se um determinado número de telefone está ligado a uma conta de Signal ativa é uma tarefa banal.

Existem soluções para este problema, mas todas elas envolvem a obtenção de um número de telefone que não esteja vinculado à sua identidade apenas para que você possa usá-lo para se registrar em uma conta do Signal. Dependendo de onde você estiver, dos recursos disponíveis e de seu nível de habilidade técnica, isto pode variar de inconveniente a proibitivamente difícil.

O Signal também não permite facilmente que várias contas sejam utilizadas a partir do mesmo telefone ou laptop. A criação de múltiplas contas do Signal para identidades diferentes, ou a associação a projetos diferentes, torna-se uma tarefa enorme, especialmente porque você precisa de um número de telefone distinto para cada uma delas.

Geralmente é bastante fácil para os adversários com recursos limitados identificar um indivíduo com base em seu número de telefone. Além disso, se um adversário obtiver um telefone que não esteja devidamente fechado ou criptografado, ele terá acesso aos números de telefone dos contatos e membros do grupo. Obviamente, esta é uma questão de segurança operacional que vai além do Signal, mas o fato de que o Signal exige que cada conta esteja vinculada a um número de telefone, complica em muito o potencial de perdas de dados prejudiciais.

Não se sabe se o Signal alguma vez permitirá a existência de contas sem estar vinculado a um número de telefone, ou algum outro identificador da vida real semelhante. Tem sido relatado como algo que eles nunca farão, ou algo em que estão trabalhando, mas que está para sempre no limbo[xxvii]. De qualquer forma, é um grande problema para muitos anarquistas que usam esses processos.

PCTeando pesado

Tendo discutido o Signal por muitas páginas, é hora de introduzir algumas alternativas que abordem algumas das problemáticas com o Signal: **Briar** e **Cwtch**.

Briar e **Cwtch** são, por sua concepção, extremamente resistentes a metadados, e oferecem um melhor potencial de anonimato. Também são mais resistentes, sem um servidor central ou um único ponto de falha. Mas estas vantagens vêm com custos - maior segurança vem com algumas peculiaridades de usabilidade a que você tem que se acostumar.

Lembre-se, tanto **Cwtch** quanto **Briar** são aplicações PCT porque são:

1. Peer-to-peer (ponto a ponto)
2. Como o Signal, as mensagens são criptografadas de extremidade a extremidade
3. As identidades e atividades dos usuários são anonimizadas

enviando todas as mensagens através do Tor

Por compartilharem uma arquitetura básica, eles têm muitas características e considerações em comum.

Peer-to-peer (Ponto a Ponto)

O Signal é um serviço de comunicação centralizado, que utiliza um servidor para retransmitir e transmitir cada mensagem que você envia a seu amigo. As questões com este modelo foram amplamente discutidas! Você provavelmente já está entediado de ouvir falar sobre isso. O P em PET é peer-to-peer. Em um modelo peer-to-peer, você troca mensagens diretamente com seu amigo. Não existe um servidor central intermediário dirigido por um terceiro. Toda conexão direta depende apenas da infraestrutura mais ampla da Internet.

Lembra-se dos Correios do Signal? Com um modelo peer-to-peer, você não usa um serviço postal para lidar com seu correio. Você mesmo entrega cada carta diretamente a seu amigo. Você a escreve, a sela em um envelope (criptografia de ponta a ponta), a coloca em sua bolsa de mensageiro e atravessa a cidade de bicicleta onde você a entrega em mãos a seu amigo.

A comunicação ponto-a-ponto confere muita resistência aos metadados. Não há um servidor central que trate de todas as mensagens às quais os metadados podem ser expostos. É mais difícil para os adversários que tentam coletar metadados sobre comunicações de massa, monitorar o tráfego que entra e sai dos servidores centrais conhecidos. E não há um só ponto de falha.

Desde que haja uma rota através da Internet para você e seu amigo se conectarem, você pode conversar.

Sincronicidade

Há uma coisa importante a notar sobre a comunicação peer-to-peer: porque não há um servidor central para armazenar e retransmitir mensagens, você e seu amigo precisam ambos ter o aplicativo funcionando e on-line a fim de trocar mensagens. Devido a isso, estas aplicações PCT são inclinadas para a comunicação síncrona.

E se você atravessar a cidade de bicicleta para entregar uma carta a seu amigo e... eles não estão em casa!? Se você realmente quer ficar em peer-to-peer você tem que entregar a carta diretamente a seu amigo. Você não pode simplesmente deixá-lo para eles (não há lugar suficientemente seguro!).

Você deve ser capaz de alcançar diretamente seu amigo para entregar a mensagem - este é o aspecto síncrono da comunicação peer-to-peer.

As chamadas telefônicas também são um bom exemplo de comunicação síncrona. Você não pode ter uma conversa telefônica a menos que estejam ambos ao telefone ao mesmo tempo. Mas quem realmente faz mais chamadas telefônicas? Hoje em dia, estamos muito mais acostumados a uma mistura de mensagens síncronas e assíncronas, e serviços de comunicação centralizados

como o Signal são ótimos para isso. Às vezes, você e seu amigo estão conectados e trocam mensagens em tempo real, mas há um grande atraso entre as mensagens de ida e volta. Pelo menos para algumas pessoas... alguns leitores provavelmente têm seu telefone ligado e ao seu alcance o tempo todo, e respondem a cada mensagem que recebem imediatamente, em todas as horas do dia. Para eles, toda comunicação é e deve ser sincrônica... você sabe quem você é.

Mudar para comunicação de texto apenas sincronizada pode ser um verdadeiro choque inicialmente. Alguns leitores podem se lembrar de como foi usar o aim, icq, ou msn Messenger (se você se lembra deles, suas costas doem). Você precisa estar consciente se alguém está realmente online ou não.

