Il a choisi Linux et s'en félicite

Dan Gillmor, qui avait l'an dernier expliqué pourquoi il disait au revoir à google, Microsoft et Apple dans un article que nous avons publié, fait aujourd'hui le point sur ses choix et constate qu'il ne regrette rien. D'autres bonnes raisons de migrer sont apparues, comme l'accélération de la re-centralisation du Web, l'hégémonie croissante des grands acteurs et bien sûr la surveillance généralisée.

Dan Gillmor évoque avec précision les matériels et logiciels qu'il a adoptés progressivement, fait état également sans à priori des avancées et des faiblesses des produits *open source*. Il reconnaît la difficulté relative du passage au Libre intégral (il peine encore à se *dégoogliser* □) mais les valeurs qu'il défend sont celles de l'indépendance, du choix libre pour l'utilisateur de ses usages et de ses produits…

Je suis passé à Linux et c'est encore mieux que ce que j'espérais

Dire adieu à Microsoft et Apple n'a jamais été aussi facile, ni aussi satisfaisant

par Dan Gillmor

Article original sur Medium : I Moved to Linux and It's Even Better Than I Expected
Traduction Framalang : line, goofy, Sphinx, r0u, david_m, Manegiste, sebastien, teromene, galadas, roptat, Omegax, didimo

Un beau jour du printemps 2012, j'ai refermé mon MacBookAir pour la dernière fois. À partir de ce moment, mon environnement informatique (en tout cas, en ce qui concerne mon portable) était GNU/Linux. J'ai abandonné, autant que possible, les environnements propriétaires et obsédés du contrôle qu'Apple et Microsoft ont de plus en plus imposés aux utilisateurs d'ordinateurs personnels.

Presque quatre ans plus tard, me voici, et j'écris cet article sur un portable qui tourne sous le système d'exploitation Linux, avec LibreOffice Writer, et non sur une machine Mac ou Windows avec Microsoft Word. Tout va bien.

Non, c'est même mieux que ça, tout est sensationnel.

Je recommanderais ce changement à beaucoup de personnes (pas à tout le monde, ni à n'importe quel prix, mais à quiconque n'est pas effrayé à l'idée de poser une question à l'occasion, et plus particulièrement quiconque réfléchit à la trajectoire prise par la technologie et la communication au 21ème siècle). Plus que tout, aux gens qui se soucient de leur liberté.

> *Ils nous ont donné plus de confort, et nous avons dit collectivement : « Génial ! »*

L'informatique personnelle remonte à la fin des années 1970. Elle a défini une ère de la technologie où les utilisateurs pouvaient adapter ce qu'ils achetaient de toutes sortes de manières. Lorsque l'informatique mobile est arrivée sous la forme de smartphones, la tendance s'est inversée. Les constructeurs, en particulier Apple, ont gardé bien plus de contrôle. Ils nous ont donné plus de confort, et nous avons dit collectivement : « Génial ! ».

Il y a quelques mois, lorsque Apple a annoncé son iPad Pro, une grande tablette avec un clavier, son président Tim Cook l'a appelée « la plus claire expression de notre vision pour

le futur de l'informatique personnelle ». « Ouh là, ça craint » me suis-je dit à ce moment-là. Entre autres, dans l'écosystème iOS, les utilisateurs ne peuvent obtenir leurs logiciels que sur l'Apple store, et les développeurs sont obligés de les vendre au même endroit seulement. C'est peut-être la définition de l'informatique personnelle pour Apple, mais pas pour moi.

Pendant ce temps-là, Windows 10 de Microsoft (sur presque tous les points, une grande avancée en termes de facilité d'utilisation par rapport à Windows 8) ressemble de plus en plus à un logiciel espion déguisé en système d'exploitation (une appellation qui pourrait être injuste, mais pas de beaucoup). Oui, la mise à jour depuis les versions précédentes, extrêmement répandues, est gratuite, mais elle prend des libertés extraordinaires avec les données des utilisateurs et le contrôle de ceux-ci, d'après ceux qui en ont analysé le fonctionnement interne.

Ce n'est pas exactement un duopole commercial. Le système d'exploitation Chrome OS de Google fait tourner un nouvel arrivant : le *Chromebook*, vendu par différents constructeurs. Mais il comporte plus de limites et oblige ses utilisateurs à être totalement à l'aise (je ne le suis pas) sous l'emprise d'une entreprise qui repose sur la surveillance pour soutenir son modèle économique basé sur la publicité.

Ainsi, pour ceux qui ont le moindre intérêt à garder une indépendance substantielle dans l'informatique mobile ou de bureau, Linux semble être le dernier refuge. Sur toute une gamme de machines, des super-ordinateurs aux serveurs, en passant par les téléphones portables et les systèmes embarqués, Linux est déjà incontournable. Je suis content d'avoir franchi le pas.

Avant d'expliquer le comment, il est vital de comprendre le contexte de ma petite rébellion. La re-centralisation est la nouvelle norme dans les technologies et les communications,

une tendance qui m'a préoccupé il y a quelque temps sur ce site, quand je décrivais de manière plus générale mes efforts pour me sevrer des produits et services d'entreprises fournis par Apple (c'est fait), Microsoft (fait en grande partie) et Google (encore difficile). Le gain en confort, comme je le disais à l'époque, ne vaut pas les compromis que nous concédons.

Un duopole mobile ?

Comme j'en discuterai plus bas, je dois me demander à quel point il est pertinent de déclarer son indépendance sur son ordinateur personnel, puisque l'informatique évolue de plus en plus vers les appareils mobiles. Qu'on le veuille ou non, Apple et Google en ont plus ou moins pris le contrôle avec iOS et Android. Apple, comme je l'ai dit, est un maniaque obsédé du contrôle. Même si Google distribue gratuitement une version ouverte d'Android, de plus en plus de pièces essentielles de ce système d'exploitation sont intégrées en un amas logiciel terriblement verrouillé qui emprisonne les utilisateurs dans le monde de Google contrôlé par la publicité. Peut-on parler de « duopole » mobile ?

