La NSA vous souhaite une bonne année 2041

La référence au célèbre roman d'Orwell *1984* a déjà beaucoup servi, on a pu en abuser pour alarmer inutilement et inversement pour rassurer de façon un peu rapide[1], tout comme on a tendance à voir partout des situations kafkaïennes, surréalistes ou ubuesques.

Pourtant lorsque ce sont des lanceurs d'alerte qui aujourd'hui font clairement appel à la dystopie d'Orwell, on est contraint de se poser sérieusement la question de la dérive totalitaire d'une société de surveillance de masse dont semaine après semaine ils dévoilent l'impressionnante étendue.

Voici par exemple un extrait des vœux d'Edward Snowden (à voir sur dailymotion) :

> *L'écrivain britannique Georges Orwell nous a avertis des dangers de ce type de surveillance. Mais les moyens de surveillance décrits dans son livre : les micros, les caméras, la télé qui nous espionnent, ne sont rien à côté des moyens disponibles aujourd'hui.*

Le journaliste Glenn Greenwald, intervenant récemment au 30e Chaos Communication Congress et qui a contribué activement à la diffusion des révélations d'Edward Snowden, nous livre ci-dessous une analyse assez alarmante et optimiste tout à la fois de ce qu'il appelle l'état de la surveillance, qui est aussi en l'occurrence la surveillance de l'état…

Pas de nouvelles révélations ici mais une réflexion sur la conscience de l'enjeu chez les lanceurs d'alerte devenus pour beaucoup des héros de la défense de nos libertés numériques, des considérations décapantes sur la servilité des médias à

l'égard de la parole institutionnelle, la nécessité d'adopter un solide chiffrement, et l'urgence de l'action nécessaire également pour tous ceux qui sont en capacité de brider les appétits de nos *surveillants*.

La conclusion assez glaçante est selon lui que la compulsion à la surveillance qui anime la NSA et les autres services de renseignement vise en réalité la disparition totale de toute vie privée.

Est-ce une vision paranoïaque ? À vous d'en juger. Gardons en tête toutefois que ce sont les mêmes personnes qui nous traitaient de paranoïaques il y a dix ans qui nous disent aujourd'hui : « bah, tout le monde le savait que nous étions espionnés, je ne vois pas ce que ça change », « moi je n'ai rien à cacher, etc. »

Le courage de Snowden, de Poitras, de Greenwald, d'Assange et de quelques autres activistes déterminés, dont on veut croire qu'ils sont de plus en plus nombreux, nous donne l'exemple d'une lutte active pour nos libertés à laquelle chacun à sa manière peut et doit contribuer.

- La vidéo intégrale en anglais sur YouTube
- l'enregistrement audio intégral
- La transcription en anglais de la conférence due à **poppingtonic**, elle est sous licence Creative Commons Attribution-ShareAlike 4.0 International License.
- La traduction intégrale de Korben sur son blog

Traduction Framasoft des extraits essentiels de la conférence : sinma, goofy, Bruno, KoS, Asta, Pol, + anonymes

* * * * *

Présentateur : …ces applaudissements étaient pour vous, Glenn ! bienvenue au 30ème Chaos Communication Congress à Hambourg. À vous de jouer.

Glenn Greenwald : Merci, merci beaucoup.

Merci à tous pour cet accueil chaleureux, et merci également aux organisateurs de ce congrès pour m'avoir invité à prendre la parole. Ma réaction, quand j'ai appris qu'on me demandait de faire le discours inaugural de cette conférence, a été la même que celle que vous auriez peut-être eue à ma place, c'est-à-dire : « hein, quoi ? »

La raison en est que mes compétences cryptographiques et de hacker ne sont pas, c'est le moins que l'on puisse dire, reconnues mondialement. Vous le savez, on a déjà raconté plusieurs fois comment la couverture de la plus importante histoire de sécurité nationale de la dernière décennie a failli me filer entre les doigts, parce que je trouvais l'installation de PGP d'une difficulté et d'un ennui insurmontables.

Il existe une autre anecdote, très semblable, qui illustre le même problème, et qui je pense n'a pas encore été racontée, la voici : avant de me rendre à Hong Kong, j'ai passé de nombreuses heures avec Laura Poitras et Edward Snowden, à essayer de me mettre à niveau très vite sur les technologies basiques de sécurité qui m'étaient nécessaires pour rendre compte de cette histoire. Ils ont essayé de me guider dans l'usage de toutes sortes d'applications, pour finalement arriver à la conclusion que la seule que je pouvais maîtriser, du moins à l'époque et à ce moment-là, était TrueCrypt.

Ils m'ont appris les rudiments de TrueCrypt, et quand je suis arrivé à Hong Kong, avant d'aller dormir, j'ai voulu jouer un peu avec. J'ai appris par moi-même quelques fonctionnalités qu'ils ne m'avaient pas indiquées et j'ai vraiment gagné en confiance. Le troisième ou quatrième jour, je suis allé les rencontrer tous les deux, tout gonflé de fierté. Je leur ai montré toutes les choses nouvelles que j'avais appris à faire tout seul avec TrueCrypt et je me voyais déjà le Grand Gourou de la crypto. J'avais atteint un niveau vraiment avancé. Je

les ai regardés tous les deux sans déceler la moindre admiration à mon égard. En fait, ce que j'ai vu, c'est qu'ils faisaient de gros efforts pour ne pas se regarder l'un l'autre avec les yeux qui leur sortaient de la tête.