Você não pode enviar um monte de mensagens se as pessoas estiverem offline, para serem entregues mais tarde.

Se algum de vocês não mantiver o aplicativo funcionando e online o tempo todo, você e seu amigo podem adquirir o hábito de marcar datas para conversar. Isto pode ser muito legal. Paradoxalmente, a normalização da comunicação assíncrona resultou em uma expectativa de estar basicamente online e responsiva o tempo todo. A comunicação assíncrona encoraja uma intencionalidade em nossas comunicações, restringindo-a aos momentos em que estamos de fato online, em vez da expectativa de estar espontaneamente disponível mais ou menos o tempo todo.

Outra consequência importante da sincronicidade das conexões peer-to-peer: ela pode tornar as conversas em grupo um pouco estranhas. E se nem todos no grupo estiverem online ao mesmo tempo? **Briar** e **Cwtch** lidam cada um com este problema de maneira diferente, de modo que será dividido na respectiva seção de cada aplicativo.

Tor

Embora a comunicação peer-to-peer seja muito resistente a metadados e evite outras armadilhas de usar um servidor central, por si só não protege contra a coleta de metadados "Big Data" e a análise do tráfego. Tor é uma solução de redução muito boa para isso, e os aplicativos PCT encaminham todo o tráfego através do Tor.

Se você é um anarquista lendo isto, você já deve estar familiarizado com Tor e como ele pode ser alavancado para fornecer anonimato.[xxviii] Os aplicativos PCT formam conexões peer-to-peer diretas para trocar mensagens através do Tor. Isto o torna muito, muito mais difícil para qualquer adversário, seja um que observa você de uma forma orientada ou um que tenta observar e correlacionar atividades através da Internet, para identificar quem está falando com quem ou fazer quaisquer outras determinações úteis. É muito mais difícil ligar um determinado usuário de um aplicativo PCT a uma identidade da vida real. Tudo o que qualquer observador pode ver é que você está usando o Tor.

Tor não é à prova de balas, e possíveis problemas com Tor ou ataques à rede Tor são possíveis. Entrar nos detalhes de como o Tor funciona ocuparia muito espaço aqui, e há muitos recursos online

para ensiná-lo[xxix]. Entender as advertências gerais ao uso do Tor também é importante[xxx]. Como o Signal, o tráfego no Tor também pode ser interrompido por interferência no nível da infraestrutura da Internet, ou por ataques de Negação de Serviço que visam toda a rede Tor[xxxi]. Ainda é muito mais difícil para um adversário bloquear ou interromper o Tor do que derrubar ou bloquear o Servidor Central do Signal.

Deve-se notar que, em algumas situações, o uso do Tor pode isolar você. Se você é o único que usa o Tor em uma determinada região ou em determinados momentos, isto pode destacar você. Mas isto pode ser verdade para qualquer aplicativo não muito utilizado. Ter Signal em seu telefone também costumava fazer com que você se destacasse. Quanto mais pessoas usarem Tor, melhor, e se usado corretamente, Tor oferece melhor proteção contra tentativas de identificar usuários do que não. Os aplicativos PCT usam o Tor para tudo, por padrão, em uma implementação razoavelmente infalível.

Sem telefone, sem problemas

Uma vitória fácil. Ambos os aplicativos PCT descritos aqui não precisam de um número de telefone para registrar uma conta.

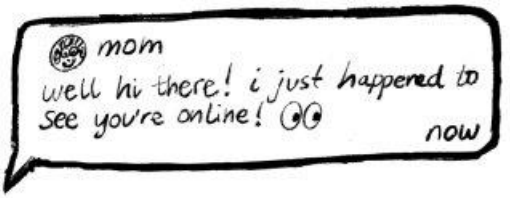
Sua conta é gerada localmente em seu dispositivo e o ID da conta é uma sequência aleatória muito longa de caracteres que você compartilha com seus amigos para se tornar contatos. Você pode facilmente usar estes aplicativos apenas em um computador, em um telefone sem cartão SIM, ou em um telefone, mas sem vincular diretamente ao seu número de telefone.

Advertências gerais sobre os aplicativos PCT

O status de vazamento

A comunicação ponto a ponto vaza inevitavelmente um pedaço específico de metadados: o status online/offline de um determinado

usuário. Qualquer pessoa que você tenha adicionado como contato, ou a quem você tenha confiado sua ID de usuário (ou qualquer adversário que tenha conseguido obtê-lo) pode dizer se você está online ou offline a qualquer momento. Isto não se aplica realmente ao nosso modelo de risco, a menos que você seja particularmente descuidado com quem você adicionou como contato. Mas vale a pena notar porque às vezes você não quer que um amigo que você está evitando saiba que você está online!



Uma única conta em cada dispositivo

Quando você abre estes aplicativos pela primeira vez, você cria uma senha que é usada para criptografar seu perfil de usuário, contatos e histórico de mensagens (se você optar por salvá-lo). Estes dados permanecem criptografados em seu dispositivo quando você não está usando o aplicativo.

Como não há um servidor central, não é possível sincronizar sua conta através de múltiplos dispositivos. Você pode migrar manualmente sua conta de um dispositivo para outro, como de um telefone antigo para um telefone novo, mas não há sincronização de nuvem mágica. Ter uma conta separada em cada dispositivo é uma solução fácil que incentiva a compartimentação. Não ter que se preocupar com versões assimétricas em um servidor central (mesmo que codificadas) ou em outro dispositivo também é uma vantagem. Ele força uma consideração mais intencional de onde seus dados estão e como você os acessa, em vez de simplesmente manter tudo 'na nuvem' (também chamado de computador de

outrem). Também não há cópia de segurança dos dados de sua conta em um servidor de terceiros que irá restaurar sua conta se você esquecer sua senha ou perder seu dispositivo. Se ele se foi, ele se foi.