La re-centralisation est particulièrement terrifiante au vu du pouvoir croissant de l'industrie des télécommunications, qui se bat bec et ongles pour contrôler ce que vous et moi faisons des connexions que nous payons, malgré le jugement bienvenu de la FCC (commission fédérale des communications aux États-Unis) en faveur de la « neutralité du net » en 2015. Comcast détient le monopole du véritable haut débit sur la vaste majorité de son territoire, même si l'on distingue quelques concurrents ici et là. Les fournisseurs d'accès par câble avancent rapidement pour imposer des limites d'utilisation qui n'ont rien à voir avec la capacité disponible et tout à voir avec l'extension de leur pouvoir et de leurs profits, comme l'expliquait en détail Susan Crawford. Et les fournisseurs de téléphonie mobile piétinent allègrement la neutralité du net

avec leurs services « *zero-rated* » (où l'accès à certains services spécifiques n'est pas décompté du volume de données du forfait), que la FCC considère de manière incompréhensible comme innovants.

Pendant ce temps, pour la simple et bonne raison que les utilisateurs préfèrent souvent le confort et la simplicité apparente d'un outil à la garantie de leurs libertés, des acteurs centralisés comme Facebook se constituent des monopoles sans précédents. Comme pour Google et son outil de recherche, ils recueillent les bénéfices grandissants des effets du réseau, que des concurrents vont trouver difficile sinon impossible à défier.

Goulets d'étranglement

N'oublions pas le gouvernement, qui a horreur de la décentralisation. Les services centralisés créent des goulots d'étranglement et rendent le travail facile aux services de police, espions, contrôleurs et service des impôts. L'état de surveillance raffole de la collecte de données sur ces goulots d'étranglement, ce qui met finalement en danger les communications et libertés de tous.

Les goulots d'étranglement permettent aussi de soutenir des modèles économiques qui génèrent beaucoup d'argent pour les campagnes politiques. Hollywood en est un excellent exemple ; la quasi prise de contrôle du Congrès par les lobbies du copyright a conduit à l'adoption de lois profondément restrictives comme dans le système du copyright en vigueur.

Les droits d'auteur sont la clé de ce que mon ami Cory Doctorow appelle « la prochaine guerre civile dans l'informatique générique », une campagne, parfois agressive, pour empêcher les gens qui achètent du matériel (vous et moi, de manière individuelle et dans nos écoles, entreprises et autres organisations) de réellement en être propriétaires. Les lois sur le droit d'auteur sont l'arme des maniaques du

contrôle, puisqu'elles les autorisent à nous empêcher par des moyens légaux de bricoler (ils diraient trafiquer) les produits qu'ils vendent.

Les perspectives ne sont pas toutes aussi sombres. Le mouvement des *makers* ces dernières années est l'un des antidotes à cette maladie du contrôle total. Il en est de même avec les composantes-clés de la plupart des projets de *makers* : les projets de logiciel libre et *open source* dont les utilisateurs sont explicitement encouragés à modifier et copier le code.

Image par Ian Burt via Flickr | CC BY 2.0

C'est là que Linux entre en scène. Même si nous nous servons davantage de nos appareils mobiles, des centaines de millions d'entre nous travaillent encore beaucoup avec leurs ordinateurs mobiles et de bureau. Linux et les autres logiciels développés par la communauté ne représentent peut-être qu'une solution partielle, mais clairement utile. Il vaut mieux commencer avec quelque chose et l'améliorer, que d'abandonner directement.

J’ai installé Linux un bon nombre de fois au cours des dernières années, depuis qu’il est devenu un véritable système d’exploitation. Mais je suis toujours retourné sous Windows ou Mac, en fonction de mon système principal de l’époque. Pourquoi ? Il restait encore trop d’aspérités et, pendant longtemps, Linux n’avait pas assez d’applications pour réaliser ce dont j’avais besoin. Les inconvénients étaient trop importants pour ma patience limitée, en utilisation quotidienne.

Mais cela s’est progressivement amélioré et, en 2012, j’ai décidé qu’il était temps. J’ai demandé à Cory Doctorow quelle version de Linux il utilisait. C’était une question fondamentale, car Linux se décline en de nombreuses variantes. Les développeurs ont pris le noyau essentiel du code et ont créé différentes versions, adaptées aux divers besoins, goûts et genres d’informatique. Bien que tous utilisent les composants essentiels, sur le modèle du logiciel libre, certains ajoutent du code propriétaire, comme Flash, pour mieux s’adapter aux pratiques informatiques des utilisateurs. Le matériel représentait également une question cruciale, car les ordinateurs ne sont pas tous gérés de manière fiable par Linux, à cause des incompatibilités matérielles.

Cory m’a dit qu’il utilisait Ubuntu sur un Lenovo ThinkPad. J’étais déjà convaincu par les ThinkPads, grâce à la fiabilité du matériel et le bon service après-vente du constructeur, sans oublier la possibilité de mettre à jour les composants matériels internes. Comme j’ai tendance à acheter des modèles récents, je rencontre parfois des problèmes de compatibilité avec le matériel Lenovo le plus récent. J’ai bricolé mon modèle actuel, un T450s, par tous les moyens, en remplaçant le disque dur mécanique par un disque SSD rapide et en ajoutant autant de mémoire vive (RAM) que j’ai pu.

Je penchais également pour Ubuntu, une version de Linux créée par une entreprise appelée Canonical, avec à sa tête un ancien entrepreneur informatique du nom de Mark Shuttleworth, que je

connais aussi depuis longtemps. Ubuntu est connu pour son excellente gestion des ThinkPads, surtout s'ils ne sont pas flambants neufs. J'ai utilisé Ubuntu sur quatre ThinkPads différents depuis ma conversion. On apprécie Ubuntu à l'usage parce que Canonical a une vision bien définie de la façon dont les choses doivent fonctionner.

