Le chiffrement, maintenant

Comment protéger votre vie privée à l'ère de la surveillance par la NSA

Micah Lee

Une traduction Framalang

Titre original : Encryption Works

Publication originale : https://pressfreedomfoundation.org/encryption-works

Version 1.0 20/10/2013

Ont contribué à cette traduction, par ordre alphabétique de pseudonyme :

Achille Talon, Asta, Audionuma, Bookynette, Calou, Feadurn, Goofy, Lamessen, Lolo, Paul, PeupleLa, Scailyna, Slystone

Sommaire

Préface

Internet est dans un sale état. Tout cassé, fragmenté, explosé en parcelles de territoires dont des géants prédateurs se disputent âprement les lambeaux : Google, Apple, Facebook, Amazon, et tous ceux qui sont prêts à tout pour ravir leur monopole ne voient en nous que des profils rentables et dans nos usages que des consommations. La captation par ces entreprises de nos données personnelles a atteint un degré de sophistication auquel il devient difficile d'échapper.

Mais désormais une autre menace pèse sur tous les usagers du net, celle de la surveillance généralisée. Sans remonter aux années où était révélé et contesté le réseau Echelon, depuis longtemps on savait que les services secrets (et pas seulement ceux des pays de l'Ouest) mettaient des moyens technologiques puissants au service de ce qu'on appelait alors des « écoutes ». Ce qui est nouveau et dévastateur, c'est que nous savons maintenant quelle ampleur inouïe atteint cette surveillance de tous les comportements de notre vie privée. Notre vie en ligne nous permet tout : lire, écrire, compter, apprendre, acheter et vendre, travailler et se détendre, communiquer et s'informer… Mais aucune de nos pratiques numériques ne peut échapper à la surveillance. et gare à ceux qui cherchent à faire d'Internet un outil citoyen de contestation ou de dévoilement : censure politique du net en Chine et dans plusieurs autres pays déjà sous prétexte de lutte contre la pédopornographie, condamnation à des peines disproportionnées pour Manning, exil contraint pour Assange et Snowden, avec la complicité des gouvernements les systèmes de surveillance piétinent sans scrupules les droits fondamentaux inscrits dans les constitutions de pays plus ou moins démocratiques.

Faut-il se résigner à n'être que des *consommateurs-suspects* ? Comment le simple utilisateur d'Internet, qui ne dispose pas de compétences techniques sophistiquées pour installer des contre-mesures, peut-il préserver sa « bulle » privée, le secret de sa vie intime, sa liberté de communiquer librement sur Internet — qui n'est rien d'autre que la forme contemporaine de la liberté d'expression ?

Oui, il est difficile au citoyen du net de s'installer un réseau virtuel privé, un serveur personnel de courrier, d'utiliser TOR, de chiffrer ses messages de façon sûre, et autres dispositifs que les geeks s'enorgueillissent de maîtriser (avec, n'est-ce pas, un soupçon de condescendance pour *les autres*… Souvenez-vous des réactions du type : « — Hadopi ? M'en fous… je me fais un tunnel VPN et c'est réglé »).

Aujourd'hui que *tout le monde* a compris à quelle double surveillance nous sommes soumis, c'est *tout le monde* qui devrait pouvoir accéder à des outils simples qui, à défaut de protéger intégralement la confidentialité, la préservent pour l'essentiel.

Voilà pourquoi une initiative récente de la Fondation pour la liberté de la presse (Freedom of the Press Foundation) nous a paru utile à relayer. **Encryption works** (« le chiffrement, ça marche ») est un petit guide rédigé par Micah Lee (membre actif de l'EFF et développeur de l'excellente

extension HTTPS Everywhere) qui propose une initiation à quelques techniques destinées à permettre à chacun de protéger sa vie privée.

Les contributeurs de Framalang ont traduit pour vous ce petit guide. Répétons-le, il s'agit d'une première approche, et un ouvrage plus conséquent dont la traduction est en cours sera probablement disponible dans quelques mois grâce à Framalang. Mais faisons ensemble ce premier pas vers la maîtrise de notre vie en ligne.

Comment protéger votre vie privée à l'ère de la surveillance par la NSA

> *Le chiffrement, ça marche. Correctement configurés, les systèmes de chiffrement forts font partie des rares choses sur lesquelles vous pouvez compter. Malheureusement, la sécurité des points d'accès est si horriblement faible que la NSA peut la contourner fréquemment.*

— Edward Snowden, répondant en direct à des questions sur le site du Guardian

La NSA est la plus importante et la plus subventionnée des agences d'espionnage que le monde ait pu connaître. Elle dépense des milliards de dollars chaque année dans le but d'aspirer les données numériques de la plupart des gens de cette planète qui possèdent un accès à Internet et au réseau téléphonique. Et comme le montrent des articles récents du Guardian et du Washington Post, même les plus banales communications américaines n'échappent pas à leur filet.

Vous protéger de la NSA, ou de toute autre agence gouvernementale de renseignements, ce n'est pas simple. Et ce n'est pas un problème que l'on peut résoudre en se contentant de télécharger une application. Mais grâce au travail de cryptographes civils et de la communauté du FLOSS, il reste possible de préserver sa vie privée sur Internet. Les logiciels qui le permettent sont librement accessibles à tous. C'est particulièrement important pour des journalistes qui communiquent en ligne avec leurs sources.

Type de menace

La NSA est un puissant adversaire. Si vous êtes sa cible directe, il vous faudra beaucoup d'efforts pour communiquer en toute confidentialité, et même si ce n'est pas le cas, des milliards d'innocents internautes se retrouvent dans les filets de la NSA.

Bien que les outils et conseils présentés dans ce document soient destinés à protéger votre vie privée des méthodes de collecte de la NSA, ces mêmes conseils peuvent être utilisés pour améliorer la sécurité de votre ordinateur contre n'importe quel adversaire. Il est important de garder à l'esprit que d'autres gouvernements, notamment la Chine et la Russie, dépensent d'énormes sommes pour leurs équipements de surveillance et sont réputés pour cibler spécifiquement les journalistes et leurs sources. Aux États-Unis, une mauvaise sécurité informatique peut coûter leur liberté aux lanceurs d'alerte, mais dans d'autres pays c'est leur vie même que risquent à la fois les journalistes et leurs sources. Un exemple récent en Syrie a montré à quel point une mauvaise sécurité informatique peut avoir des conséquences tragiques.

Mais la modification de certaines pratiques de base peut vous garantir une bonne vie privée, même si cela ne vous protège pas d'attaques ciblées par des gouvernements. Ce document passe en revue quelques méthodes qui peuvent

vous servir dans les deux cas.

Systèmes de crypto

> *Nous avons découvert quelque chose. Notre seul espoir contre la domination totale. Un espoir que nous pourrions utiliser pour résister, avec courage, discernement et solidarité. Une étrange propriété de l'univers physique dans lequel nous vivons. L'univers croit au chiffrement.Il est plus facile de chiffrer l'information que de la déchiffrer.*

— Julian Assange, in Menace sur nos libertés : comment Internet nous espionne, comment résister

Le chiffrement est le processus qui consiste à prendre un message textuel et une clé générée au hasard, puis à faire des opérations mathématiques avec ces deux objets jusqu'à ce qu'il ne reste plus qu'une version brouillée du message sous forme de texte chiffré. Déchiffrer consiste à prendre le texte chiffré et sa clé et à faire des opérations mathématiques jusqu'à ce que le texte initial soit rétabli. Ce domaine s'appelle la cryptographie, ou crypto en abrégé. Un algorithme de chiffrement, les opérations mathématiques à réaliser et la façon de les faire, est un ensemble appelé « code de chiffrement ».

Pour chiffrer quelque chose vous avez besoin de la bonne clé, et vous en avez aussi besoin pour la déchiffrer. Si le logiciel de chiffrement est implémenté correctement, si l'algorithme est bon et si les clés sont sécurisées, la puissance de tous les ordinateurs de la Terre ne suffirait pas à casser ce chiffrement.

Nous développons des systèmes de cryptographie qui relèvent de problèmes mathématiques que nous imaginons difficiles, comme la difficulté à factoriser de grands nombres. À moins que des avancées mathématiques puissent rendre ces problèmes moins complexes, et que la NSA les garde cachées du reste du monde, casser la crypto qui dépend d'eux au niveau de la sécurité est impossible.

La conception des systèmes de chiffrement devrait être complètement publique. Le seul moyen de s'assurer que le code de chiffrement ne contient pas lui-même de failles est de publier son fonctionnement, pour avoir de nombreux yeux qui le scrutent en détail et de laisser les experts des véritables attaques à travers le monde trouver les bogues. Les mécanismes internes de la plupart des cryptos que nous utilisons quotidiennement, comme le HTTPS, cette technologie qui permet de taper son code de carte bancaire et les mots de passe sur des formulaires de sites internet en toute sécurité, sont totalement publics. Un attaquant qui connaît parfaitement chaque petit détail du fonctionnement du système de chiffrement ne réussira pas à le casser sans en avoir la clé. En revanche, on ne peut pas avoir confiance dans la sécurité d'une cryptographie propriétaire et dans son code sous-jacent.

Voici une question importante à se poser lors de l'évaluation de la sécurité d'un service ou d'une application qui utilise la crypto : est-il possible pour le service lui-même de contourner le chiffrement ? Si c'est le cas, ne faites pas confiance à la sécurité du service. Beaucoup de services comme Skype et

Hushmail promettent un chiffrement « de bout en bout », mais dans la majorité des cas cela signifie aussi que les services eux-même ont les clés pour déchiffrer le produit. Le véritable chiffrement « de bout en bout » signifie que le fournisseur de service ne peut pas lui-même regarder vos communications, même s'il voulait le faire.

