COMO MANTER COMUNICAÇÕES PRIVADAS NA ERA DO BIG BROHTER – UM GUIA PRÁTICO

The Saker

RESUMO

Vivemos em tempos complicados e, francamente, perigosos em que a capacidade de manter comunicações seguras é absolutamente crucial para a maior parte das pessoas. Até recentemente, a espécie de tecnologia que podia protegê-las era simplesmente demasiado complexa. Nos dias de hoje podemos utilizar serviços MUITO refinados que não exigem essa espécie de perícia da nossa parte.

RELATÓRIO

Caros amigos:

Decidi partilhar convosco algo que originalmente enviei aos membros chave da comunidade Saker: minha recomendação de como manter privadas suas comunicações na era do "Big Brother", também conhecido como NSA, ECHELON, GCHQ, Unit 8200, etc.

Já há muitos anos tenho estado interessado no tópico da encriptação e no passado utilizei técnicas de encriptação para proteger-me da bisbilhotice de patrões indelicados. Também tem havido algumas discussões no interior da comunidade Saker acerca do que funciona ou não para nós. Cheguei agora à conclusão de que há dois serviços externos que sinto poder recomendar a toda a nossa comunidade, um para emails e outro para a partilha de mensagens/áudio/vídeo/ficheiros. Por que dois serviços diferentes ao invés de um?

A verdade é que as questões de confidencialidade através do email são únicas e exigem uma solução única. Tipicamente, os emails são concebidos para permanecerem em alguma espécie de dispositivo de armazenamento, ao passo que a maior parte dos telefonemas ou conferências de vídeo não o são (pelo menos não pelos participantes).

Vamos examinar as duas questões separadamente

RESUMO: **Se quiser proteger suas comunicações de qualquer espécie de bisbilhotice, incluindo bisbilhotice governamental, a solução mais confiável e avançada actualmente disponível são:**

– Para emails: **Protonmail** https://protonmail.com (gratuito)
– Para mensagens de telefone/vídeo/partilha de ficheiros: o **Silent Phone** , aplicação para Android e iOS https://www.silentcircle.com/products-and-solutions/software/ (US$9,99/mês)

A protecção dos seus emails com Protonmail:

A Protonmail é uma companhia suíça cuja história está bem descrita neste artigo da Wikipedia: https://en.wikipedia.org/wiki/ProtonMail. Não o repetirei aqui. Direi apenas que com o Protonmail sua caixa de correio permanece encriptada de tal maneira que mesmo os administradores e técnicos da empresa não podem ter acesso a ela. Eis alguns vídeos que lhe darão mais pormenores:

Introdução rápida ao ProtonMail e ProtonMail Plus :
https://www.youtube.com/watch?v=HRnQGRaeOy4

ProtonMail – Será o email alternativo que procurávamos?
https://www.youtube.com/watch?v=AxYbrgiCW2E

Protonmail e encriptação – uma nova visita:
https://www.youtube.com/watch?v=jGaHYXC8Gzo

Proteger suas mensagens/telefonemas/vídeos com o Silent Phone da Silent Circle:

Ao contrário do Protonmail que trata APENAS de emails, o software da Silent Circle (chamado "Silent Phone", que pode ser instalado em qualquer smartphone Android ou iOS, protege suas mensagens instantâneas, suas conversações telefónicas (áudio), suas conferências vídeo e permite mesmo enviar com segurança seus ficheiros com dimensão de até 100 MB. Entretanto, apesar de o software Silent Phone ser de descarregamento gratuito, será preciso pagar US$9,99 por mês para obter o que se segue:

- Serviço de voz/mensagens seguras ilimitado a nível mundial entre membros do Silent Circle
- Transferências de ficheiros até 100 MB
- Funcionalidade Full Burn
- Chamada vídeo
- Conferência reunindo até 6 participantes
- Acesso directo ao apoio técnico
- Disponível no iOS, Android e Silent OS

Pode examinar todos os seu materiais de marketing aqui: https://www.silentcircle.com/

Aqui está o artigo da Wikipedia acerca deles: https://en.wikipedia.org/wiki/Silent_Circle_(software)

Este é o link para a sua solução de software: https://www.silentcircle.com/products-and-solutions/software/

E este é o link para o seu Livro Branco: https://www.silentcircle.com/enterprise-cybersecurity-white-paper/

Finalmente, aqui estão alguns dos seus estudos de caso: www.silentcircle.com/wp-

content/uploads/2017/01/SilentCircle_Case-Studies.pdf

Tudo isto é muito ardiloso e poderia ocultar algo, não é? Realmente, não. O que torna a sua oferta interessante é que se baseia exclusivamente em fonte com código aberto que está disponível publicamente. Por que isto é importante? Por duas razões: primeiro, eles não podem esconder alguns alçapões (backdoors) no software. Em segundo lugar, ainda MUITO mais importante, é que os melhores algoritmos de encriptação NÃO são um segredo que ninguém possa verificar, mas sim públicos, abertos a toda gente. Isto é demorado de explicar, mas por favor confiem em mim. O nível de confiança que se pode ter nas tecnologias utilizadas no Silent Phone é tão bom quanto se pode obter. Talvez não perfeito, mas muito próximo disso.