Libre à vous de tester une autre « distribution » Linux, comme on appelle les différentes versions. Il y en a trop pour les nommer toutes, ce qui est à la fois le meilleur et le pire atout de l'écosystème Linux. Les nouveaux utilisateurs devraient presque toujours essayer une des distributions les plus populaires, qui aura été testée de manière plus poussée et offrira la meilleure assistance de la part de la communauté ou de l'entreprise qui l'a créée.

L'une de ces distributions est Linux Mint. Elle est basée sur Ubuntu (qui est elle-même basée sur Debian, une version encore plus proche de la version de base de Linux). Mint m'est apparue comme à beaucoup d'autres personnes comme probablement la meilleure distribution Linux pour ceux qui ont utilisé des systèmes propriétaires et souhaitent la transition la plus

simple possible. Je suis parfois tenté de changer moi-même, mais je vais garder Ubuntu, à moins que Canonical ne le foire complètement, ce que je n'espère pas.

Avant de faire le grand saut, j'ai demandé à bon nombre de personnes des conseils sur la façon migrer au mieux mes usages informatiques depuis des programmes propriétaires vers des programmes *open source*. Plusieurs m'ont suggéré ce qui s'est avéré être un bon conseil : j'ai cessé d'utiliser l'application Mail d'Apple et j'ai installé Thunderbird de Mozilla sur mon Mac, et après un mois, je me suis tellement habitué à cette manière différente (pas si différente non plus) de gérer mon courrier électronique (non, je n'utilise pas Gmail, sauf pour un compte de secours). J'ai aussi installé LibreOffice, une sorte de clone *open source* de Microsoft Office, qui est moins courant mais adéquat pour arriver à ses fins dans la plupart des cas.

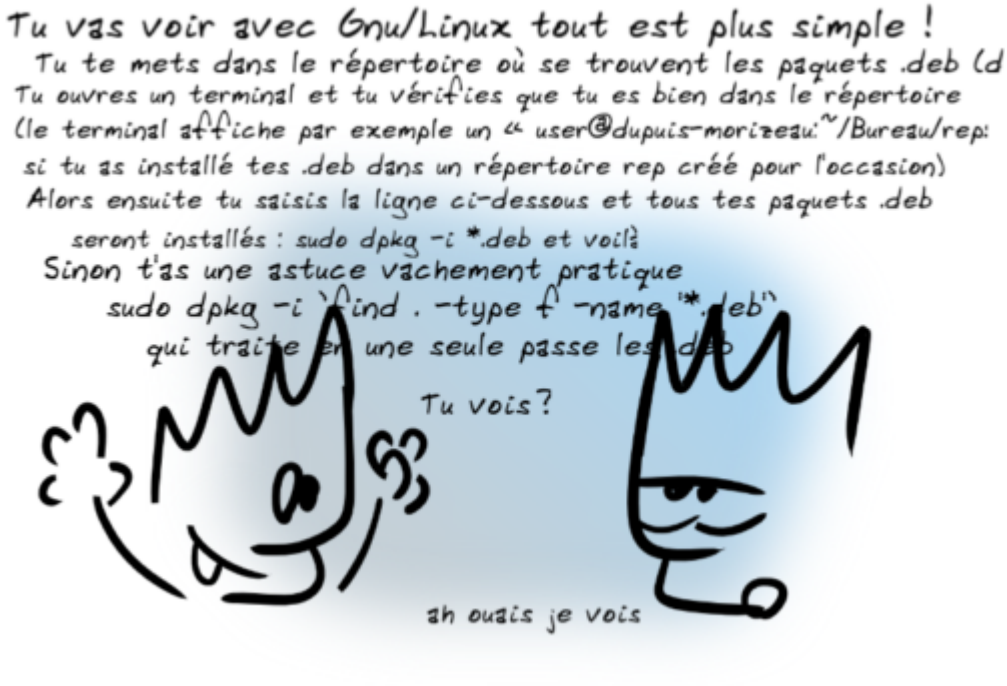
Comme la plupart des gens qui utilisent un ordinateur personnel, je passe mon temps presque exclusivement sur tout petit nombre d'applications : navigateur internet, client courriel, traitement de texte. Sous Linux, j'ai installé Firefox et Chromium, une variante *open source* du Chrome de Google. Comme déjà mentionné, Thunderbird faisait bien son job pour gérer mes courriels, et LibreOffice était satisfaisant en tant que logiciel de traitement de texte.

Mais j'avais encore besoin d'utiliser Windows pour certaines choses. En particulier, le logiciel de cours en ligne que j'utilisais à mon université refusait de fonctionner sous Linux, quel que soit le navigateur utilisé. J'ai donc installé Windows dans une machine virtuelle, afin de faire tourner Windows et ses programmes à l'intérieur de Linux. J'ai aussi installé Windows sur une partition séparée de mon disque dur pour les occasions encore plus rares où j'aurais besoin d'utiliser un Windows natif, contrairement à un Windows virtuel ce qui réduit les performances.