Un aspect important du chiffrement est qu'il permet bien plus que la protection de la confidentialité des communications. Il peut être utilisé pour « signer électroniquement » les messages d'une manière qui permette de prouver que l'auteur du message est bien celui qu'il prétend être. Il peut également être utilisé pour utiliser des monnaies numériques comme Bitcoin, et il peut être utilisé pour produire des réseaux qui permettent l'anonymat comme Tor.

Le chiffrement peut aussi servir à empêcher les gens d'installer des applications pour iPhone qui ne proviennent pas de l'App Store, à les empêcher d'enregistrer des films directement à partir de Netflix ou encore les empêcher d'installer Linux sur une tablette fonctionnant sous Windows 8. Il peut aussi empêcher des attaques de type « homme du milieu » (NdT : attaque consistant à intercepter les communications entre deux terminaux sans que ces derniers se doutent que la sécurité est compromise) d'ajouter des malwares pour compromettre les mises à jour légitimes de logiciels.

En bref, le chiffrement englobe de nombreux usages. Mais ici nous nous contenterons de regarder comment nous pouvons l'utiliser pour communiquer de façon sécurisée et privée.

Des logiciels de confiance ?

Quand Snowden emploie les termes « *endpoint security* », il sous-entend que la sécurité sur les ordinateurs à chaque extrémité de la conversation est assurée par le chiffrement et le déchiffrement, contrairement à la sécurité assurée seulement pendant le transit du message. Si vous envoyez un courriel chiffré à un ami mais que vous avez un enregistreur de frappe sur votre ordinateur qui enregistre aussi bien l'intégralité de votre message que la phrase de passe qui protège votre clé de chiffrement, votre chiffrement n'est plus efficace.

Depuis que Glenn Greenwald et Laura Poitras, deux membres du conseil de la Freedom of the Press Foundation, ont révélé la surveillance généralisée des réseaux par la NSA, de nombreuses informations concernant les agences de renseignement ont été rendues publiques. Particulièrement Bloomberg, qui a publié des révélations sur des programmes volontaires de partage des informations entre les compagnies et les agences d'espionnage étatsuniennes.

Jusqu'à présent, la révélation la plus choquante au sujet de ces programmes de partage des informations, c'est que Microsoft a une politique de communication des informations sur les vulnérabilités dans son logiciel au gouvernement états-unien *avant de publier les mises à jour de sécurité pour le public*. L'article dit :

> Microsoft Corporation, la plus grosse entreprise de logiciels du monde, fournit aux agences d'espionnage des informations sur

> les bogues dans ses logiciels grand public avant d'envoyer un correctif. Ces informations peuvent être utilisées pour protéger les ordinateurs du gouvernement et pour accéder aux ordinateurs de terroristes ou forces militaires ennemies.

Cela signifie que la NSA a en main les clés pour accéder à n'importe quel ordinateur utilisant Windows, Office, Skype ou tout autre logiciel Microsoft. Si vous utilisez ces logiciels sur votre ordinateur, il est très probable que la NSA, avec suffisamment d'efforts, peut compromettre votre ordinateur ainsi que vos communications chiffrées, si vous devenez une de leurs cibles.

Nous avons aussi appris du New York Times que Skype, logiciel qui en dehors de la communauté de la sécurité a longtemps eu la réputation d'être un moyen sécurisé de communiquer, a envoyé des conversations privées au gouvernement états-unien durant les cinq dernières années.

> Skype, le service d'appel sur Internet, a commencé son propre programme secret, intitulé *Project Chess*, pour explorer les problèmes légaux et techniques afin de mettre les appels via Skype à disposition des agences de renseignements et des forces de l'ordre. Cette information vient de gens informés sur le programme qui ont demandé à ne pas être nommés pour éviter les ennuis avec les agences de renseignement.
>
> Le projet *Chess*, qui n'avait jamais été mentionné auparavant, était discret et limité à moins d'une douzaines de personnes chez Skype. L'une des personnes informées sur le projet a expliqué qu'il a été développé suite à des entretiens parfois houleux avec le gouvernement sur des questions juridiques. Il a commencé il y a 5 ans, avant que la majorité de la société ne soit vendue par son propriétaire, eBay, à des investisseurs externes en 2009. Microsoft a acquis Skype dans un accord de 8.5 milliards de dollars (environ 6.5 milliards d'euros) qui s'est conclu en octobre 2011.
>
> Un responsable de Skype a nié l'année dernière dans un article de blog que les récents changements dans le fonctionnement de Skype aient été faits à la demande de Microsoft pour faciliter l'application de la loi sur l'espionnage. Cependant, il semble que Skype ait compris comment collaborer avec les agences de renseignements avant même que Microsoft n'en prenne le contrôle, comme le dévoilent les documents divulgués par Edward J. Snowden, un ancien sous-traitant de la C.I.A. L'un des documents sur le programme PRISM qu'il a rendu public indique que Skype a rejoint le programme le 6 février 2011.

Les logiciels propriétaires, comme la majorité de ceux proposés par Microsoft, Apple et Google, ont une autre faille. Il est beaucoup plus difficile pour les utilisateurs de vérifier de façon indépendante qu'il n'existe pas de portes dérobées secrètes à la demande clandestine de la surveillance d'état. Bien que des rapports récents aient montré que de nombreuses sociétés ont

remis une quantité inconnue d'informations en réponse aux requêtes FISA, aucune de ces entreprises ne s'est avérée avoir *directement* de portes dérobées dans leurs systèmes.

Il existe un autre type de logiciel qui est plus fiable à cet égard. Les logiciels libres et open source ne sont pas forcément ergonomiques ? et ne sont pas nécessairement sans risques ? Cependant quand ils sont développés de façon ouverte, avec un logiciel de suivi de bogue ouvert, des listes de diffusion ouvertes, une architecture ouverte et un code *open source*, il est plus difficile pour ces projets d'avoir une politique de trahison de leurs utilisateurs comme celle de Microsoft.

GNU/Linux est un système d'exploitation qui est entièrement composé de logiciels libres et *open source*. On peut prendre l'exemple de distributions GNU/Linux comme Ubuntu, Debian ou Fedora, qui sont les alternatives à Windows et Mac OS X les plus courantes. Bien que les projets de logiciels libres puissent toujours intégrer du code malveillant (voir le concours C Underhanded), la personne qui écrit ce code doit le cacher proprement et espérer qu'aucun des autres développeurs ou en aval des packagers GNU/Linux qui préparent et compilent le code source du projet pour l'intégrer à leur distribution ne le détectent.

Dans les années 1990, quand le chiffrement public est devenu populaire et que le gouvernement étatsunien faisait tout ce qu'il pouvait pour l'empêcher, le mouvement « cypherpunk » est né. De nombreux logiciels permettant aux gens de chiffrer sont nés de ce mouvement.

> Les cypherpunks écrivent du code. Nous savons que quelqu'un doit développer des logiciels pour défendre notre vie privée. Et comme nous ne pouvons pas avoir de vie privée tant que nous ne le feront pas tous, nous allons les développer. Nous publions notre code pour que nos compatriotes cypherpunks puissent s'entraîner et jouer avec. Notre code est utilisable librement par n'importe qui dans le monde. Nous n'en avons rien à faire que vous n'approuviez pas le logiciel que nous développons. Nous savons que le logiciel ne peut être détruit et qu'un système largement dispersé ne peut être stoppé.

— Eric Hughes, dans son *Manifeste du Cypherpunk* de 1993

Ce code, qui est ouvert et public de façon à ce que d'autres cypherpunks puissent s'entraîner et jouer avec, que n'importe qui dans le monde peut utiliser librement, est à l'origine des logiciels et protocoles dans lesquels nous pouvons avoir confiance : LUKS (le chiffrement de disque intégré à GNU/Linux), OpenPGP, Off-the-Record et Tor.

Le collectif de technologie tactique a conçu un très bon guide sur les logiciels de sécurité open source dans lesquels on peut avoir confiance pour préserver notre vie privée de toute surveillance. Il est important de rappeler que la simple utilisation de ces logiciels, même à la perfection, ne peut pas garantir la sécurité de votre chiffrement. Nous ne savons pas, par exemple, si Apple a transmis des failles 0-day de iOS à la NSA comme a pu le faire Microsoft. ChatSecure, qui permet d'avoir des discussions chiffrées sur les terminaux iOS, n'est pas plus sécurisé que le système d'exploitation sur lequel il

fonctionne.