[Se estiver interessado nos pormenores, posso explicar-lhe individualmente porque você SEMPRE deve preferir utilizar apenas tecnologias e encriptação de fontes abertas (pode encontrar aqui os protocolos e algoritmos utilizados pelo Silent Circle: https://www.silentcircle.com/products-and-solutions/technology/zrtp/)]

Note também que tanto o Protonmail como o Silent Circle (a companhia que fabrica a aplicação Silent Phone) estão localizados na Suíça. Isto não é mau uma vez que as leis suíças acerca da privacidade são bastante boas. Entretanto, esta não é a razão porque pode confiar nestes produtos. De facto, no passado a Suíça trabalhou com a CIA dos EUA para vender aos iranianos dispositivos de encriptação com alçapões (backdoors). O actual governo suíço é tão favorável aos EUA quanto qualquer outro. Não, a verdadeira razão porque gosto disto é que a Suíça tem alguns dos melhores criptógrafos do planeta (ainda que muito poucas pessoas saibam disto). De facto, a tecnologia para o Silent Phone é tão segura que mesmo o governo dos EUA teve de certificá-la para utilização governamental (apesar de ser de fonte aberta, o que me diz que eles não têm algo muito melhor): www.zdnet.com/article/silent-circle-phone-app-cleared-for-us-government-use/

Espero que esta referência ao governo estado-unidense não provoque estranheza. Se provocar – descanse. Silent Circule foi co-fundada por Phil Zimmerman, o homem que forçou sozinho o governo dos EUA a abandonar tentativas de manter um monopólio sobre encriptação de grau militar (ler acerca dele aqui: https://en.wikipedia.org/wiki/Phil_Zimmermann).

Aqui está a linha mestra da apresentação de Zimmerman : https://www.youtube.com/watch?v=LI78ttpRdr8

e aqui está um entrevista dele: https://www.youtube.com/watch?v=PvsWRMcxnzI

Por outras palavras, suas credenciais "não trabalho para a NSA" são as melhores do planeta.

Nesta altura, deve estar a perguntar-se se trabalho para a Silent Circle ou se comprei acções da sua companhia. Não se preocupe, não fiz nada disso. Estou a escrever apenas para informá-lo de que penso que este produto é bastante seguro e tem um preço muito razoável. Simplesmente pense nisto – telefonemas ilimitados para o mundo todo (incluindo VÍDEO!) por 10 dólares já é um negócio bastante decente. Mas com encriptação sólida como rocha torna-se mesmo muito bom.

Há uma **importante advertência** que se deve ter em mente: Tanto o Protonmail como o Silent Phone só são verdadeiramente seguros se AMBAS as pessoas que se comunicam estiverem a usá-los (de endereços Protonmail para endereços Protonmail ou de assinante do Silent Phone para assinante do Silent Phone). Além disso, os custos de US$9,99 da assinatura do Silent Phone cobrem todas as comunicações entre assinantes Silent Phone. Você "pode" telefonar para um número não assinante, mas não será seguro e pagará taxas de chamada internacionais.

Além disso, se obtiver Silent Phone, ser-lhe-ão dadas duas opções: a) utilizar apenas um username; b) pagar dois dólares por mês por um número de telefone dedicado. Uma vez que utilizar Silent Phone só faz sentido realmente se for entre dois assinantes Silent Phone, recomendo abster-se do custo extra de um número de telefone dedicado a menos que realmente o necessite (conforme o uso que faz do seu telefone).

Aqui estão alguns vídeos que mostram como o Silent Phone funciona no Android (para iOS ver o canal do YouTube Silent Circle).

Telefonema e conferência telefónica (Calling and Conference calling) : https://www.youtube.com/watch?v=e522oCdVRCU

Registo e configuração (Logging and Setting): https://www.youtube.com/watch?v=sKgAo_Upy5Y

Mensagens (Messaging): https://www.youtube.com/watch?v=J0OCSTA0mNs

Conclusão:

Vivemos em tempos complicados e, francamente, perigosos. Tendo trabalhado pessoalmente em Guerra Electrónica (Electronic Warfare, EW), Inteligência de comunicação (Communication Intelligence, COMINT) e inteligência militar em geral, acredito que a capacidade de manter comunicações seguras é absolutamente crucial para a maior parte das pessoas. Até recentemente, a espécie de tecnologia que podia protegê-lo da bisbilhotice do seu governo (ou da sua empresa) era simplesmente demasiado complexa para ser utilizada pela maior parte das pessoas (ter em mente que má encriptação é muito pior do que nenhuma encriptação uma vez que lhe dá uma ilusão de segurança!). Mesmo um software como o famoso **PGP / GNUpg** não era de uso fácil e exigia um entendimento razoavelmente sólido das tecnologias usadas. Nos dias de hoje somos felizes por podermos utilizar serviços MUITO refinados que não exigem essa espécie de perícia da nossa parte. Mas então, pode-se perguntar, como sabemos que podemos confiar neles? Há duas respostas a isto. Podemos confiar neles porque:

1. Todas as tecnologia utilizadas por estes serviços, incluindo o código fonte, protocolos, algoritmos, etc são plenamente de "fonte aberta", o que significa que elas estão disponíveis para descarregamento e auditoria. Não por si ou por mim, mas por colégios, institutos, corporações e mesmo governos de todo o mundo. Para encriptação isto é o mais alto padrão de segurança: quando todos podem ser o seu código e examiná-lo à procura de viéses.

2. Porque todos estes serviços são regularmente auditado por entidades em confiáveis, tais como a **Electronic Frontier Foundation (EFF)** a qual, por exemplo, fez esta avaliação do Silent Phone:

	Encrypted in transit?	Encrypted so the provider can't read it?	Can you verify contacts' identities?	Are past comms secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
Silent Phone	✓	✓	✓	✓	✓	✓	✓
Silent Text	✓	✓	✓	✓	✓	✓	✓

'.

(Revelação completa: sou membro inscrito tanto da **Electronic Frontier Foundation (EFF)** como da **Free Software Foundation (FSF)**)

Se for um membro activo da Comunidade Saker (autor, investigador, tradutor, técnico em computação, editor, etc) recomendo FORTEMENTE que utilize tanto o Protonmail como o Silent Phone. Se não for membro da nossa comunidade, recomendo que use pelo menos o Protonmail. Se faz numerosas chamadas internacionais para parentes, amigos ou colegas de confiança, também recomendo FORTEMENTE a assinatura do Silent Phone pois por US$9,99 obtém chamadas áudio mundiais ilimitadas e de alta qualidade (telefone) e mesmo vídeo tão boas ou melhores do que o Skype ou Whatsapp. E isto acontece em comunicações tão seguras quanto as melhores de grau governamental/militar.

Finalmente, três pontos finais e menores:

Primeiro: vamos imaginar que alguma agência governamental (suíça, americana ou outra) se dirija à Protonmail ou à Silent Circle e lhes ordene abrirem todas as suas comunicações (como já aconteceu tantas vezes): nem a Protonmail nem a Silent Circle serão capazes de cumprir essa exigência, não devido a má vontade ou alguma heróica resistência à pressão, mas porque essas empresas NÃO TERÃO ACESSO aos seus dados. No caso da sua caixa de correio, ela estará completamente encriptada e só você terá a capacidade de descriptá-la e, no caso do Silent Phone, a encriptação utilizada é entre utilizador final e utilizador final , a qual não é partilhada de qualquer forma com o Silent Circle e no momento em que desliga o telefone também será apagada.

Segundo, a companhia Silent Circle também fabrica um telefone "físico" real, chamado **"Blackphone 2"** . Ele fracassou, não quero ocupar-me dele e não quero discutir as razões para isso, simplesmente ignore essa opção que não trabalha tão bem e apresenta grandes problemas.

Terceiro: quero mencionar algo crucial: **tanto o Protonmail como o Silent Phone apresentam a opção de destruir seus emails após um prazo específico**. Por outras palavras, podem-se configurar estes dois serviços para destruírem tudo o que enviou através deles. Assim, no momento em que alguém tentar obter esses dados eles já se terão desvanecido. Desse modo, apesar de a sua caixa de correio Protonmail estar fortemente encriptada e apesar das chaves de encriptação apenas entre utilizadores finais (p2p) do Silent Phone, você tem esse nível de segurança adicional de ter todos os seus dados auto-destruídos após uma certa data ou período de tempo enviado previamente.

É isso. Favor não me bombardearem com perguntas acerca destas tecnologias e produtos. Se fizer sua própria investigação e seguir todos os links acima deverá obter toda a informação de que precisa. Neste momento não tenho tempo para fazer mais do que partilhar convosco o texto acima. Tenho agora um penoso ataque de gota que me dificulta sentar e teclar. Se ainda tiver perguntas, faça-as na secção de comentários e aqueles tecnicamente mais sábios provavelmente o ajudarão. A comunidade geek chama a isto RTFM ou Read the "French" Manual :-) Assistam também aos vídeos acima, que são muito informativos.

Espero que este texto tenha sido útil e que pelo menos alguns de vocês se decidam a pelo menos tentar estes dois importantes serviços.

18/Maio/2017

O original encontra-se em http://thesaker.is/keeping-communications-private-in-the-age-of-big-brother-a-practical-howto/
Este artigo encontra-se em http://resistir.info/ .