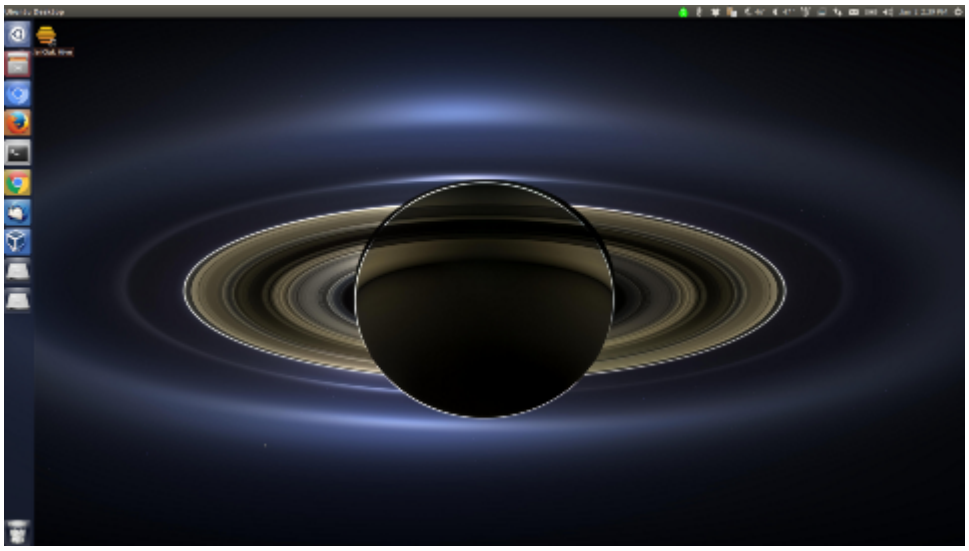
Aujourd'hui je n'ai presque plus jamais besoin de Windows. LibreOffice s'est énormément amélioré. Pour l'édition collaborative, Google Docs (hum… j'ai déjà dit que se passer de Google est difficile, hein ?) est difficile à battre, mais LibreOffice progresse. Le logiciel utilisé dans mon université pour les cours en ligne fonctionne maintenant avec Linux. Le seul programme pour lequel j'ai encore besoin de Windows est Camtasia, pour le « screencasting » – enregistrer (et diffuser) ce qu'affiche l'écran, ainsi que le son. Plusieurs programmes de *screencasting* existent sous Linux, mais ils sont limités. Et parfois, je suis obligé d'utiliser MS PowerPoint pour lire les rares diaporamas qui hoquètent avec le logiciel de présentations de LibreOffice (Impress).

Étrangement, le plus compliqué, dans cette transition, fut de m'adapter aux différentes conventions utilisées pour les claviers : désapprendre le style Apple et réapprendre les combinaisons Windows, équivalentes pour la plupart à celles utilisées par Linux. Au bout de quelques mois, tout était rentré dans l'ordre.

La fréquence de mise à jour des logiciels est un des aspects que je préfère avec Linux. Ubuntu et de nombreuses autres versions proposent régulièrement des mises à jour même si je préfère choisir les versions qui disposent d'un support étendu (aussi appelées versions « LTS » soit *Long Term Support* en anglais). Ils corrigent rapidement les failles de sécurité qui sont trouvées et il se passe souvent moins d'une semaine entre deux mises à jour, un rythme beaucoup plus élevé que celui auquel j'étais habitué avec Apple.



Ce que j’aime le moins avec Linux, c’est qu’il faut parfois faire quelque chose qui pourrait paraître intimidant pour un nouvel utilisateur. Personne ne devrait avoir à ouvrir une interface en ligne de commande pour saisir sudo apt-get update ou autre. Personne ne devrait avoir à faire face à un avertissement indiquant que l’espace disque est insuffisant pour que la mise à jour du système puisse être appliquée (ce qui nécessitera alors de retirer les composants obsolètes du système d’exploitation, une opération qui n’est pas à la portée de tout le monde). Personne ne devrait découvrir, après une mise à jour, qu’un composant matériel a cessé de fonctionner, ce qui m’est arrivé avec mon *trackpad*, inutilisable jusqu’à ce que je trouve une solution grâce à un forum (oui, cela peut arriver avec Windows mais les fabricants testent beaucoup plus le fonctionnement de leur matériel avec les logiciels Microsoft. Quant à Apple, ça arrive également, mais il a l’avantage de produire du matériel et des logiciels qui sont associés de façon harmonieuse).



Le bureau de Dan Gillmor sous Ubuntu

Lorsqu'il y a un problème, les communautés apparues autour du logiciel libre et *open source* s'avèrent incroyablement utiles. Poussant toujours un peu les limites pour adopter ce système, je demande souvent de l'aide. Je reçois toujours des réponses. Certains experts super pointus de ces forums peuvent être condescendants voire irrespectueux si on ose poser une question qui leur semblera simplissime ou qui a déjà reçu une réponse par ailleurs. On trouve également cette aide précieuse (et cette éventuelle intempérance) pour Windows, Mac et les autres systèmes mobiles (certains fanatiques d'Apple sont parfois étonnamment violents avec les hérétiques) mais il existe une atmosphère unique lorsqu'il s'agit de personnes œuvrant sur des technologies ouvertes, pour tous.

Si vous souhaitez essayer Linux sur votre ordinateur, c'est plutôt simple. Ubuntu, ainsi que d'autres distributions, vous permettent de créer un DVD ou une clé USB contenant le système d'exploitation et de nombreuses applications et vous pouvez démarrer votre ordinateur en utilisant ce support de test. C'est une bonne technique pour savoir si le matériel que vous avez à votre disposition fonctionnera avec. Ce sera vraisemblablement le cas si vous n'utilisez pas un ordinateur flambant neuf. Linux brille particulièrement par son support des ordinateurs déjà anciens.

Pour éviter les soucis d'installation de Linux, on peut acheter un ordinateur avec le système d'exploitation pré-installé et obtenir des mises à jour régulières, adaptées au matériel. J'ai réfléchi à différents modèles fabriqués par des entreprises comme Dell, System76, ZaReason entre autres. Je viens de visiter une entreprise appelée Purism, qui vend des ordinateurs portables construits uniquement avec du matériel et du logiciel non-propriétaire, du moins autant qu'il est possible à l'heure actuelle. Le modèle Librem 13 est impressionnant, Purism a adapté Linux pour ce matériel ergonomique et j'ai hâte de l'essayer.

Je voyage beaucoup et penche plutôt en faveur d'une entreprise qui dispose de point de dépôt dans différents pays et qui (avec le coût que ça implique) pourra dépêcher un technicien chez moi, à mon bureau ou à mon hôtel si ma machine tombe en panne. Si je dois abandonner Lenovo (et les dernières affaires à leur sujet me font douter), je me dirigerai probablement vers les machines Dell fournies avec Linux.