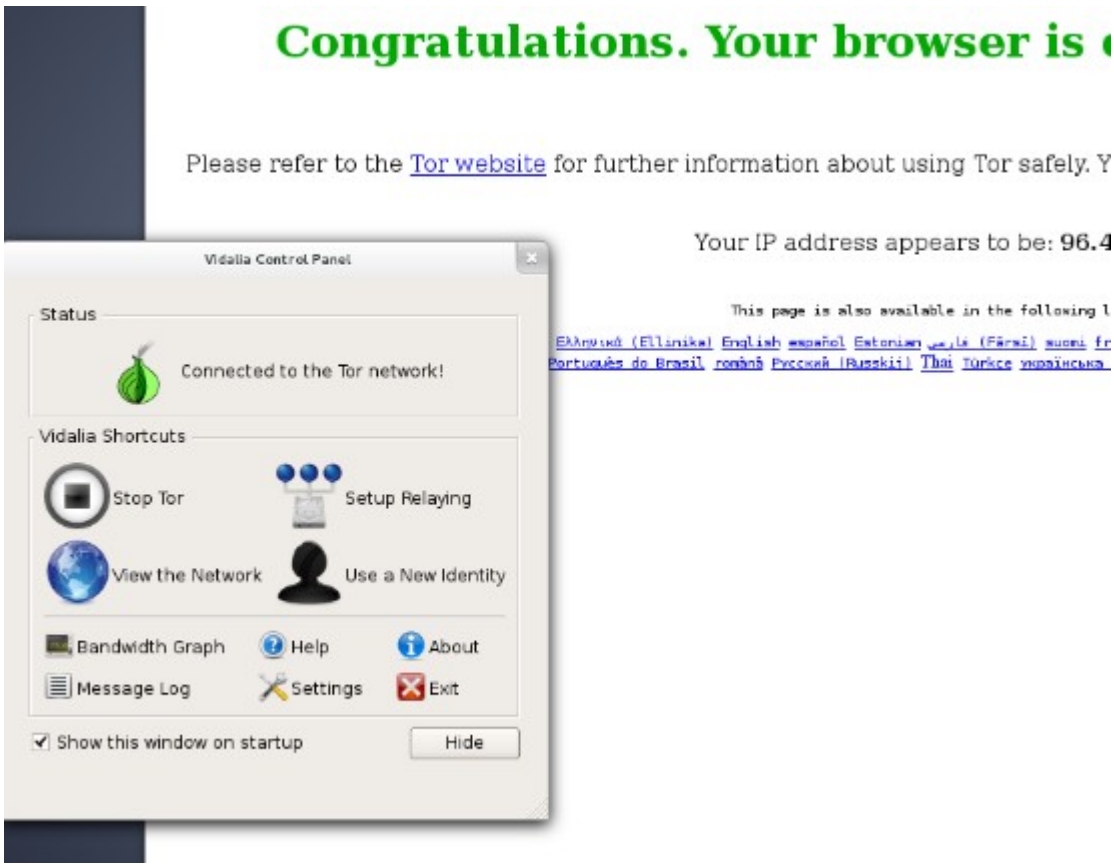
Il est important de rappeler que le simple fait d'utiliser du logiciel libre ne veut pas dire que l'on ne peut pas s'introduire dans vos systèmes. Des gens trouvent tout le temps des failles 0-day pour du logiciel libre, et parfois les vendent à des gouvernements ou d'autres attaquants malveillants. Des utilisateurs de logiciels libres téléchargent toujours des pièces jointes malveillantes avec leurs courriels, et ils ont souvent mal configuré des services simples sur leurs ordinateurs. Pire encore, les malwares sont souvent très bons pour se dissimuler. Si un utilisateur de logiciel libre attrape sur son ordinateur un malware, ce dernier peut y demeurer jusqu'à ce que l'utilisateur formate ses disques durs. Tails, qui est une distribution GNU/Linux bootable sur live USB et live CD et dont il sera question plus loin, résout beaucoup de ces problèmes.

Anonymisez votre localisation avec Tor

Tor est un service logiciel qui vous permet d'utiliser Internet en dissimulant votre adresse IP, qui constitue, en général, une représentation assez précise de votre localisation. Le réseau Tor est composé de 3600 serveurs, maintenus par des bénévoles, appelés nœuds. Quand quelqu'un utilise le réseau Tor pour visiter un site, sa connexion est relayée à travers trois de ces nœuds (appelé circuit) avant de finalement accéder à l'Internet normal. Quiconque interceptera le trafic pensera que votre emplacement est le nœud final duquel sort votre trafic. Il est important toutefois de se souvenir que le fait d'anonymiser votre connexion à Internet ne la rend pas magiquement sécurisée. EFF a créé un schéma interactif montrant comment Tor et le HTTPS peuvent travailler ensemble pour protéger votre vie privée. Comme tout bon logiciel de cryptographie, Tor est un logiciel libre, avec un logiciel de suivi de bogues ouvert, des listes de diffusion et un code source disponible. La documentation de Tails, la distribution live GNU/Linux qui force tout le trafic du réseau de l'utilisateur à passer par le réseau Tor, dit ceci à propos des adversaires globaux :

> Un adversaire passif serait une personne ou une entité capable de surveiller le trafic entre tous les ordinateurs d'un même réseau simultanément. En étudiant, par exemple, la synchronisation et le volume de données des différentes communications sur le réseau, il pourrait être possible d'identifier les circuits Tor et ainsi identifier les utilisateurs de Tor et les serveurs de destination.

On peut considérer que la NSA et la GHCQ comptent parmi les adversaires globaux, car nous savons qu'ils surveillent une large portion d'Internet. On ne peut savoir de manière sûre à quelle fréquence ces agences de renseignement peuvent mettre en échec l'anonymat du réseau Tor. Récemment, le réseau Tor a fait l'objet d'une attaque par Botnet. Il est probable que la guerre contre le chiffrement a déjà commencé.



Même si cela leur est possible, utiliser Tor nous procure toujours plusieurs avantages. Cela rend leur travail plus difficile, et nous laissons moins de données nous identifiant sur les serveurs par lesquels nous nous connectons au réseau Tor. Cela rend une attaque MITM plus difficile dans notre réseau local ou au niveau de notre fournisseur d'accès à internet (FAI). Et même si certains circuits Tor peuvent être infiltrés par un adversaire global, si suffisamment de personnes font transiter leur trafic par le même nœud Tor au même moment, il sera difficile pour l'adversaire de dire quel trafic correspond à quel circuit.Le moyen le plus simple pour utiliser Tor est de télécharger et d'installer le Tor Browser Bundle. Des informations détaillées sur l'installation et la configuration de Tor selon votre système d'exploitation figurent sur le site du projet Tor. Elles sont malheureusement en anglais. Vous trouverez une documentation en français pour Ubuntu sur cette page.

Lorsque Snowden a répondu aux questions sur le site du Guardian depuis une « connexion sécurisée à Internet », il routait probablement son trafic par le réseau Tor. Il peut avoir également eu recours à un « pont » pour se connecter au réseau Tor afin de rendre le fait qu'il utilise Tor à partir de son adresse IP moins évident pour les oreilles indiscrètes.

Un service de chat furtif : Off-the-Record (OTR)

Off-the-Record (OTR) est une couche de chiffrement qui peut être ajoutée à n'importe quel système de messagerie instantanée existant, pourvu que vous puissiez vous connecter à cette messagerie instantanée avec un client qui prend en charge l'OTR, comme Pidgin ou Adium. Avec OTR, il est possible

d’avoir des conversations sécurisées, chiffrées de bout en bout, en passant par des services comme Google Talk ou Facebook sans que ni Facebook ni Google n’aient accès au contenu de ces conversations. Notez bien que c’est un système différent de l’option « off the record » de Google, qui n’est pas sécurisée. Et souvenez-vous : bien qu’une connexion HTTPS avec Google ou Facebook offre une très bonne protection à vos messages quand ils circulent, les deux services ont les clés de vos échanges et peuvent donc les communiquer aux autorités.

OTR remplit deux missions : le chiffrement des conversations de messagerie instantanée en temps réel et la vérification de l’identité des personnes avec lesquelles vous communiquez. Cette dernière est extrêmement importante mais beaucoup d’utilisateurs d’OTR la négligent. Même si OTR est bien plus facile à prendre en main que d’autres formes de chiffrement à clé publique, vous devez malgré tout en comprendre le fonctionnement et savoir à quelles attaques il peut être exposé si vous souhaitez l’utiliser en toute sécurité.

Fournisseurs de services et Jabber

OTR assure uniquement le chiffrement du contenu de vos conversations et non celui des métadonnées qui leur sont associées. Celles-ci comprennent vos interlocuteurs, quand et à quelle fréquence vous communiquez avec eux. C’est la raison pour laquelle je recommande d’utiliser un service qui n’est pas connu pour collaborer avec les services secrets. Cela ne protègera pas forcément vos métadonnées, mais vous aurez au moins une chance qu’elles restent privées.

Je vous conseille aussi d’utiliser un service XMPP (aussi appelé Jabber). Tout comme le courrier électronique, Jabber est un protocole ouvert et fédéré. Les utilisateurs d’un service Jabber comme riseup.net peuvent discuter tant avec des utilisateurs du service jabber.ccc.de qu’avec ceux du service jabber.org.

Clients OTR

Pour utiliser OTR, vous devrez télécharger un logiciel. Sous Windows, vous téléchargerez et installerez Pidgin et le plugin OTR séparément. Sous GNU/Linux, vous installerez les paquets pidgin et pidgin-otr. La documentation explique comment configurer vos comptes Pidgin avec OTR. Si vous êtes sous Mac OS X, vous pouvez télécharger et installer Adium, un client de chat libre qui intègre le support d’OTR. Là aussi, reportez vous à la documentation officielle pour configurer le chiffrement OTR avec Adium. Il existe aussi des clients Jabber et OTR disponibles pour Android (Giggerbot) et pour iOS (ChatSecure).

Votre clé

Quand vous commencez à utiliser OTR, votre client de chat génère une clé de chiffrement et la stocke dans un fichier de votre répertoire utilisateur personnel sur votre disque dur. Si votre ordinateur ou votre smartphone est perdu, volé ou rendu inutilisable par un logiciel malveillant, il est possible que l’inviolabilité de votre clé OTR soit compromise. Si c’est le cas, un attaquant aura la possibilité de prendre le contrôle de votre serveur Jabber et

de lancer une attaque de l'homme du milieu (MIDTM) contre vous pendant que vous discutez avec des interlocuteurs qui avaient auparavant vérifié votre identité.

Sessions

Si vous souhaitez utiliser OTR pour discuter en privé avec vos amis, ces derniers doivent l'utiliser également. Une session chiffrée entre deux personnes nécessite deux clés de chiffrement. Par exemple, si vous-même et votre correspondant vous êtes tous deux identifiés sur le chat de Facebook en utilisant Adium ou Pidgin après avoir configuré OTR, vous pourrez discuter en privé. En revanche, si vous vous êtes logué en messagerie instantanée en utilisant Adium ou Pidgin mais que votre interlocuteur discute en utilisant directement facebook.com, vous ne pouvez pas avoir de conversation chiffrée.