Lembre-se que as únicas maneiras de contornar tudo isso são confiar em um servidor central com uma cópia de seus contatos e rede social, ou confiar em outra rede social da mesma forma que o Signal usa sua lista de contatos de números de telefone. Não devemos confiar em um servidor central para armazenar estas informações (mesmo em forma criptografada), nem usar algo como números de telefone. A possibilidade de ter que reconstruir nossa rede social a partir do zero é o custo de evitar essas questões de segurança, e na verdade incentiva uma prática de manutenção e restabelecimento de conexões confiáveis com nossos amigos.

Duração da bateria

A execução de conexões peer-to-peer Tor significa que este aplicativo tem que ser conectado e estar sempre ouvindo no caso de algum de seus amigos lhe enviar uma mensagem. Estes aplicativos podem ser bastante ávidos por bateria em telefones mais antigos. No entanto, isto está se tornando cada vez menos problemático, pois o uso da bateria melhora em geral e as baterias dos telefones ficam melhores.

Não é compatível com iOS

Nenhum destes aplicativos é executado no iOS da Apple, principalmente devido ao iOS ser hostil a qualquer aplicativo que estabeleça conexões peer-to-peer Tor. É improvável que isto mude no futuro (embora não impossível).

Conhecendo os aplicativos PCT

Chegou a hora de conhecer estes aplicativos PCT. Ambos têm excelentes guias de usuário que fornecem informações detalhadas

sobre como usá-los, mas aqui está uma rápida visão geral de como cada um deles funciona, suas características e como é usá-los.

BRIAR

Site web do Briar: https://briarproject.org

Manual do usuário Briar: https://briarproject.org/manual/

Verificação dos bastidores e das dinâmicas

O Briar é desenvolvido pelo Projeto Briar, que é um coletivo de desenvolvedores, hackers e entusiastas do Software-livre, em sua maioria sediados na Europa. Além de resistir à vigilância e à

censura, a visão maior do projeto é construir infraestrutura de comunicação e ferramentas a serem usadas durante um desastre ou apagão na internet. Obviamente, esta visão é de interesse para os anarquistas que se encontram em regiões onde há um alto potencial para um desligamento parcial ou total da Internet durante uma rebelião, ou onde pode ocorrer um colapso geral da infraestrutura (ou seja, em todos os lugares). Se a Internet estiver desligada, o Briar pode sincronizar mensagens através de Wi-Fi ou Bluetooth.

O Briar também permite o fácil compartilhamento do próprio aplicativo diretamente com um amigo. Ele pode até formar uma rede de malha rudimentar entre os pares, de modo que alguns tipos de mensagens podem saltar de usuário para usuário.

Briar é de código aberto e também encomendou uma auditoria de segurança independente em 2013[xxxii].

- Atualmente, o Briar está disponível para Android e a

versão corrente é 1.4.9.

■ Há uma versão beta desktop disponível para Linux (versão atual 0.2.1.), embora faltem muitas funcionalidades.

■ As versões Windows e macOS do cliente desktop estão planejadas.

Uso do Briar

Bate-papo básico

O bate-papo básico funciona muito bem. Ambos os amigos têm que se adicionar um ao outro para poder se conectar. Briar tem uma pequena interface agradável para fazer isso pessoalmente, onde você escaneia os códigos QR um do outro. Mas o canal também é feito à distância, compartilhando ID de usuário (tipo um 'briar://link'), ou qualquer usuário pode "introduzir" usuários dentro do aplicativo, permitindo que dois usuários se tornem contatos um com o outro através de seu amigo mútuo.

Um pouco de fricção na forma como você adiciona contatos pode parecer inconveniente, mas considere como este modelo encoraja práticas melhores e mais intencionais em torno da confiança. Briar tem até mesmo um pequeno indicador ao lado de cada nome de usuário para lembrá-lo de como você o "conhece" (pessoalmente, através de links de compartilhamento, ou através de uma introdução).

Atualmente, em chats diretos você pode enviar fotos, usar emojis, apagar mensagens e definir mensagens para desaparecer automaticamente após sete dias (). Se seu amigo não estiver online, você pode escrever-lhe uma mensagem e ela será enviada automaticamente na próxima vez que você o vir online.

Grupos privados

Os Grupos Privados do Briar são conversas básicas de grupo. Somente o criador do grupo pode convidar membros adicionais, portanto os Grupos Privados são muito intencionais, destinados a um propósito específico. Os Grupos Privados suportam threading (você pode responder diretamente a uma mensagem especifíca, mesmo que não seja a mensagem mais recente em um chat), mas é bastante grosseiro. Você não pode enviar imagens em um Grupo Privado, nem permitir o desaparecimento de mensagens.

Como as conversas em grupo do Briar são realmente sem servidor, as coisas podem ser um pouco estranhas quando nem todos no grupo estão online ao mesmo tempo. Lembra-se da sincronicidade? Qualquer mensagem de grupo será enviada a todos os membros de um grupo que estejam online no momento. Briar conta com todos os membros de um grupo para transmitir mensagens a outros membros que são offline. Se você perdeu algumas mensagens em um bate-papo em grupo, qualquer um dos outros membros que recebeu essas mensagens pode retransmiti-las a você quando ambos estiverem online.

Fóruns

Briar também tem uma característica chamada Fóruns. Os Fóruns funcionam da mesma forma que os Grupos Privados, exceto que qualquer membro pode convidar mais membros.

Blog

O blog do Briar é realmente muito legal? Cada usuário, por padrão, tem um feed do Blog. Os posts de blog feitos por seus contatos aparecem no feed do blog.