Vous avez pu remarquer que je n'ai presque pas abordé la question du coût. Pour le système d'exploitation, ce n'est plus nécessaire car Microsoft et Apple ont fait fondre le prix apparent de leur système d'exploitation et il apparaît comme nul. Bien entendu, vous le payez toujours quand vous achetez un ordinateur. Cela dit, même les mises à jour importantes sont devenues gratuites, un changement fondamental si on regarde en arrière. Cependant, en ce qui concerne Microsoft, la « gratuité » semble exister au détriment de la collecte intrusive des données.

En revanche, pour les applications, c'est une autre histoire. Vous pouvez économiser beaucoup d'argent en utilisant des logiciels libres et open source. Comparé à LibreOffice, Microsoft Office reste cher même si les versions de base « Famille et Étudiant » sont abordables et que beaucoup de personnes utilisent MS Office grâce à la version fournie par leur école ou leur entreprise.

Mais voilà, j'apprécie de payer pour certains logiciels, car je veux être sûr, autant que possible, que j'aurai de l'aide si besoin et que les développeurs auront une source de motivation pour continuer à corriger et à améliorer le logiciel. Je serais heureux de pouvoir payer pour des versions de Camtasia et Scrivener sur Linux (ce dernier possède une version communautaire pour Linux). En attendant, je fais des dons à différents projets dont j'utilise les logiciels régulièrement, qu'ils soient créés par des entreprises ou intégralement développés par des bénévoles. Ubuntu a beau être une entreprise qui gagne de l'argent en fournissant des services (une approche populaire et éprouvée dans le monde du logiciel libre et open source), je continue d'y donner. Avec moi, LibreOffice a gagné un utilisateur, mais aussi un donateur. Il en va de même pour d'autres projets.

Linux reste en arrière, enfin « officiellement », quand il s'agit de lire des DVD. Il faut installer certains logiciels jugés illégaux par le cartel du divertissement afin de pouvoir lire les disques que vous avez achetés (Apple a l'air d'un parangon de liberté par rapport à Hollywood). L'utilisation de services de streaming comme Netflix ou Amazon peut également être source d'ennuis. Enfin ça devient plus simple grâce à… humpf l'ajout de verrous numériques (NdT : DRM ou Digital Rights Management) dans certains navigateurs.

Est-ce que tous ces ajustements en valent la peine ? Je dirais que oui. Tout ce qui améliore ou préserve notre capacité à utiliser les technologies comme nous l'entendons en vaut la chandelle par rapport aux voies imposées par des pouvoirs centralisés. Et si nous ne sommes pas plus nombreux à essayer, ces monstres du contrôle verront leur victoire assurée.

Il est probablement presque trop tard pour que Linux devienne un système d'exploitation extrêmement populaire, dans les pays développés tout au moins. Mais il n'est pas trop tard pour que suffisamment d'entre nous l'utilisent afin de garantir des libertés informatiques pour ceux qui les veulent.

Que pouvons-nous faire à propos des écosystèmes mobiles, si nous ne voulons pas leur laisser l'hégémonie sur toute l'informatique personnelle, voilà bien le problème. Des versions tierces d'Android ont émergé au travers de communautés dynamiques telles que XDA Developers, qui veulent plus de liberté. Ubuntu travaille sur un système d'exploitation mobile parmi d'autres nombreux acteurs de la communauté *open source* ; des années ont été dédiées à tendre vers un système d'exploitation qui puisse fonctionner sur tous les appareils. Mais la domination d'Apple et Google sur le monde mobile en intimide plus d'un.

> *nous avons vraiment le choix*

J'essaie en ce moment beaucoup d'options parmi les appareils possibles dans l'espoir que j'en trouverai un qui soit suffisamment bon pour une utilisation au quotidien, même s'il devait ne pas être aussi pratique que les propriétés privées bien gardées des géants de l'internet (un de mes téléphones est actuellement sous un système d'exploitation appelé Cyanogenmod). Bientôt, je vous en dirai plus sur la façon dont ça se passe.

En attendant, souvenez-vous : nous avons vraiment le choix – nous pouvons faire des choix qui repoussent les limites des libertés technologiques. Récemment, mon choix a consisté à me détacher libérer de l'emprise de ceux qui veulent tout contrôler. J'espère vous donner à réfléchir pour faire de même. En fonction de ce que nous choisissons, nous avons beaucoup à gagner, et à perdre.

(1) *Même si cela va vexer certaines personnes, j'ai fait référence à GNU/Linux par son nom de loin le plus couramment utilisé – Linux, tout simplement – après la première occurrence. Pour en savoir plus à ce propos, les Wikipédiens ont rassemblé tout un tas de sources pertinentes.*

Merci à Evan Hansen et Steven Levy.

Biographie et plus d'informations : http://dangillmor.com/about (Photo par Joi Ito)

Le chiffrement, maintenant (6)