Si vous souhaitez utiliser les services de Facebook ou Google pour discuter avec vos amis, je vous recommande de désactiver le chat de l'interface web pour ces services et de n'utiliser qu'Adium ou Pidgin pour vous connecter, et d'encourager vos amis à faire de même ; voici la marche à suivre pour Facebook et Google.

Quand vous lancez une session chiffrée avec OTR, votre logiciel client vous indique quelque chose comme :

```
Lancement d'une conversation privée avec
utilisateur@jabberservice...
Conversation non-vérifiée avec
utilisateur@jabberservice/démarrage du client chat.
```

Si vous avez déjà vérifié l'empreinte OTR de la personne à laquelle vous parlez (voir plus bas), votre session ressemblera à ceci :

```
Lancement d'une conversation privée avec
utilisateur@jabberservice...
Conversation privée avec
utilisateur@jabberservice/démarrage du client chat.
```

Quand vous commencez une nouvelle session OTR, votre logiciel OTR et celui de votre correspondant s'échangent une série de messages pour s'accorder sur une clé pour la nouvelle session. Cette clé temporaire n'est connue que par vos deux clients de messagerie instantanée, ne circule jamais sur Internet et sert à chiffrer et déchiffrer les messages. Une fois la session terminée, les deux logiciels clients « oublient » la clé. Si vous recommencez à chatter plus tard avec la même personne, votre client OTR génèrera une nouvelle clé de session.

De cette façon, même si une personne indiscrète enregistre toutes vos conversations chiffrées — ce que la NSA pense être légalement autorisée à faire même si vous êtes un citoyen étatsunien et qu'elle n'a pas un mandat ou une bonne raison de le faire — et que plus tard elle compromet votre clé OTR, elle ne pourra pas retrouver ni déchiffrer vos anciennes conversations.

Cette propriété est appelée sécurité *itérative*, et c'est une particularité d'OTR dont PGP ne dispose pas. Si votre clé PGP privée (article à venir sur les clés

PGP) est compromise et que l'attaquant a eu accès à tous les messages chiffrés que vous avez reçus, il peut les retrouver et en déchiffrer l'intégralité.

Apprenez-en davantage sur la façon dont fonctionne la sécurité itérative, et la raison pour laquelle la majorité des grandes sociétés d'Internet devraient l'adopter pour leurs site web ici. La bonne nouvelle, c'est que Google utilise déjà la sécurité itérative et que Facebook va l'implémenter dès que possible.

Vérification d'empreinte OTR

Quand vous commencez une nouvelle session OTR avec quelqu'un, votre logiciel de chat reçoit une empreinte[1] de sa clé de chiffrement et votre logiciel OTR se souvient de cette empreinte. Aussi longtemps que la personne utilise la même clé de chiffrement lorsqu'elle communique avec vous, probablement parce qu'elle utilise le même logiciel, elle aura la même empreinte. Si cette empreinte change, c'est soit parce que la personne utilise une clé OTR différente, soit que vous êtes tous deux victimes d'une attaque MITM.

Sans cette vérification de clés, vous n'avez aucun moyen de savoir si vous êtes victime d'une attaque MITM réussie et non détectée.

Même en étant sûr que la personne avec qui vous discutez est réellement votre interlocuteur, parce qu'elle connaît des choses qu'elle seule peut connaitre, et en utilisant un chiffrement OTR, un attaquant peut être en train de lire votre conversation. Peut-être avez vous en réalité une conversation chiffrée avec l'attaquant, lui-même en pleine conversation chiffrée avec votre interlocuteur, relayant les messages entre vous et ce dernier. Au lieu de l'empreinte de votre interlocuteur, votre client verra celle de l'attaquant. Tout ce que vous pouvez constater en tant qu'utilisateur est que la conversation est « non vérifiée ».

Les captures d'écran suivantes montrent les indications visuelles de Pidgin concernant la vérification de l'empreinte. Si vous avez vérifié l'empreinte OTR, votre discussion est privée : dans le cas contraire, votre conversation est chiffrée mais rien ne garantit que vous n'êtes pas en train de subir une attaque. Vous ne pouvez en avoir la certitude absolue qu'à la condition de vérifier.

Si vous cliquez sur un lien non vérifié (sur Adium c'est une icône de cadenas), vous pouvez choisir « authentifier l'ami ». Le protocole OTR propose trois méthodes de vérification : le protocole du millionnaire socialiste, le secret partagé et la vérification manuelle de l'empreinte. Tous les clients OTR permettent la vérification manuelle de l'empreinte, mais pas forcément les autres types de vérification. Dans le doute, choisissez la vérification manuelle de l'empreinte.

Dans la capture d'écran ci-dessus, on voit l'empreinte OTR des deux utilisateurs de la session. Votre interlocuteur doit voir exactement les mêmes empreintes que vous. Pour être certain que chacun des interlocuteurs voit les mêmes empreintes, vous devez soit vous rencontrer en personne, soit avoir un échange téléphonique (si vous pouvez reconnaître vos voix) soit trouver une autre solution en-hors du chat mais sécurisée pour vérifier les empreintes, comme envoyer un courriel PGP chiffré et signé.

Les empreintes OTR sont constituées d'une suite de 40 caractères hexadécimaux. Il est statistiquement impossible de générer deux clés OTR ayant la même empreinte, ce qui est appelé une collision. Il est toutefois possible de générer une clé OTR qui, sans être véritablement une collision,

semble en être une lors d'une vérification superficielle. Par exemple, les premiers et derniers caractères peuvent identiques et les caractères centraux différents. Il est donc important de comparer chacun des 40 caractères un à un pour être sûr d'avoir la bonne clé OTR.

Comme, en général, vous créez une nouvelle clé OTR chaque fois que vous utilisez un nouveau terminal (par ex., si vous voulez utiliser le même compte Jabber pour discuter à partir de votre téléphone Android avec Gibberbot et à partir de votre PC Windows avec Pidgin), vous vous retrouvez souvent avec plusieurs clés et, par conséquent, plusieurs empreintes. Il est important de répéter l'étape de vérification sur chaque terminal et pour chaque contact avec qui vous discutez.

Utiliser OTR sans vérifier les empreintes est toujours préférable à ne pas utiliser OTR du tout. Comme un attaquant qui tente une attaque MITM contre une session OTR court un risque important d'être pris, cette attaque n'est utilisée qu'avec prudence.

Journaux d'activité

Voici un extrait d'un des journaux de discussion entre Bradley Manning et Adrian Lamo, transmis aux autorités par ce dernier et publié par Wired.

```
(1:40:51 PM) bradass87 n'a pas encore été identifié. Vous
devez authentifier cet utilisateur.

(1:40:51 PM) une conversation non vérifiée avec bradass87
a commencé.

(1:41:12 PM) bradass87: Salut

(1:44:04 PM) bradass87: Comment vas-tu?

(1:47:01 PM) bradass87: je suis analyste du renseignement
à l'armée, à l'est de Bagdad et dans l'attente d'une
décharge pour « trouble de l'adaptation » au lieu de «
trouble de l'identité de genre ».

(1:56:24 PM) bradass87: Je suis sûr que tu es très
occupé... Tu dois avoir plein de boulot...

(1:58:31 PM) bradass87: Si tu avais un accès privilégié à
des réseaux classifiés 14 heures par jour, 7 jours sur 7
et plus de 8 mois dans l'année, que ferais-tu ?

(1:58:31 PM) info@adrianlamo.com: je suis fatigué d'être
fatigué

(2:17:29 PM) bradass87: ?

(6:07:29 PM) info@adrianlamo.com: Quel est ton MOS[2]
```

Comme on peut le voir grâce à la ligne « une conversation non vérifiée avec bradass87 a commencé », les deux interlocuteurs utilisaient OTR pour chiffrer leur conversation, or cette dernière a été en définitive rendue publique sur le site web de Wired et utilisée comme pièce à conviction contre Bradley Manning. Il est possible que leur conversation ait fait l'objet d'une attaque MITM, mais c'est très improbable. Ce sont plutôt les clients OTR de Bradley Manning et Adian Lamo qui conservaient une copie de leur conversation sur leur disque dur, non chiffré.

Même s'il peut parfois être utile de garder des journaux de conversations, cela peut aussi gravement mettre en danger votre vie privée. Si Pidgin et

Adium ne journalisaient pas les conversations par défaut, il est probable que ces journaux de conversations n'auraient pas fini sur la place publique.

Avec la sortie d'OTR 4.0 en septembre 2012, Pidgin a arrêté de journaliser les conversations OTR par défaut. Adium continue de le faire. Vous devez donc manuellement arrêter cette journalisation, ce qui est une faille d'Adium. Adium étant un logiciel libre avec un système ouvert de suivi de bogues, vous pouvez suivre et participer aux discussions concernant la résolution de cette faille ici et là.

Notes

[1] rien à voir avec les empreintes digitales que certains confient à leur iPhone

[2] Military Occupation Speciality, la classification des activités au sein de l'armée des États-Unis.

Le chiffrement du courriel avec PGP (Pretty Good Privacy)

En 1991, Phil Zimmermann a développé un logiciel de chiffrement des courriels qui s'appelait PGP, destiné selon lui aux militants anti-nucléaires, pour qu'ils puissent organiser leurs manifestations.

Aujourd'hui, PGP est une entreprise qui vend un logiciel de chiffrement propriétaire du même nom. OpenPGP est le protocole ouvert qui définit comment fonctionne le chiffrement PGP, et GnuPGP (abrégé en GPG) est le logiciel libre, 100% compatible avec la version propriétaire. GPG est aujourd'hui beaucoup plus populaire que PGP parce que tout le monde peut le télécharger gratuitement, et les cyberphunks le trouvent plus fiable parce qu'il est *open source*. Les termes PGP et GPG sont fréquemment employés l'un pour l'autre.