Você também pode comentar um post de Blog, ou 'reblogar' um post de Blog de um contato para que ele seja compartilhado com todos os seus contatos (com seu comentário) - é uma rede social rudimentar que funciona apenas no Briar.

Leitor de feed RSS

Briar também tem um leitor de feeds RSS embutido que vai buscar novos posts em sites de notícias sobre o Tor. Esta pode ser uma ótima maneira de ler o mais novo comunicado de seu site de informação anarquista ilustrado favorito (que provavelmente fornece um feed RSS, se você ainda não sabia!). Novos posts dos feeds RSS que você adicionou aparecem no feed do Blog, e você pode 'reblogá-los' para compartilhá-los com todos os seus contatos.

Sinta-se confuso

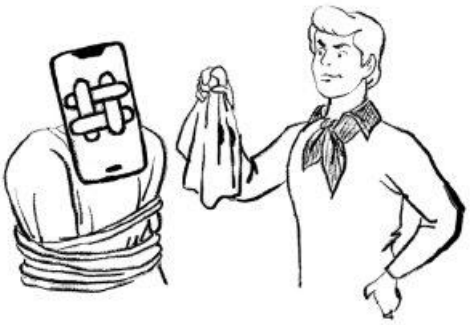
Briar faz um monte de coisas legais para mover mensagens entre contatos sem nenhum servidor central. Da mesma forma como Grupos Privados sincronizam mensagens entre membros sem um servidor, Fóruns e Blogs são retransmitidos de contato para contato. Todos os seus contatos podem receber uma cópia de um post de Blog ou Fórum mesmo que você nunca esteja online ao mesmo tempo - contatos compartilhados transmitem a mensagem para você. O Briar não cria uma verdadeira rede em malha onde as mensagens são passadas através de qualquer outro usuário do Briar (o que poderia proporcionar uma oportunidade para um adversário operar muitas contas Briar maliciosas e coletar metadados). O Briar não confia nenhuma de suas mensagens a usuários para os quais elas não são destinadas. Em vez disso, todo usuário que deve receber uma mensagem também participa da transmissão dessa mensagem para outros que também devem recebê-la, e apenas com seus próprios contatos.

Isto pode ser especialmente útil para criar uma rede de comunicação confiável que funcione mesmo que a Internet esteja fora do ar. Os usuários do Briar podem sincronizar as mensagens através de Wi-Fi ou Bluetooth.

Você poderia caminhar até a loja de informática local, ver alguns amigos e sincronizar uma variedade de posts de blogs e fóruns. Depois você volta para casa e seus colegas de quarto podem sincronizar com você para obter as mesmas atualizações de todos os seus contatos compartilhados mutuamente.

As limitações do Briar

Cada instância do aplicativo suporta apenas uma conta. Portanto, não se pode ter várias contas no mesmo dispositivo. Isto não é um problema se você estiver usando Briar apenas para conversar com um grupo próximo de amigos, mas faz com que seja difícil para usar Briar em vários projetos ou redes diversas que você de outra forma desejaria compartimentar. Para isso, o Briar fornece várias justificativas baseadas em segurança, e uma simples é a seguinte: se o mesmo dispositivo usa várias contas, teoricamente poderia ser mais fácil para um adversário determinar se essas contas estão ligadas, apesar de usar o Tor. Se um perfil e outro nunca forem vistos on-line ao mesmo tempo, há uma boa chance de estarem usando o mesmo telefone celular para suas contas individuais do Briar. Há outras razões, e também potenciais soluções, mas por enquanto não há suporte para ter vários perfis no mesmo dispositivo.



O protocolo Briar também exige que ambos os usuários se adicionem como contatos, ou sejam apresentados por um amigo mútuo, antes que possam interagir. Isto impede a publicação de um endereço Briar para receber mensagens anônimas, como se você

quisesse publicar seu ID de usuário do Briar para receber críticas honestas sobre uma publicação comparando diversos aplicativos de bate-papo seguro.

Briar e assincronia

Os usuários realmente gostam de sua comunicação assíncrona. O Projeto Briar está trabalhando em uma Briar Mailbox, que é outro aplicativo que poderia ser executado facilmente em um velho telefone Android ou outro hardware barato. A Caixa de Correio ficaria essencialmente online para receber mensagens para você, e então sincronizar com seu dispositivo principal através do Tor quando você estiver online. Esta é uma ideia interessante. Uma única caixa de correio Briar poderia ser potencialmente usada por vários usuários que confiam uns nos outros, como colegas de quarto em uma casa coletiva, ou clientes regulares de uma loja de informática local. Em vez de depender de um servidor central para facilitar a assincronia, um servidor pequeno e fácil de configurar que você controla é usado para armazenar mensagens recebidas para você e seus amigos enquanto você estiver offline. Isto ainda está em desenvolvimento, portanto, quão seguro seria (por exemplo, as mensagens armazenadas ou outros metadados seriam seguros o suficiente se a caixa postal fosse acessada por um adversário?) não é conhecido e teria que ser avaliado.

CWTCH

Site web do Cwtch: https://cwtch.im/

Manual do usuário do Cwtch: https://docs.cwtch.im/

Verificação dos bastidores e das dinâmicas

Então o nome... rima com 'butch'. Evidentemente, é uma palavra galesa que significa *um abraço que cria um lugar seguro*.

Cwtch é desenvolvido pela Open Privacy Research Society que é uma sociedade não profit sediada em Vancouver. A dinâmica do

Cwtch pode ser descrita como " Signal Queer". A Open Privacy é muito investida na construção de ferramentas para apoiar comunidades subrepresentadas, perseguidas ou vitimizadas e para resistir à opressão. Eles também trabalharam em outros projetos legais, como a pesquisa de algo chamado 'Shatter Secrets', projetado para proteger segredos contra cenários onde indivíduos podem ser obrigados a revelar uma senha (como uma passagem de fronteira).