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

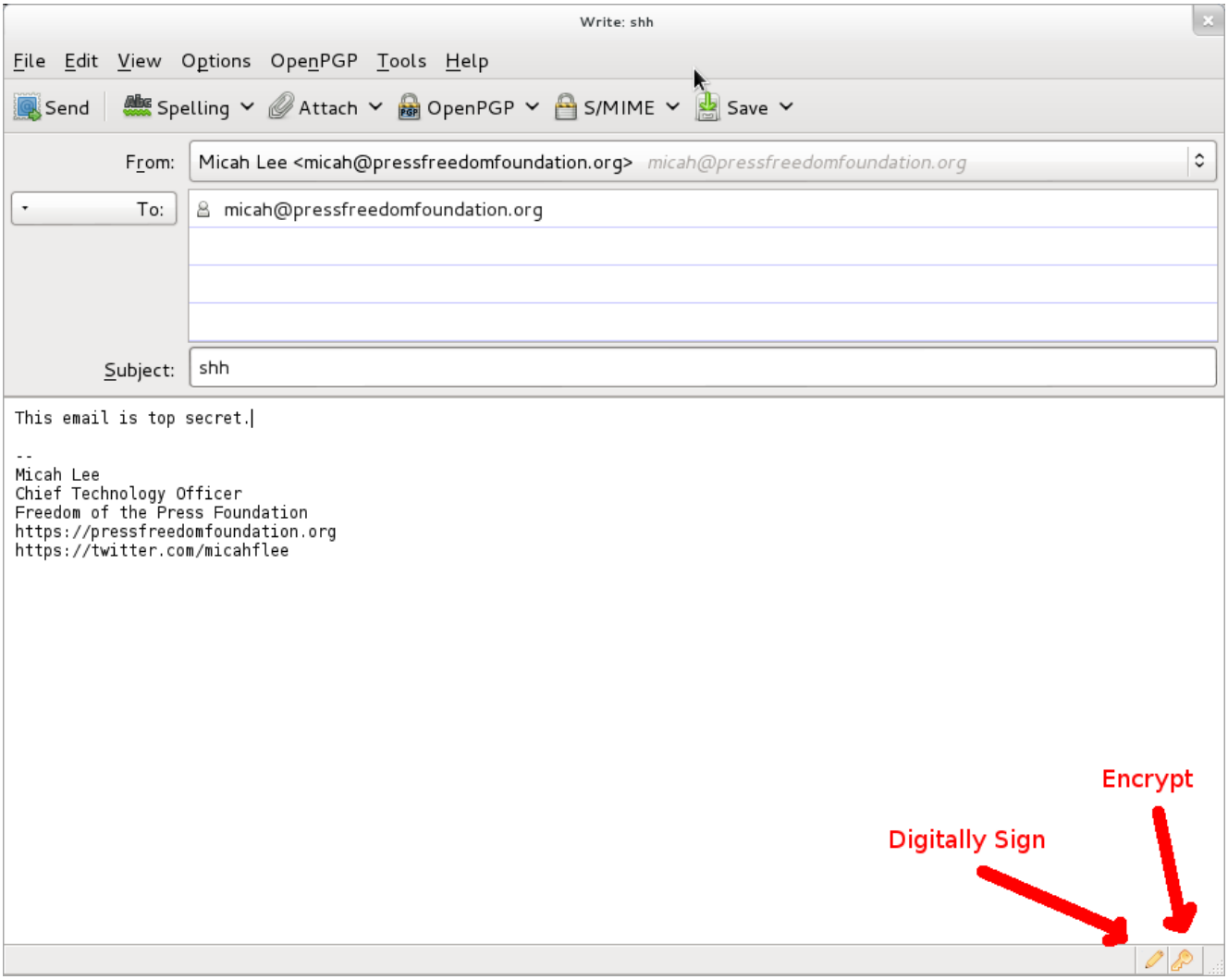
télécharger Gpg4win, et les utilisateurs de Mac OS X GPGTools. Si vous utilisez GNU/Linux, GPG est probablement déjà installé. GPG est un programme en ligne de commande, mais il y a des logiciels qui s'interfacent avec les clients de messagerie, pour une utilisation simplifiée.

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.