Malheureusement, PGP est notoirement difficile à utiliser. Greenwald en a donné l'exemple quand il a expliqué qu'il ne pouvait pas dans un premier temps discuter avec Snowden parce que PGP était trop difficile à installer.

Paires de clés et trousseaux

Comme pour l'OTR, chaque utilisateur qui souhaite envoyer ou recevoir des messages chiffrés doit générer sa propre clé PGP, appelée paire de clés. Les paires de clés PGP sont en deux parties, la clé publique et la clé privée (secrète).

Si vous disposez de la clé publique de quelqu'un, vous pouvez faire deux choses : chiffrer des messages qui ne pourront être déchiffrés qu'avec sa clé privée, et vérifier les signatures qui sont générées avec sa clé secrète. On peut donner sans problème sa clé publique à tout le monde. Le pire qu'on puisse faire avec est de chiffrer des messages que vous seul pourrez déchiffrer.

Avec votre clé privée vous pouvez faire deux choses : déchiffrer des messages qui ont été chiffrés avec votre clé publique et ajouter une signature

numérique pour vos messages. Il est très important que votre clé privée reste secrète. Un attaquant disposant de votre clé privée peut déchiffrer des messages qui ne sont destinés qu'à vous et peut fabriquer de faux messages qui auront l'air de venir de vous. Les clés privées sont généralement chiffrées avec une phrase secrète, donc même si votre ordinateur est compromis et que votre clé privée est volée, l'attaquant devra obtenir votre phrase secrète avant de pouvoir l'utiliser. Contrairement à OTR, PGP n'utilise pas la sécurité itérative. Si votre clé PGP privée est compromise et que l'attaquant dispose de copies de courriels chiffrés que vous avez reçus, il pourra donc tous les déchiffrer.

Comme vous avez besoin des clés publiques des autres personnes pour chiffrer les messages à leur intention, le logiciel PGP vous laisse gérer un trousseau de clé avec votre clé publique et celles de tous les gens avec qui vous communiquez.

Utiliser PGP pour le chiffrement des courriels peut s'avérer problématique. Par exemple, si vous configurez PGP sur votre ordinateur mais que vous recevez un courriel chiffré sur votre téléphone, vous ne pourrez pas le déchiffrer pour le lire avant d'être de retour sur votre ordinateur.

Comme OTR, chaque clé PGP possède une empreinte unique. Vous pouvez trouver une copie de ma clé publique ici, et mon empreinte est 5C17 6163 61BD 9F92 422A C08B B4D2 5A1E 9999 9697. Si vous jetez un coup d'œil à ma clé publique, vous allez voir qu'elle est très longue et qu'il sera difficile de la lire sur un téléphone. Une empreinte est une version plus courte et moins contraignante de représenter une clé de manière unique. Avec ma clé publique, vous pouvez chiffrer des messages que je serais seul à pouvoir déchiffrer, tant que ma clé privée n'a pas été compromise.

Phrases secrètes

La sécurité de la crypto repose souvent sur la sécurité d'un mot de passe. Comme les mots de passes sont très facilement devinés par les ordinateurs, les cryptographes préfèrent le terme phrase secrète pour encourager les utilisateurs à créer leurs propres mots de passe, très long et sécurisés.

Pour obtenir des conseils sur la façon de choisir de bonnes phrases secrètes, consultez la section phrase secrète du livre blanc de l'EFF (NdT : Electronic Frontier Foundation, http://www.eff.org) "Défense de la vie privée aux frontières des USA : un guide pour les voyageurs qui transportent des terminaux numériques". Voyez aussi la page d'accueil de Diceware Passphrase.

Mais protéger vos clés privées PGP ne suffit pas : vous devez aussi choisir de bonnes phrases secrètes pour le chiffrement de vos disques et trousseaux de mots-de-passe.

Logiciels

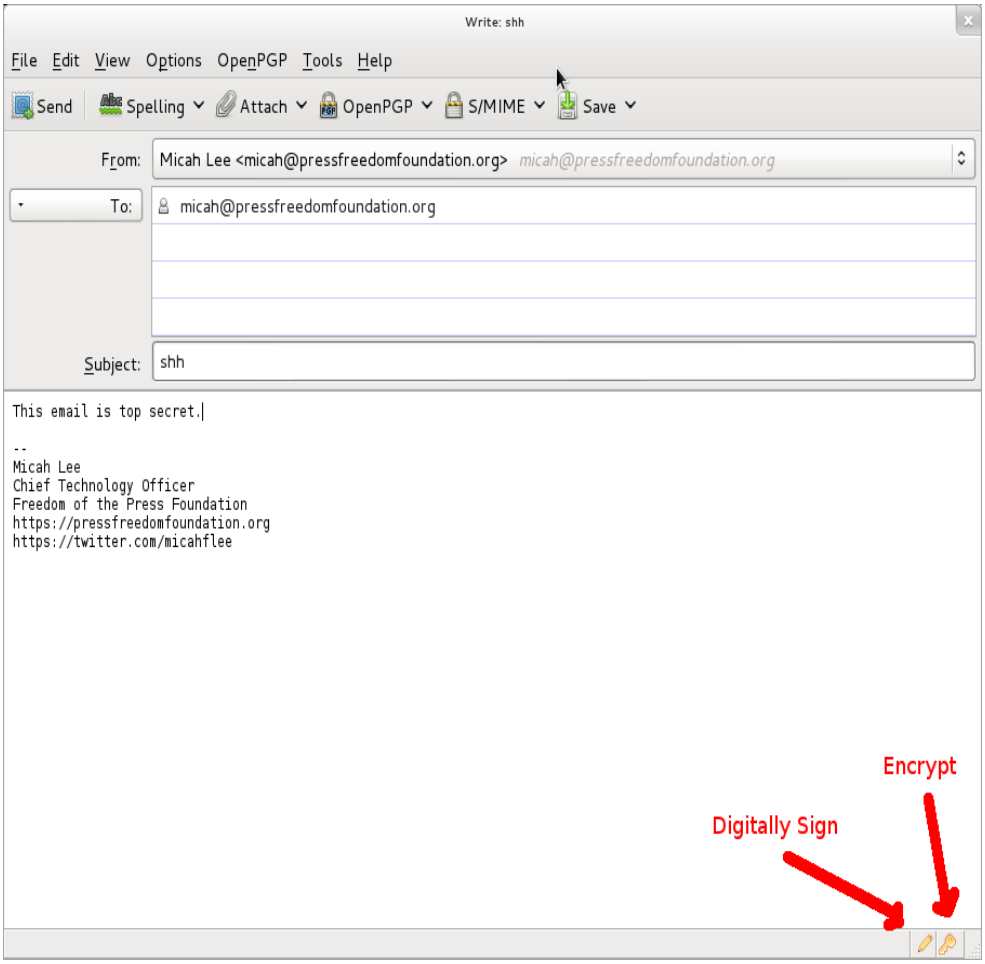
Pour installer GPG, les utilisateurs de Windows peuvent télécharger Gpg4win, et les utilisateurs de Mac OS X GPGTools. Si vous utilisez GNU/Linux, GPG est probablement déjà installé. GPG est un programme en

ligne de commande, mais il y a des logiciels qui s'interfacent avec les clients de messagerie, pour une utilisation simplifiée.

Vous devrez télécharger un client messagerie pour utiliser PGP correctement. Un client de messagerie est un programme sur votre ordinateur que vous ouvrez pour vérifier vos courriels, contrairement à l'utilisation de votre navigateur web. La configuration PGP la plus populaire est le client de messagerie Thunderbird accompagné de l'add-on Enigmail. Thunderbird et Enigmail sont des logiciels libres disponibles sur Windows, Mac et GNU/Linux.

À l'heure actuelle, PGP est très difficile à utiliser de façon sécurisée à partir d'un navigateur web. Bien que quelques extensions de navigateurs existants puissent aider à le faire, je recommande de passer par un client de messagerie de bureau jusqu'à ce que le domaine de la crypto de navigateur mûrisse. Il est possible d'utiliser un chiffrement PGP avec Gmail, mais la façon la plus simple est de passer par un client de messagerie comme Thunderbird et de configurer votre compte Gmail à travers lui.

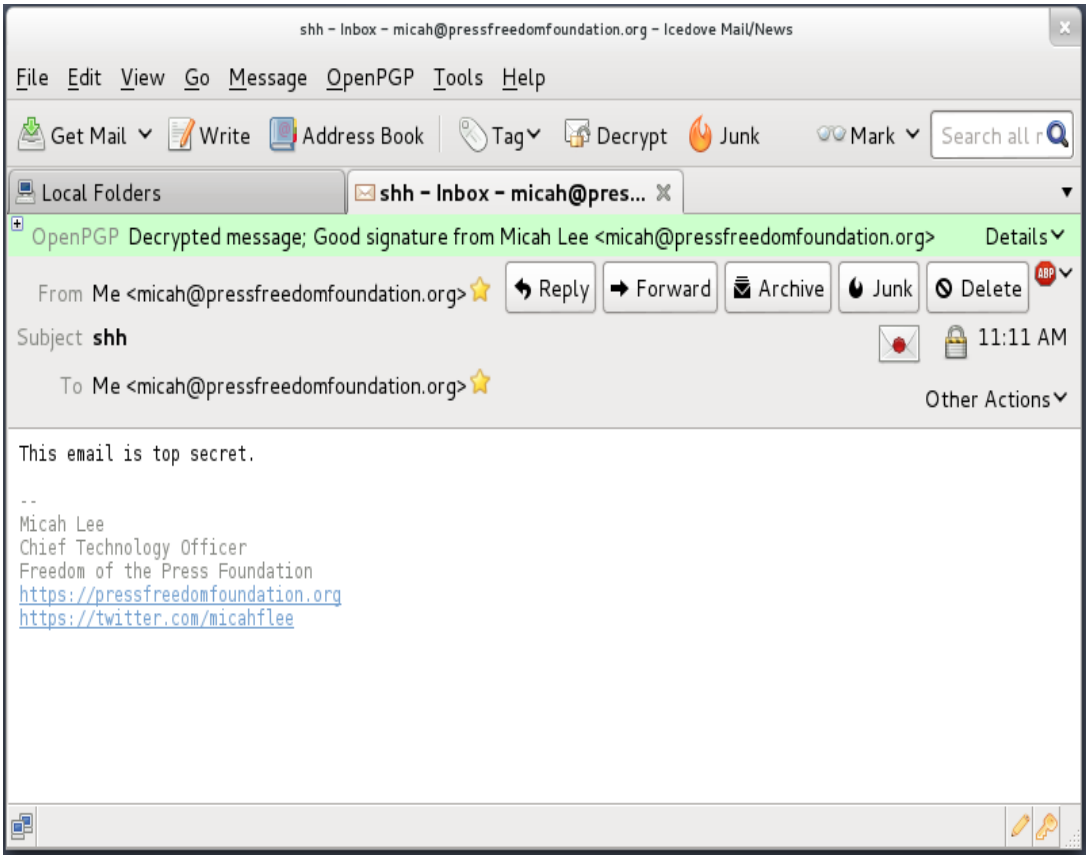
Chiffrement, déchiffrement, et signatures