Cwtch também é de código aberto e seu protocolo é baseado em parte no projeto PCT anterior Ricochet. O Cwtch é um projeto mais novo que o Briar, mas seu desenvolvimento se moveu rapidamente e novas versões saem com frequência.

- Atualmente, a versão corrente é a 1.8.0.
- Cwtch está disponível para Android, Windows, Linux e MacOS.

Uso do Cwtch

Quando você abre o Cwtch pela primeira vez, você cria seu primeiro perfil, protegido com uma senha. Seu novo perfil recebe um lindo avatarzinho gerado e um endereço Cwtch. Ao contrário do Briar, o Cwtch suporta vários perfis no mesmo dispositivo, e você pode ter vários perfis desbloqueados ao mesmo tempo. Isto é ideal se você quiser ter identidades compartimentadas para projetos ou redes diversas sem trocar entre múltiplos dispositivos (mas atenda às potenciais questões de segurança ao fazer isto!).
Para adicionar um amigo, basta dar a ele seu endereço Cwtch. Você e seu amigo não têm que trocar endereços primeiro para conversar. Isto significa que com Cwtch você pode publicar um endereço Cwtch publicamente e amigos e críticos podem contatá-lo anonimamente. Você também pode configurar o Cwtch para bloquear automaticamente as mensagens recebidas de estranhos.
Aqui está um endereço Cwtch para entrar em contato com o autor desta publicação com feedback ou correio de ódio:

g6px2uyn5tdg2gxpqqktnv7qi2i5frr5kf2dgnyielvq4o4emry4qzid

No bate-papo direto, Cwtch apresenta uma formatação de texto rica e agradável, emojis e respostas. Cada conversa pode ser definida para "salvar seu histórico" ou "apagar histórico" quando o Cwtch é desligado.
Este é o esqueleto e funciona muito bem. Atualmente, todas as outras características do Cwtch são "experimentais" e você pode optar por elas nos parâmetros. Isto inclui bate-papos em grupo, compartilhamento de arquivos, envio de fotos, imagens de perfil, pré-visualização de imagens e links clicáveis com pré-visualização de links. O desenvolvimento do Cwtch tem sido bastante rápido, portanto, quando você estiver lendo isto, todas estas características podem estar totalmente desenvolvidas e disponíveis por padrão.

Bate-papo de grupo

Cwtch também oferece Grupos de bate-papo como uma "Característica Experimental". A Cwtch atualmente usa servidores operados por usuários para facilitar as Conversas em Grupo, o que é muito diferente da abordagem do Briar. A Open Privacy considera os bate-papos em grupo resistentes a metadados como um problema aberto, e espera-se que da leitura até aqui você possa entender o porquê. Semelhante a como o Servidor do Signal funciona, os servidores Cwtch são projetados de tal forma que eles são sempre considerados "não confiáveis" e aprendem o mínimo possível sobre o conteúdo das mensagens ou metadados. Mas é claro que estes servidores são operados por usuários individuais e não por uma terceira parte central.

Qualquer usuário Cwtch individual pode se tornar o "servidor" de um bate-papo em grupo. Isto é ótimo para conversas em grupo de uso único, onde um usuário pode se tornar o "anfitrião" de uma reunião ou discussão rápida. Os servidores Cwtch de Bate-papo em Grupo também permitem a entrega assíncrona de mensagens, para

que um grupo ou comunidade possa operar seu próprio servidor continuamente como um serviço para seus membros.

Como o Cwtch aborda os bate-papos em grupo ainda está em desenvolvimento e pode mudar no futuro, mas é uma solução muito promissora e legal no momento.

Cwtch e assincronia

Os Grupos de bate-papo no Cwtch permitem o envio assíncrono de mensagens (desde que o servidor/hospedeiro esteja online), mas como Briar, Cwtch exige que ambos os contatos estejam online para que mensagens diretas sejam enviadas. Ao contrário do Briar, Cwtch não permitirá que você coloque em fila as mensagens para enviar a um contato quando ele estiver online.

Cripto advertência do Cwtch

No final de 2019, a Open Privacy que desenvolve a Cwtch, recebeu uma doação de $40.000 dólares canadenses sem compromisso da fundação Zcash. Zcash é outra moeda criptográfica centrada na privacidade semelhante, mas decididamente inferior a Monero[xxxiii]. Em 2019, a Cwtch estava em desenvolvimento muito precoce, e a Open Privacy fez algumas experiências exploratórias em torno do uso de Zcash ou de moedas criptográficas de cadeia de bloqueio similares como soluções criativas para vários desafios criptográficos, com a ideia de que ela poderia ser incorporada à Cwtch em algum momento[xxxiv]. Desde então, nenhum trabalho adicional com Zcash ou outras moedas criptográficas foi associado ao Cwtch, e parece não ser uma prioridade ou área de pesquisa para Privacidade Aberta. Mas deve ser mencionado como um potencial sinal vermelho para pessoas que são altamente cautelosas com os esquemas de moedas criptográficas. Recordando, o Signal já tem uma moeda criptográfica totalmente funcional embutida no aplicativo, permitindo aos usuários enviar e receber MobileCoin.

Considerações finais

...saiu do grupo

Muitos leitores podem estar dizendo a si mesmos "os aplicativos PCT não parecem suportar muito bem bate-papos em grupo... e eu adoro bate-papos em grupo"! Em primeiro lugar, quem realmente ama os bate-papos em grupo? Em segundo lugar, vale a pena fazer críticas de como os anarquistas acabam usando as conversas em grupo em Signal para fazer notar que a forma como são implementadas em Briar e Cwtch não deveria ser uma quebra de contrato.

