Le chiffrement, maintenant (7)

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 sur 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.

Copyright: Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance est publié sous licence Creative Commons Attribution 3.0 Unported License.