Vous pouvez envoyer des courriels chiffrés et les signer numériquement en utilisant une interface utilisateur graphique via Thunderbird et Enigmail. Voici un exemple de courriel chiffré que je m'envoie à moi-même.

Quand je clique sur envoyer, mon logiciel prend le corps du message et le

chiffre en utilisant ma clé publique, rendant son contenu incompréhensible pour les oreilles indiscrètes, y compris mon fournisseur de courriel.



Quand j'ai ouvert ce courriel, j'ai dû entrer ma phrase secrète de chiffrement pour le déchiffrer. Comme je l'avais chiffré en utilisant ma clé publique, le seul moyen que j'ai de le déchiffrer est d'utiliser ma clé privée. Comme ma clé privée est protégée par une phrase secrète, j'ai eu besoin de la taper pour déchiffrer temporairement ma clé privée qui est alors utilisée pour déchiffrer le message.

PGP n'est pas limité aux courriels

Bien que PGP soit principalement utilisé pour chiffrer les courriels, rien ne vous empêche de l'utiliser pour chiffrer autre chose et le publier en utilisant n'importe quel support. Vous pouvez poster des messages chiffrés sur les blogs, les réseaux sociaux et les forums.

Kevin Poulsen a publié un message PGP chiffré sur le site web de Wired à l'attention d'Edward Snowden. Aussi longtemps que Wired aura une copie de la vrai clé publique de Snowden, seul quelqu'un en possession de la clé privée de Snowden pourra déchiffrer ce message. Nous ne savons pas comment Wired a obtenu une copie de cette clé publique.

Voici un message qui a été chiffré avec ma clé publique. Sans avoir accès à ma clé privée associée, la NSA ne sera pas en mesure de casser ce chiffrage (chère NSA, faites-moi savoir si vous avez réussi à le faire).

```
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.12 (GNU/Linux)
hQIMA86M3VXog5+ZAQ//Wep9ZiiCMSmLk/Pt54d2wQk07fjxI4c1rw+jfkKQAi4n6HzrX
9YIbgTukuv/0Bjl+yp3qcm22n6B/mk+P/3Cbxo+bW3gsq5OLFNenQO3RMNMi9RC+qJ82s
gPXX6i9V/KszNxAyfegbMseoW9FcFwViD14giBQwA7NDw3ICm89PTjy+YBMA50iRqdErm
ACz0fHfA/Ed5yu5cOVVa8DD12/upTzx7i0mmkAxwsKiktEaKQvg8i1gvzqeymWYnckGon
y08eCCIZFc78CeuhODy0+MXyrnBRP9p+fcQE7/GspKoSbxVT3evwT2UkebezQT2+AL57N
EnRsJzsgQM4R0sMgvZI7I6kfWKerhFMt3imSt1QGphXmKZPRvKqib59U57GsZU1/2CMIl
YBVMTZIpYKRh6NgE8ityaa4gehJDl16xapZ8z3DMNt3CRF8hqWmJNUfDwUvXBEk8d/8Lk
h39/IFHbWqNJh6cgq3+CipXH5HjLiVh7tzGPfB6yn+RETzcZjesZHtz4hFudOxTMV0YnT
Iv0FGtfxsfEQe7ZVmmfqGNGglxE0EfbXt0psLXngFMneZYBJqXGFsK3r5bHjRm6wpC9ED
AzXp+Tb+jQgs8t5eWVxiQdBpNZnjnGiIOASOxJrIRuzbTjo389683NfLvPRY8eX1iEw58
ebjLvDhvDZ2jSpwGuWuJ/8QNZou1RfU5QL0M0SEe3ACm4wP5zfUGnW8o1vKY9rK5/9evI
iA/DMAJ+gF20Y6WzGg4llG9qCAnBkc3GgC7K1zkXU5N1VD50Y0qLoNsKy6eengXvmiL5E
kFKRnLtP45kD2rn6iZq3/Pnj1IfPonsdaNttb+2fhpFWa/r1sUyYadWeHs72vH83MgBI6
h3Ae9ilF5tYLs2m6u8rKFM8zZhixSh=a8FR
-----END PGP MESSAGE-----
```

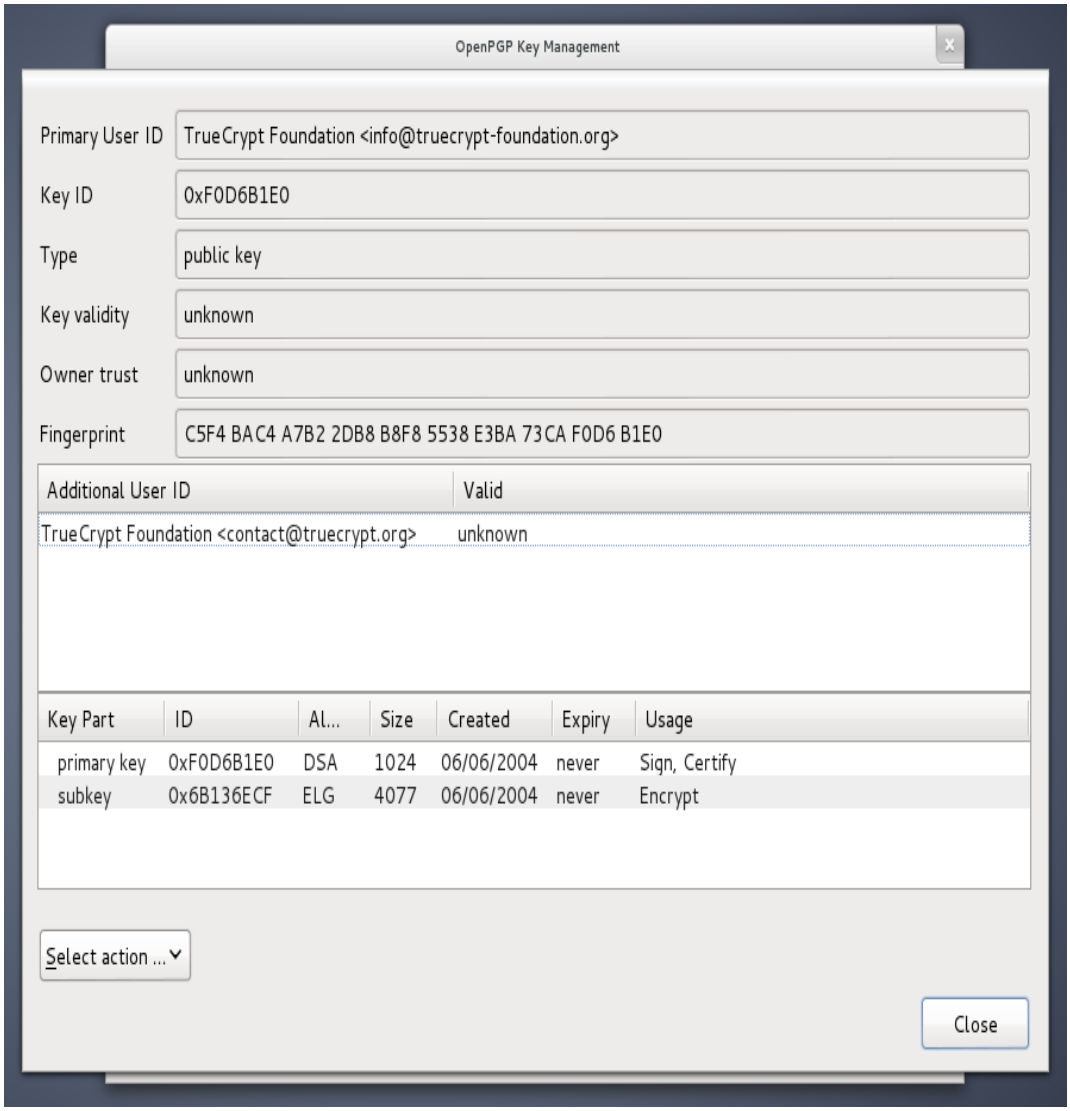
Contrôle d’identité

Comme avec l’OTR, il est important de vérifier les clés PGP des personnes avec qui vous communiquez. Avec PGP, vous faites cela en utilisant votre clé privée pour signer numériquement la clé publique de quelqu’un d’autre.

Depuis Thunderbird, cliquez sur le menu OpenPGP et ouvrez le gestionnaire de clé. Cochez la case « afficher toutes les clés par défaut » pour voir toutes les clés de votre trousseau. De là, vous pouvez importer des clés à partir de fichiers, de votre presse-papier ou de serveurs de clés. Vous pouvez aussi générer une nouvelle paire de clé et voir le détail de toutes les clés de votre trousseau.