Signal, Cwtch e Briar permitem que você tenha facilmente uma conversa em grupo em tempo real (sincronizada!) para uma reunião ou discussão coletiva rápida que de outra forma não poderia acontecer pessoalmente. Mas quando as pessoas se referem a um "bate-papo em grupo" (especialmente no contexto do Signal), isto não é normalmente o que elas querem dizer. Os bate-papos em grupo no Signal muitas vezes se transformam em enormes e duradouros feeds de atualizações semipúblicas, postes de lixo, links compartilhados novamente, etc., que na prática são mais como mídia social. Há mais membros do que se poderia realisticamente estar tendo uma conversa funcional, muito menos tomando decisões.

A diminuição da utilidade e segurança com o aumento do tamanho, abrangência e persistência dos grupos do Signal foi bem discutida na excelente peça "Signal Fails"[xxxv]. Quanto mais um grupo conversa em grupo se afasta de um objetivo pequeno, de curto prazo, intencional e único, mais difícil é implementar com Briar e Cwtch - e isto não é uma coisa ruim. Se alguma coisa, Briar e Cwtch promovem hábitos mais saudáveis e mais seguros, sem as "características" do Signal que facilitam dinâmicas de bate-papo em grupo criticadas em peças como " Signal Fails" (Falha do Signal).

Proposta

Briar e Cwtch são ambos novos projetos. Alguns anarquistas já ouviram falar deles e estão tentando usar um ou outro para projetos ou casos de uso específicos. As versões atuais podem parecer mais complicadas de usar do que o Signal, e sofrem com o efeito de rede - todos estão usando o Signal, portanto ninguém quer usar outra coisa[xxxvi]. Vale ressaltar que as barreiras aparentes ao uso de Cwtch e Briar neste momento (ainda em beta, efeito de rede, diferente do que você está acostumado, sem versão iOS) são todas exatamente as mesmas barreiras que desencorajaram as pessoas desde cedo a usar o Signal (conhecido também como TextSecure!).

É difícil conseguir que as pessoas aprendam e comecem a usar qualquer nova ferramenta. Especialmente quando a ferramenta atual à qual estão acostumadas parece funcionar muito bem! Não há como negar o desafio. Este guia acabou com páginas e páginas longas em um esforço para fazer um argumento convincente de que os anarquistas, que possivelmente se preocupam mais com estas questões, deveriam tentar usar estes aplicativos PCT.

Os anarquistas já foram bem sucedidos na adoção de novas ferramentas eletrônicas desafiadoras, espalhando-as e empunhando-as eficazmente durante atos de luta e resistência. A normalização do uso de aplicativos PCT em adição ou em vez de Signal para comunicação eletrônica aumentará a resiliência de nossas comunidades e daquelas que podemos convencer a se juntarem a nós. Eles nos ajudarão a nos proteger da coleta e análise de metadados cada vez mais poderosos, nos isolarão da dependência de um serviço centralizado e nos proporcionarão um acesso mais fácil ao anonimato.

Portanto, aqui está a proposta. Tendo lido este guia, implemente-o e compartilhe-o. Você não pode tentar Cwtch ou Briar sozinho, você precisa de pelo menos um amigo (ou co-conspirador) para experimentá-los. Instale-os junto com sua equipe e tente usar um ou outro para um projeto específico que se encaixe. Tenha uma reunião semanal com pessoas que não podem se reunir pessoalmente para discutir notícias que de outra forma seriam compartilhadas em uma conversa num grupo do Signal espalhado. Mantenha contato com

alguns amigos distantes, ou com uma equipe que tenha sido dividida por distância. Você não precisa (e provavelmente não deveria) apagar o Signal, mas no mínimo estará ajudando a construir resiliência estabelecendo conexões de back-up para suas redes. À medida que as coisas estão aquecendo, a probabilidade do tipo de repressão intensa ou fraturas da sociedade que interrompem o Signal em outros países está se tornando mais provável em todos os lugares, e estaremos bem atendidos se tivermos nossas comunicações em reserva mais cedo do que mais tarde!

Briar e Cwtch estão ambos sob desenvolvimento ativo, por anarquistas e pessoas simpatizantes com nossos objetivos. Ao usá-los, seja seriamente ou por diversão, podemos contribuir para seu desenvolvimento relatando bugs e vulnerabilidades, e inspirando seus desenvolvedores a continuar sabendo que seu projeto está sendo usado. Talvez até mesmo alguns dos mais inclinados a computadores entre nós possam contribuir diretamente, auditando seu código e protocolos ou mesmo juntando-se ao seu desenvolvimento.

Além de ler este guia, tentar realmente usar estes aplicativos como um coletivo de usuários curiosos é a melhor maneira de apreciar como eles são estruturalmente diferentes do Signal. *Mesmo que* você não consiga usar estes aplicativos regularmente, tentando diferentes ferramentas de comunicação seguras e *compreendendo* como e por que eles são diferentes do que você está familiarizado com o assunto, melhorará sua alfabetização em segurança digital. Você não precisa dominar a matemática desafiadora que sustenta o protocolo de criptografia de dupla catraca do Signal[xxxvii], mas um melhor conhecimento e compreensão de como essas ferramentas funcionam em teoria e na prática conduz a uma melhor segurança operacional em geral. Enquanto dependermos da infraestrutura para nos comunicarmos, devemos tentar entender como essa infraestrutura funciona, como ela nos protege ou nos torna vulneráveis, e explorar ativamente formas de fortalecê-la.