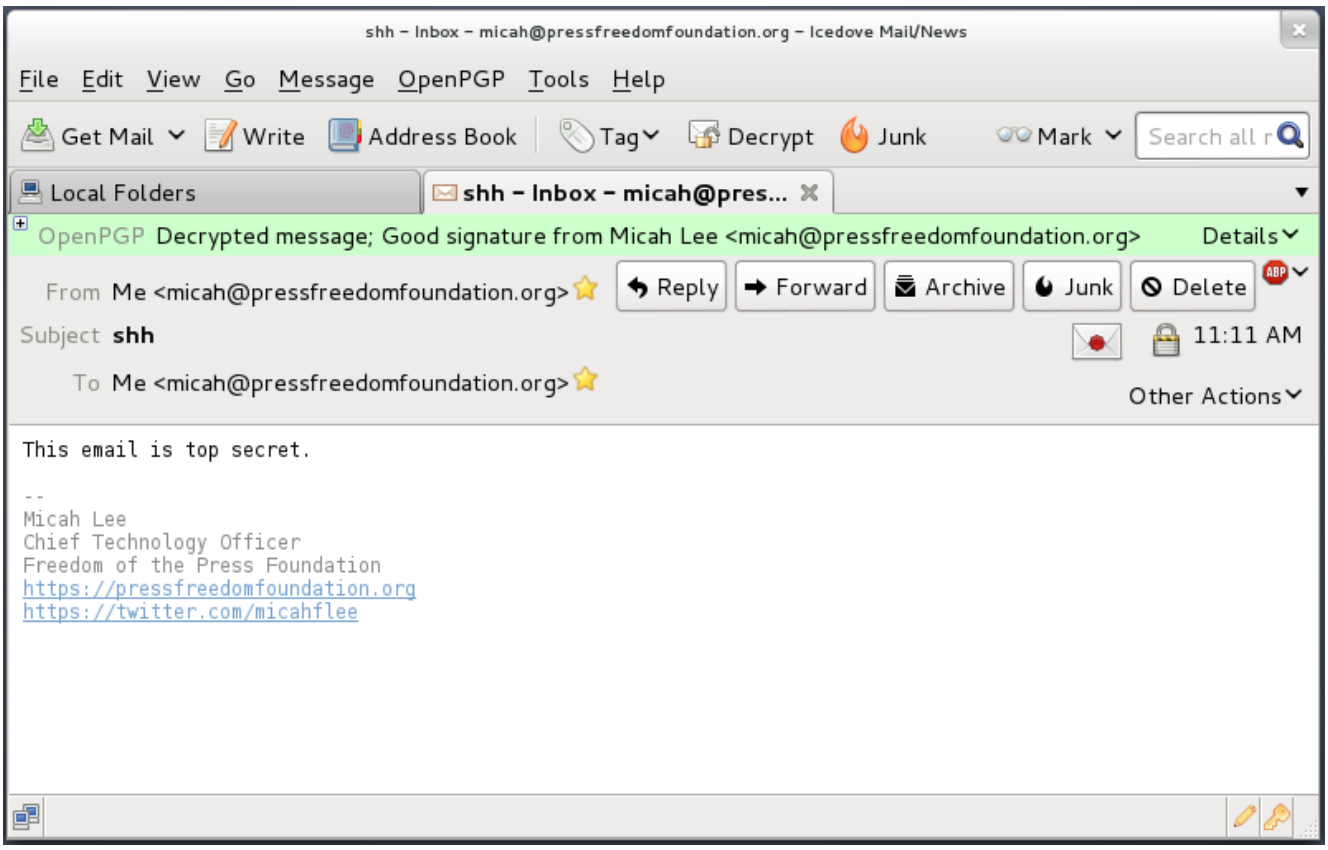
À l'heure actuelle, PGP est très difficile à utiliser de façon sécurisée à partir d'un navigateur web. Bien que quelques extensions de navigateurs existants puissent aider à le faire, je recommande de passer par un client de messagerie de bureau jusqu'à ce que le domaine de la crypto de navigateur mûrisse. 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+jfkKQAi4n
6HzrX9YIbgTukuv/0Bjl+yp3qcm22n6B/mk+P/3Cbxo+bW3gsq5OLFNenQO3RMNM
i9RC+qJ82sgPXX6i9V/KszNxAyfegbMseoW9FcFwViD14giBQwA7NDw3ICm89PTj
y+YBMA50iRqdErmACz0fHfA/Ed5yu5cOVVa8DD12/upTzx7i0mmkAxwsKiktEaKQ
vg8i1gvzqeymWYnckGony08eCCIZFc78CeuhODy0+MXyrnBRP9p++fcQE7/GspKo
SbxVT3evwT2UkebezQT2+AL57NEnRsJzsgQM4R0sMgvZI7I6kfWKerhFMt3imSt1
QGphXmKZPRvKqib59U57GsZU1/2CMIlYBVMTZIpYKRh6NgE8ityaa4gehJDl16xa
pZ8z3DMNt3CRF8hqWmJNUfDwUvXBEk8d/8Lkh39/IFHbWqNJh6cgq3+CipXH5HjL
iVh7tzGPfB6yn+RETzcZjesZHtz4hFudOxTMV0YnTIv0FGtfxsfEQe7ZVmmfqGNG
glxE0EfbXt0psLXngFMneZYBJqXGFsK3r5bHjRm6wpC9EDAzXp+Tb+jQgs8t5eWV
xiQdBpNZnjnGiIOASOxJrIRuzbTjo389683NfLvPRY8eX1iEw58ebjLvDhvDZ2jS
pwGuWuJ/8QNZou1RfU5QL0M0SEe3ACm4wP5zfUGnW8o1vKY9rK5/9evIiA/DMAJ+
gF20Y6WzGg4llG9qCAnBkc3GgC7K1zkXU5N1VD50Y0qLoNsKy6eengXvmiL5EkFK
RnLtP45kD2rn6iZq3/Pnj1IfPonsdaNttb+2fhpFWa/r1sUyYadWeHs72vH83MgB I6h3Ae9ilF5tYLs2m6u8rKFM8zZhixSh =a8FR -----END PGP MESSAGE-----

Contrôle d’identité

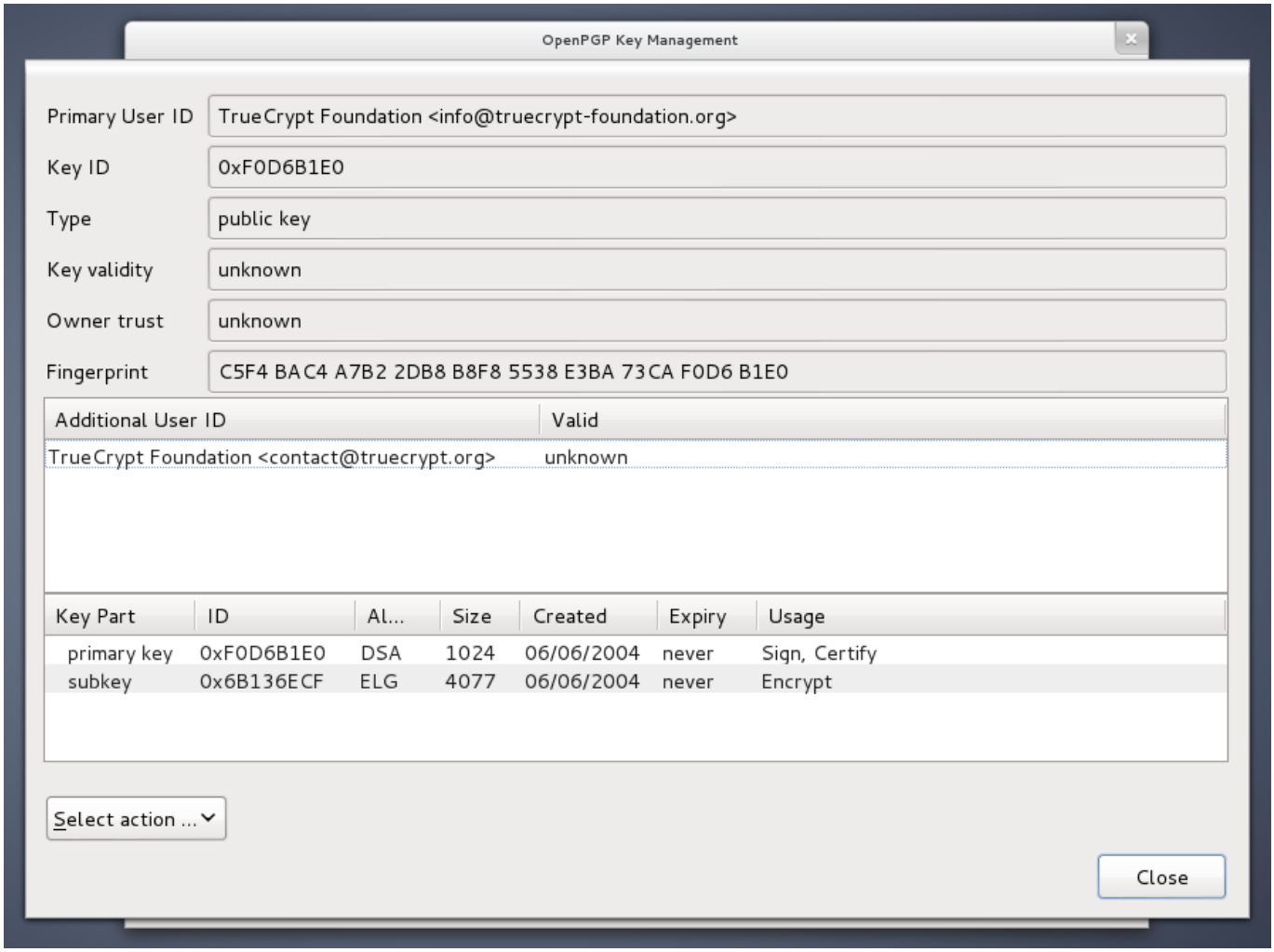
Comme avec l’OTR, il est important de vérifier les clés PGP