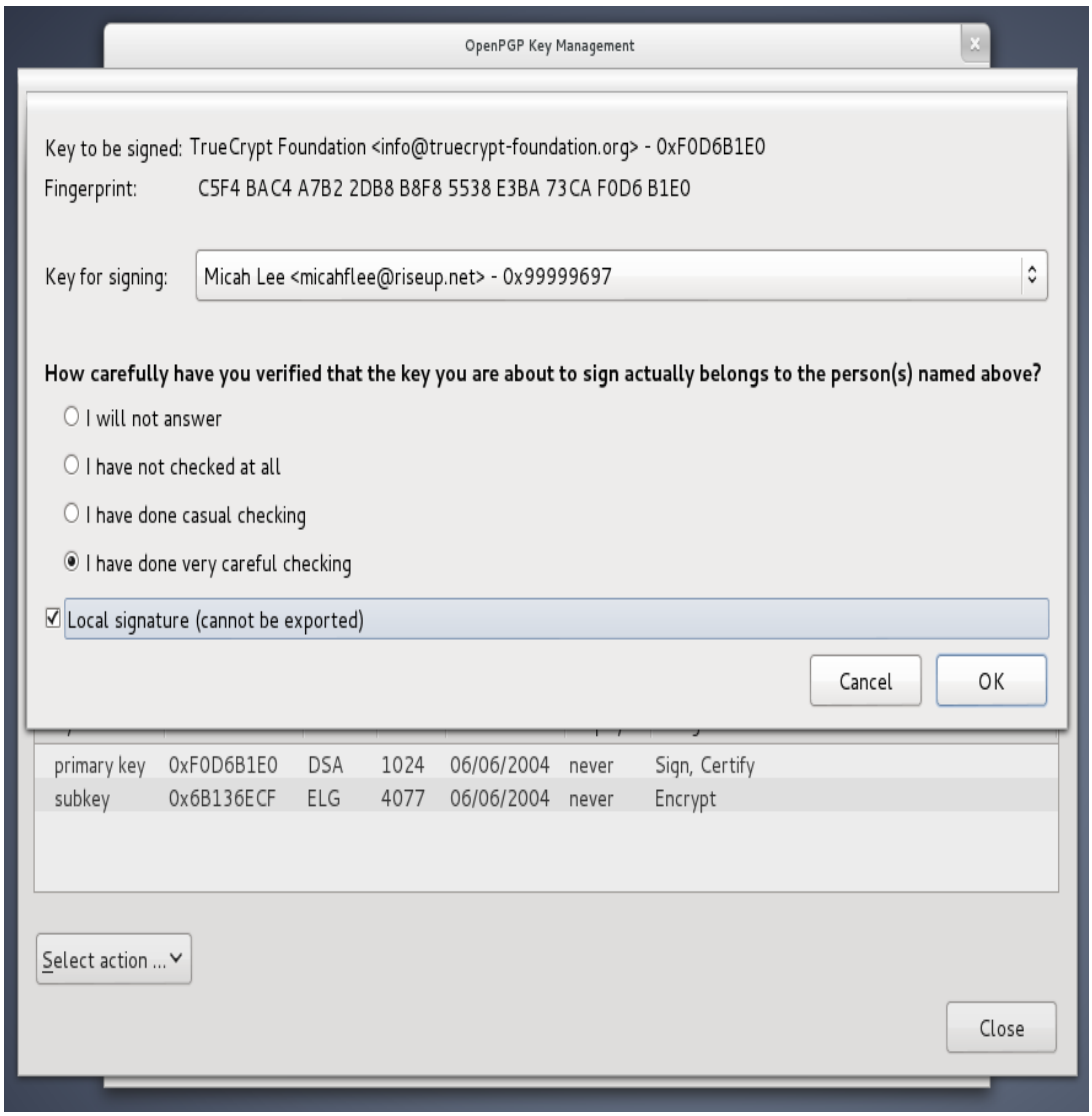
Comme avec les clés OTR, chaque clé PGP a une empreinte unique. Et comme pour OTR, vous avez besoin d’afficher l’intégralité de l’empreinte pour être sûr que la clé publique que vous êtes en train de regarder est bien celle de la personne à qui vous pensez qu’elle appartient.

Faites un clic droit sur une clé de cette liste et choisissez « détailler » pour voir son empreinte. Voici le détail de la clé PGP que le logiciel de chiffrement TrueCrypt utilise pour signer numériquement les r*eleases* de son logiciel.



Toujours comme OTR, vous avez besoin de vous rencontrer en personne, parler au téléphone ou utiliser une session OTR déjà vérifiée pour comparer chaque caractère de l'empreinte.

Après avoir vérifié que la clé publique dont vous disposez appartient bien à la personne que vous pensez, cliquez sur « choisir une action » et sélectionnez « Signer la clé ».



Sur la capture d'écran ci-dessus, j'ai coché la case « signatures locales (ne peuvent pas être exportées) ». De cette façon, vous pouvez signer les clé PGP, ce qui est nécessaire pour Enigmail et d'autres logiciels PGP pour afficher des messages de sécurité sensés, mais vous ne risquez pas de dévoiler accidentellement avec qui vous communiquez à un serveur de clés PGP.

Si vous recevez un courriel chiffré de quelqu'un que vous connaissez mais que le courriel n'est pas signé numériquement, vous ne pouvez pas être sûr qu'il a vraiment été écrit par la personne à laquelle vous pensez. Il est possible qu'il provienne de quelqu'un qui falsifie son adresse de courriel ou que son compte courriel soit compromis.

Si votre ami vous dit dans son courriel qu'il a généré une nouvelle clé, vous devez le rencontrer en personne ou lui parler au téléphone et inspecter l'empreinte pour être certain que vous n'êtes pas victime d'une attaque.

Attaques

Si vous ne vérifiez pas les identités, vous n'avez pas la possibilité de savoir si vous n'êtes pas victime d'une attaque de l'homme du milieu (MITM).

Le journaliste du Washington Post Barton Gellman, à qui Edward Snowden a confié des informations à propos du programme PRISM de la NSA, a écrit ceci à propos de son expérience dans l'utilisation de PGP.

> Le jeudi, avant que The Post ne publie la première histoire, je l'ai contacté sur un nouveau canal. Il ne m'attendait pas à cet endroit et m'a répondu alarmé. « Je te connais ? » a-t-il écrit.
>
> Je lui ai envoyé un message sur un autre canal pour vérifier mon « empreinte » numérique, une sécurité qu'il prennait depuis quelque temps. Fatigué, je lui en ai envoyé une mauvaise. « Ce n'est pas du tout la bonne empreinte », m'a-t-il dit, se préparant à se déconnecter. « Vous êtes en train de faire une attaque de MITM». Il parlait d'une attaque de type « homme du milieu », une technique classique de la NSA pour contourner le chiffrement. J'ai immédiatement corrigé mon erreur.

Snowden avait raison de prendre des précautions et d'insister sur le fait qu'il vérifiait la nouvelle empreinte PGP de Gellman. PGP, s'il est bien utilisé, fournit les outils nécessaires pour éviter les attaques de l'homme du milieu. Mais ces outils ne fonctionnent que si les utilisateurs sont vigilants lors des vérifications d'identité.

Tails : un système live anonyme et amnésique

L'utilisation de « systèmes crypto implémentés proprement » a une courbe d'apprentissage énorme et nécessite des utilisateurs dévoués qui soient prêts à travailler un peu plus pour reprendre le contrôle de leur vie privée. C'est principalement pour cette raison que OTR et PGP ne sont pas largement répandus. Mais même en utilisant ces outils, comment être sûr d'avoir une sécurité « de bout en bout » quand vous ne pouvez pas forcément faire confiance à votre système d'exploitation ou aux autres logiciels que vous utilisez tous les jours ?

La solution consiste à utiliser un système d'exploitation totalement différent composé uniquement de « logiciels de confiance » quand vous avez besoin d'une confidentialité absolue. Tails vous aide à résoudre ce problème.

> Tails est un système live dont le but est de préserver votre vie privée et votre anonymat. Il vous permet d'utiliser Internet de manière anonyme et de contourner la censure quasiment partout où vous allez et sur n'importe quel ordinateur. Tails ne laisse aucune trace de ce que vous avez fait, sauf si vous le demandez explicitement.
>
> Tails est un système d'exploitation complet destiné à être utilisé depuis un DVD ou une clef USB indépendamment du système installé sur l'ordinateur. C'est un logiciel libre basé sur Debian GNU/Linux.

> Tails est livré avec de nombreuses applications, configurées avec une attention particulière accordée à la sécurité : navigateur web, client de messagerie instantanée, client email, suite bureautique, éditeur d'image et de son, etc.

Tails n'est pas destiné à tout le monde. Il est toujours difficile de le comparer à un système d'exploitation classique. Il est lent, il ne comporte pas tous les logiciels que vous pourriez vouloir. Mais Tails a ces particularités parce qu'il a été conçu spécifiquement pour être plus difficile de compromettre la protection des points d'accès. Si vous êtes dans une situation qui vous fait penser que la NSA ou n'importe quel attaquant potentiel peut vous cibler vous et vos collègues (les journalistes ou les relations des lanceurs d'alarme me viennent à l'esprit), c'est l'un des meilleurs outils disponibles.

Comme Tails n'est pas pratique pour une utilisation quotidienne de l'ordinateur, c'est une bonne idée de s'habituer à utiliser OTR et PGP sur votre système d'exploitation principal autant que possible. Tails n'aide pas à adoucir les effets de la surveillance en elle-même, mais chiffrer autant que possible les actions quotidiennes le permettra.