Palavra final

Toda esta discussão tem sido sobre aplicativos de chat de comunicação segura que rodam em nossos telefones e computadores. A palavra final deve ser um lembrete de que tanto quanto o uso de ferramentas que codificam e tornam anônimas as comunicações on-line podem capacitá-lo e protegê-lo contra adversários, você nunca deve digitar ou dizer nada em qualquer aplicativo ou dispositivo sem apreciá-lo pode ser lido de volta para você em tribunal. Encontrar-se com seus amigos, cara a cara, ao ar livre e longe de câmeras e outros eletrônicos é de longe a maneira mais segura de ter qualquer conversa - que precisa ser segura e privada. Desligue seu telefone, abaixe o telefone e vá para fora!

Apêndice: algumas outras aplicações de que você já deve ter ouvido falar

Ricochet Refresh

https://www.ricochetrefresh.net/

Ricochet foi um aplicativo PCT de desktop muito antigo, financiado pelo projeto para liberdade de expressão baseado na Europa. Ricochet Refresh é a versão atual. Fundamentalmente é muito semelhante ao Cwtch e Briar, mas é bastante rudimentar - apresenta bate-papo direto básico e transferência de arquivos, e só roda em MacOS, Linux e Windows. É funcional, mas um produto de base, e não tem aplicativos móveis.

OnionShare

https://onionshare.org

O OnionShare é um projeto fantástico que roda em qualquer computador desktop e vem embalado com Tails e outros sistemas operacionais. Ele facilita o envio e a recepção de arquivos ou a existência de uma rudimentar sala de bate-papo efêmera sobre o Tor. Ele também é um PCT!

Telegram

O Telegram é basicamente Twitter. Ter uma presença lá pode ser útil em certos cenários, mas não deve ser usado para qualquer comunicação segura e vaza metadados em todos os lugares. Passar mais tempo criticando o Telegram provavelmente não é útil aqui, mas ele não deve ser usado onde a privacidade ou segurança é desejada[xxxviii].

Toxicologia

https://tox.chat

Toxicologia é um projeto semelhante ao Briar e Cwtch, mas não usa Tor - é apenas PE. A Toxicologia pode ser roteada manualmente através do Tor. Nenhum dos aplicativos desenvolvidos para o Tox são particularmente fáceis de usar.

Sessão

https://getsession.org

Vale a pena abordar o Sessão com algum tempo de duração. A dinâmica é de tipo muito libertária-de-livre-palavra-e-ativista. A sessão emprega o protocolo de criptografia robusto do Signal, é peer-to-peer para mensagens diretas e também usa o roteamento Onion para o anonimato (a mesma ideia está atrás do Tor). Entretanto, ao invés do Tor, Session usa sua própria rede de roteamento Onion onde é necessária uma "participação financeira" para executar um nó de serviço para compor a rede Onion. É crucial que esta participação financeira seja na forma de uma moeda criptográfica que é administrada pela fundação que desenvolve o Session. O projeto é interessante do ponto de vista tecnológico, inteligente mesmo, mas é uma solução muito 'web3' envolta em cultura criptográfica.
Apesar de toda sua postura, seus chats de grupo não são construídos para serem terrivelmente resistentes a metadados, e os grandes chats de grupo semipúblicos são apenas hospedados em servidores centralizados (e aparentemente sobrecarregados com criptorapazes de direita). Talvez se a cadeia de bloqueio prevalecer no final, esta será uma boa opção, mas no momento não pode ser

recomendada em boa consciência.

Molly

https://molly.im

Molly é uma versão bifurcada do cliente Signal para Android. Ele ainda usa o Servidor do Signal, mas oferece um pouco mais de segurança e recursos no dispositivo.

Notas e fontes

i. https://itsgoingdown.org/signal-warning-why-moxies-departure-is-not-the-end-of-signal/

ii. Por gancho ou por vigarista.

iii. https://pugetsoundanarchists.org/snitches-sleuths-an-update-from-puget-sound-prisoner-support/

iv. Veja o aplicativo de bate-papo encriptado Anom do FBI honeypot para um exemplo da vida real desta rede www.vice.com/en/article/akgkwj/ operation-trojan-shield-anom-fbi-secret-phone-network

v. https://www.opentech.fund/results/supported-projects/open-whisper-systems/

vi. http://www.wsj.com/articles/moxie-marlinspike-the-coder-who-encrypted-your-texts-1436486274

vii. https://www.rt.com/op-ed/513732-signal-messenger-us-national-security/

viii. https://www.theverge.com/2013/7/17/4517480/ nsa-spying-prism-surveillance-cheat-sheet

ix. https://www.politico.com/news/2022/06/29/ canada-national-police-spyware-phones-00043092

x. https://tails.boum.org/sponsors/index.en.html

xi. Embora o Signal pareça realmente querer mais doações dos usuários, apesar de estar bem posicionado com um empréstimo de US$ 50 milhões. ¯_(ツ)_/¯

xii. Em vez de um único servidor físico, trata-se na verdade de uma enorme rede de servidores alugados em datacenters da Amazon em todos os EUA - isto pode ser abstrato - a um único servidor do Signal para os propósitos de nossa discussão.

xiii. https://signal.org/bigbrother/ eastern-virginia-grand-jury/

xiv. Recentemente, a Signal optou por fazer alguns de seus códigos de servidor de fonte fechada, ostensivamente para permitir-lhes combater o spam na plataforma (ver https://signal.org/blog/keeping-spam-off-signal/). Isto significa que agora existe uma pequena parte do código do Servidor de Signal que não é compartilhada publicamente. Esta mudança também denota um aumento, embora extremamente mínimo, na coleção de metadados do lado do servidor, uma vez que é necessário facilitar o combate eficaz ao spam mesmo de uma forma básica.