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.

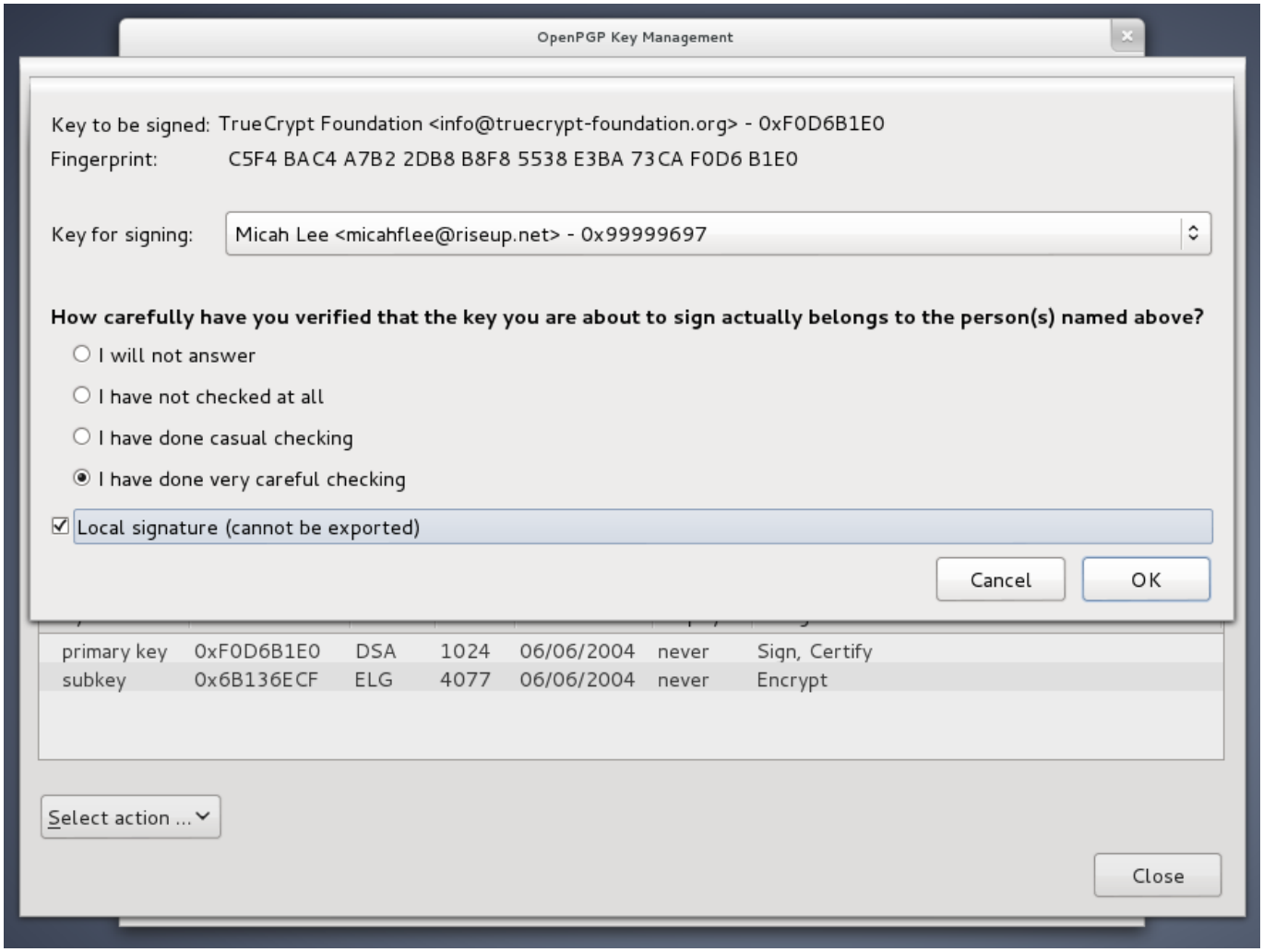
Comme avec les clés OTR, chaque clé PGP a une empreinte unique. Et comme pour OTR, vous avez besoin d'afficher l'intégralité de l'empreinte pour être sûr que la clé publique que vous êtes en train de regarder est bien celle de la personne à qui vous pensez qu'elle appartient.

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.