À chaque fois que vous lancez Tails, vous démarrez sur un système propre. Tout ce que vous avez fait lors de vos précédentes sessions sur Tails est effacé et vous repartez de l'état initial. Ce qui signifie que si vous avez été infecté par un malware en utilisant Tails, celui-ci aura disparu à votre prochaine connexion.

Vous pouvez commencer à utiliser Tails en téléchargeant l'image ISO et en la gravant sur un DVD. Vous devez alors démarrer sur le DVD. Cette étape dépend de votre modèle d'ordinateur, mais nécessite généralement d'entrer dans le BIOS et de changer l'ordre de démarrage de votre ordinateur de façon à ce qu'il tente de démarrer sur le DVD avant d'essayer sur votre disque dur. Sur les nouveaux PC, vous devrez peut-être désactiver le « secure boot » de l'UEFI : il s'agit du crypto utilisé pour être sûr que votre ordinateur ne va démarrer que sur une version de Windows signée numériquement (ce qui, en fait, rend le démarrage sur un système d'exploitation non-Windowsien plus difficile). Le site web de Tails propose davantage d'informations sur les outils de démarrage sur un DVD ou une clé USB.

Après avoir démarré sur le DVD, vous avez la possibilité d'installer Tails sur une clé USB. C'est particulièrement utile car cela permet de configurer un volume persistant, c'est à dire une partie de votre clé USB chiffrée pour stocker vos données. Malgré le retour à un espace propre à chaque démarrage, il est important de pouvoir accéder à vos clés OTR et PGP, vos configurations Claws mail (voir plus bas) et Pidgin ainsi que les documents sur lesquels vous travaillez. Votre volume persistant vous permet tout ceci.

PGP et courriels avec Tails

Je parlais de l'utilisation de Thunderbird avec l'add-on Enigmail pour accéder à vos courriels et utiliser PGP. Cependant, ce logiciel n'est pas fourni avec Tails. Tails est livré avec Claws Mail qui comprend un plug-in PGP.

Au lieu d'utiliser l'interface graphique utilisateur du gestionnaire de clé

d’Enigmail pour importer, exporter, générer et voir le détail des clés signées, vous pouvez cliquer sur l’icône du presse-papiers en haut à droite de l’écran et choisir le gestionnaire de clés pour ouvrir SeaHorse, qui propose ces mêmes fonctions.

Procédure

Pour commencer à avoir un espace de communication privé avec vos amis et collègues, et disposant d’un haut niveau de sécurité des points d’accès, voici les étapes à suivre.

- Rencontrez vos amis en face à face. Chacun devra apporter son propre PC portable ou clé USB.
- Téléchargez et gravez un DVD de Tails, puis démarrez dessus et créez une clé USB pour chaque personne.
- Quand tout le monde a sa clé USB Tails, chacun doit démarrer dessus sur son propre PC et configurer un volume persistant. Une fois que ce volume est chiffré, chacun peut générer sa propre phrase de passe sécurisée qu’il devra entrer à chaque démarrage sur Tails, avant de redémarrer sur son PC avec Tails et cette fois monter le volume persistant.
- Chacun crée alors un nouveau pseudo pour compte Jabber. L’une des solutions est d’aller sur https://register.jabber.org depuis iceweasel. Comme Tails fait transiter les échanges internet via Tor, cela permet bien de créer un compte jabber anonyme.
- Chacun ouvre alors Pidgin et le configure en utilisant ce nouveau compte Jabber et crée une nouvelle clé OTR. Chacun ajoute les autres dans sa liste d’amis et démarre une session OTR avec les autres. Une fois que tout le monde est dans la même discussion, c’est le moment idéal pour comparer les empreintes et vérifier l’identité de chaque personne afin de pouvoir communiquer de façon sécurisée via internet à l’avenir.
- Chacun devrait se créer une nouvelle adresse de courriel de la même façon. Certains fournisseurs de courriels, comme Gmail, rendent difficile la création de nouveaux comptes en utilisant Tor et en restant anonyme. Dans ce cas, utilisez un autre fournisseur de courriels. Assurez-vous que celui-ci supporte IMAP (de façon à pouvoir utiliser un client de messagerie courriel) à travers un SSL (pour que votre client de messagerie utilise une communication chiffré avec le serveur courriel). Si vous choisissez tous le même fournisseur de courriels, envoyer des courriels entre les comptes ne devrait jamais quitter le serveur, ce qui réduit les métadonnées disponibles relatives à votre utilisation du courrier électronique pour ceux qui surveillent internet.
- Chacun devra générer une nouvelle clé PGP pour son adresse de courriel. comme pour le chiffrage du disque, il est important de choisir une phrase de passe complexe au moment de cette génération de clé PGP.
- Le client de messagerie compatible PGP livré avec Tails s’apelle Claws Mail. Chacun doit configurer Claws Mail pour utiliser sa nouvelle adresse courriel, et envoyer une copie de sa clé publique aux autres personnes présentes dans votre réunion. Puis chacun devra importer la clé publique

des autres dans son propre trousseau de clé, puis vérifier manuellement l’empreinte PGP. Ne sautez pas cette étape. Finalement, chacun devra avoir un trousseau de clé contenant les clés signées de tous les autres.

Si quelqu’un de malveillant vole physiquement votre clé USB Tails, la modifie et vous la rend, il peut compromettre toute la sécurité de Tails. C’est pour cela qu’il est très important de toujours garder votre clé USB avec vous.

Si le directeur de la CIA David Petraeus (général 4 étoiles à la retraite) et sa biographe Paula Broadwell avaient décidé d’utiliser Tails, OTR et PGP, leur liaison extra-conjugale serait sans doute restée secrète.

Une chance de s'en sortir

Protéger sa vie privée à l'ère de la surveillance omniprésente de la NSA est incroyablement complexe. L'effort d'acquisition des concepts à maîtriser, représente une sacrée courbe d'apprentissage, plus ou moins facilitée par l'utilisation des logiciels déjà disponibles.

Mais même avec un accès direct à toutes les données transitant à la vitesse de la lumière par les fibres optiques, formant l’épine dorsale d'Internet, même avec la coopération des principales entreprises des États-Unis (qu'il est extrêmement difficile pour les gens de boycotter), le plus grand, le plus puissant et le meilleur système de surveillance que l'humanité ait jamais connu ne pourra pas battre les mathématiques.

Le défi pour le nouveau mouvement cypherpunk est de rendre la sécurité et le chiffrement vérifiés de bout à bout accessibles à tout le monde et activés par défaut.

Postface

Ces derniers mois, les révélations distillées par E. Snowden n'ont fait que confirmer l'ampleur considérable des transgressions commises par la NSA : le protocole https est compromis, et même un certain type de chiffrement a été « cassé » depuis 2010…

Il est donc d'autant plus justifié de rechercher les moyens de se protéger de ces intrusions de la surveillance généralisée dans nos données personnelles. À titre de prolongement de cet petit guide d'initiation, voici rapidement traduits 5 conseils donnés ce vendredi par Bruce Schneier, spécialiste de la sécurité informatique, dans un article du Guardian. Il reconnaît cependant que suivre ces conseils n'est pas à la portée de l'usager moyen d'Internet…

> 1) **Cachez-vous dans le réseau.** Mettez en œuvre des services cachés. Utilisez Tor pour vous rendre anonyme. Oui, la NSA cible les utilisateurs de Tor, mais c'est un gros boulot pour eux. Moins vous êtes en évidence, plus vous êtes en sécurité.
>
> 2) **Chiffrez vos communications.** Utilisez TLS. Utilisez IPsec. Là encore, même s'il est vrai que la NSA cible les connexions chiffrées - et il peut y avoir des exploits explicites contre ces protocoles - vous êtes beaucoup mieux protégés que si vous communiquez en clair.
>
> 3) **Considérez que bien que votre ordinateur puisse être compromis, cela demandera à la NSA beaucoup de travail et de prendre des risques - il ne le sera donc probablement pas.** Si vous avez quelque chose de vraiment important entre les mains, utilisez un « angle mort ». Depuis que j'ai commencé à travailler avec les documents Snowden, j'ai acheté un nouvel ordinateur qui *n'a jamais* été connecté à l'internet. Si je veux transférer un fichier, je le chiffre sur l'ordinateur sécurisé (hors-connexion) et le transfère à mon ordinateur connecté à Internet, en utilisant une clé USB. Pour déchiffrer quelque chose, j'utilise le processus inverse. Cela pourrait ne pas être à toute épreuve, mais c'est déjà très bien.
>
> 4) **Méfiez-vous des logiciels de chiffrement commerciaux, en particulier venant de grandes entreprises.** Mon hypothèse est que la plupart des produits de chiffrement de grandes sociétés nord-américaines ont des portes dérobées utiles à la NSA, et de nombreuses entreprises étrangères en installent sans doute autant. On peut raisonnablement supposer que leurs logiciels ont également ce genre de portes dérobées. Les logiciels dont le code source est fermé sont plus faciles à pénétrer par la NSA que les logiciels *open source*. Les systèmes qui reposent sur une clé « secrète » principale sont vulnérables à la NSA, soit par des moyens juridiques soit de façon plus clandestine.

> 5) **Efforcez-vous d’utiliser un chiffrement du domaine public qui devra être compatible avec d’autres implémentations.** Par exemple, il est plus difficile pour la NSA de pénétrer les TLS que BitLocker, parce que les TLS de n’importe quel fournisseur doivent être compatibles avec les TLS de tout autre fournisseur, alors que BitLocker ne doit être compatible qu’avec lui-même, donnant à la NSA beaucoup plus de liberté pour le modifier à son gré. Et comme BitLocker est propriétaire, il est beaucoup moins probable que ces changements seront découverts. Préférez le chiffrement symétrique au chiffrement à clé publique. Préférez les systèmes basés sur un logarithme discret aux systèmes conventionnels à courbe elliptique ; ces derniers ont des constantes que la NSA influence quand elle le peut.