Não há razão para suspeitar de crime aqui, mas é importante notar que esta é mais uma decisão política que sacrifica as preocupações de segurança no interesse da experiência do usuário.

xv. https://signal.org/blog/sealed-sender/

xvi. https://signal.org/bigbrother/

xvii. https://signal.org/blog/
a. looking-back-as-the-world-moves-forward/

xviii. https://www.nationalgeographic.com/pages/article/130612-nsa-utah-data-center-storage-zettabyte-snowden

xix. https://www.wired.com/2013/10/nsa-hacked-yahoo-google-cables/

xx. https://theintercept.com/2018/06/25/att-internet-nsa-spy-hubs/

xxi. https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of- cell-phone-location-data

xxii. Para um exemplo, veja esta história sobre jornalistas de investigação católicos que prenderam um padre por usar o Grindr comprando dados da aplicação e tornando-a anônima para identificá-lo: https://www.pillarcatholic.com/p/ pillar-investigates-usccb-gen-sec

xxiii. https://www.youtube.com/watch?v=kV2HDM86XgI (a cotação está na marca dos 18 min)

xxiv. Veja um exemplo, que desde então foi remendado, aqui: https://medium.com/tenable-techblog/turning-signal-app- into-a-coarse-tracking-device-643eb4298447

xxv. Conselho Geral da NSA Stewart Baker.

xxvi. Relatório OONI sobre o atual bloqueio aparente do Signal: https://explorer.ooni.org/search?until=2021-07-13&sin-ce=2021-06-12&test_name=signal&failure=false&only=anomalies

xxvii. Perdoe esta nota estendida sobre números de telefone. Embora o Signal tenha mencionado estar aberto para se afastar de exigir um número de telefone nos tópicos de emissão do GitHub, não houve nenhum tipo de anúncio oficial de que se trata de um recurso em desenvolvimento pesado. Supostamente, um dos problemas com a queda de números de telefone para registro é que ele quebrará a compatibilidade com contas Signal mais antigas devido a como as coisas foram implementadas nos dias TextSecure.

i. Isto é irônico, uma vez que o principal argumento da Moxie contra modelos descentralizados é que ela torna a "movimentação rápida" muito difícil - há muita sobrecarga para implementar novas funcionalidades. E ainda assim o Signal está preso a um problema muito mal alinhado por causa do código legado em torno do registro de contas em um servidor central.

ii. Moxie também explicou que os números de telefone são usados como base de sua identidade em Signal para facilitar o pré-atendimento de seu 'gráfico social'. Ao invés de Signal ter que manter algum tipo de rede social em seu nome, todos os seus contatos são identificados pelo número de telefone deles na lista de endereços de seu telefone, facilitando a manutenção e preservação de sua lista de contatos à medida que você passa de outros aplicativos para Signal, ou se você recebe um novo telefone, ou o que quer que seja. Para Moxie, parece que ter que 'redescobrir' seus contatos periodicamente em qualquer ponto é um inconveniente horrível. Para os anarquistas, deve ser considerado uma vantagem ter que manter intencionalmente nosso 'gráfico social' baseado em nossa afinidade, desejos e confiança. Quem está em nosso 'gráfico social' deve ser algo que estamos constantemente reavaliando e reexaminando por motivos de segurança (ainda confio em todos que têm meu número de telefone de 10 anos atrás) e para encorajar relações sociais intencionais (ainda sou amigo de todos que têm por número de telefone de 10 anos atrás). Trivialidades finais sobre o uso de números de telefone pela Signal: O Signal gasta mais dinheiro na verificação de números de telefone do que eles gastam em custos de hospedagem para o resto do serviço: $1.017.990 USD para o serviço de verificação telefônica do Twillio contra $887.069 USD para o serviço de hospedagem web da Amazon (https://projects.propublica.org/non-profits/display_990/824506840/02_2021_prefixes_81-83%2F824506840_201912_990_2021022217742945).

xxviii. Ou talvez mais precisamente desvinculabilidade: https://code.briarproject.org/briar/briar/-/wikis/FAQ#does-briar-provide-anonymity

xxix. Se você não está familiarizado com o funcionamento do Tor, aqui está um bom vídeo: https://www.youtube.com/watch?v=QRYzre4bf7I

xxx. Dois bons abridores para isso são https://tails.boum.org/doc/about/warnings/tor/index.en.html e https://www.whonix.org/wiki/Why_does_Whonix_use_Tor

xxxi. Tor informa sobre sua situação atual em todo o mundo, indicando onde pode haver interrupções na rede Tor: https://status.torproject.org/

xxxii. https://briarproject.org/raw/BRP-01-report.pdf

xxxiii. O criador de Zcash, um cara selvagem chamado Zooko Wilcox-O'Hearn parece inclinado a garantir que Zcash seja privado, mas não pode ser usado para o crime!

xxxiv. https://openprivacy.ca/blog/2019/12/03/ Incentivizing-Trustlessness-ZcashFoundation-Donation/

xxxv. https://north-shore.info/2019/06/02/signal-fails/

xxxvi. Você tem um momento para falar sobre interoperabilidade e federação? Talvez mais tarde?

xxxvii. Para um grande recurso de compreensão do Protocolo de Signal: https://www.redshiftzero.com/signal-protocol/

xxxviii. https://nitter.net/m_hoppenstedt/status/1532706414635978760#m

contata o autor no Cwtch:
g6px2uyn5tdg2gxpqqktnv7qi2i5frr5kf2dgnyielvq4o4emry4qzid
ou por email: pettingzoo@riseup.net
Publicado em Augusto de 2022

O MOTIM DURA UMA NOITE...

... MAS OS METADADOS DURAM **PARA SEMPRE**

i

ii

iii

iv

v

vi

vii

viii

ix

x

xi

xii

xiii

xiv

xv

xvi

xvii

xviii

xix

xx

xxi

xxii

xxiii

xxiv

xxv

xxvi

xxvii

xxviii

xxix

xxx

xxxi

xxxii

xxxiii

xxxiv

xxxv

xxxvi

xxxvii

xxxviii