Glenn Greenwald, photo par gage skidmore (CC BY-SA 2.0)

> *l'un des résultats les plus importants de ces six derniers mois… c'est le nombre croissant de personnes qui mesurent l'importance de la protection de la sécurité de leurs communications.*

Je leur ai demandé : « Pourquoi réagissez-vous ainsi ? Ce n'était pas un exploit de réussir ça ? ». Il y a eu un grand blanc. Aucun ne voulait me répondre, puis finalement Snowden a rompu le silence : « TrueCrypt est un truc que peut maîtriser votre petit frère, rien de bien impressionnant. »

Je me souviens avoir été très déconfit, et me suis remis au travail. Bon, c'était il y a six mois. Entre-temps, les technologies de sécurité et de confidentialité sont devenues d'une importance primordiale dans tout ce que j'ai pu

entreprendre. J'ai véritablement acquis des masses considérables de connaissances, à la fois sur leur importance et sur la façon dont elles fonctionnent. Je suis d'ailleurs loin d'être le seul. je pense que l'un des résultats les plus importants de ces six derniers mois, mais dont on a très peu débattu, c'est le nombre croissant de personnes qui mesurent l'importance de la protection de la sécurité de leurs communications.

Si vous regardez ma boîte mail depuis le mois de juillet, on y trouvait peut-être seulement 3 à 5 % des messages reçus chiffrés avec PGP. Ce pourcentage est passé à présent nettement au dessus des 50 %, voire plus. Quand nous avons débattu de la façon de monter notre nouvelle entreprise de presse, nous avons à peine passé quelques instants sur la question. Il était tout simplement implicite que nous allions tous faire usage des moyens de chiffrement les plus sophistiqués disponibles pour communiquer entre nous.

Et ce qui est à mon avis encore plus encourageant, c'est que toutes les fois où je suis contacté par des journalistes ou des activistes, ou quelqu'un qui travaille dans ce domaine, soit ils utilisent le chiffrement, soit ils sont gênés et honteux de ne pas savoir le faire, et dans ce cas s'excusent de leur méconnaissance et souhaitent apprendre à s'en servir bientôt.

C'est un changement radical vraiment remarquable, car même au cours de l'année dernière, toutes les fois où j'ai eu à discuter avec des journalistes spécialisés sur le sujet de la sécurité nationale dans le monde qui travaillaient sur quelques-unes des données les plus sensibles pratiquement aucun d'entre eux ne savait ce qu'était PGP ni OTR, ni n'avait connaissance des meilleures technologies qui permettent le renforcement de la confidentialité, et ne parlons même pas de savoir les utiliser. C'est vraiment encourageant de voir ces technologies se propager de façon généralisée.

> *Le gouvernement des États-Unis et ses alliés ne vont sûrement pas volontairement restreindre leur propre pouvoir de surveillance de manière significative.*

Je pense que cela souligne un point extrêmement important, un de ceux qui me rend très optimiste. On me demande souvent si je pense que tout ce que nous avons appris au cours des six derniers mois, les déclarations et les débats qui ont été soulevés vont finalement changer quoi que ce soit et imposer une limite quelconque à l'état de la surveillance par les États-Unis.

Typiquement, quand les gens pensent que la réponse à cette question est oui, la chose qu'ils répètent le plus communément et qui est sans doute la moins significative, c'est qu'il se produira une sorte de débat, et que nos représentants, dans un régime démocratique, seront en mesure d'apporter des réponses à nos interrogations, et qu'ainsi ils vont imposer des limites en réformant la législation.

Rien de tout cela ne va probablement arriver. Le gouvernement des États-Unis et ses alliés ne vont sûrement pas volontairement restreindre leur propre pouvoir de surveillance de manière significative. En fait, la tactique du gouvernement états-unien que nous voyons sans cesse à l'œuvre, et que nous avons toujours constatée, consiste à faire exactement l'inverse : lorsque ces gens sont pris sur la main dans le sac et que cela jette le discrédit sur eux en provoquant scandales et polémiques, ils sont très habiles pour faire semblant de se réformer par eux-mêmes avec des gestes symboliques. Mais dans le même temps, ils ne font qu'apaiser la colère des citoyens et souvent augmenter leurs propre pouvoirs, qui pourtant sont à l'origine du scandale.

On l'a vu au milieu des années 70, quand on s'est sérieusement inquiété aux États-Unis, au moins autant qu'aujourd'hui, des capacités de surveillance et d'abus du gouvernement. La

réaction du gouvernement a été de déclarer : « d'accord, nous allons nous engager dans toutes ces réformes, qui vont imposer des garde-fous à ces pouvoirs. Nous allons créer un tribunal spécial que le gouvernement devra saisir pour en avoir la permission avant de cibler les gens à surveiller. »

Cela sonnait bien, mais ils ont créé le tribunal de la façon la plus tordue possible. C'est un tribunal secret, devant lequel seul le gouvernement comparaît, où seuls les juges les plus pro-sécurité nationale sont nommés. Donc, ce tribunal donnait l'apparence d'une supervision quand, en réalité, c'était la chambre d'enregistrement la plus grotesque de tout le monde occidental. Il ne s'opposait quasiment jamais à quoi que ce soit. Ça créait simplement l'illusion qu'il existait un contrôle judiciaire.

Ils ont aussi prétendu qu'ils allaient créer des commissions au Congrès. Des commissions « de surveillance » qui auraient pour principal objectif de superviser les commissions sur le renseignement pour s'assurer qu'elles n'abusaient pas de leurs pouvoirs. Ce qu'ils ont fait en réalité c'est nommer immédiatement à la tête de ces commissions « de surveillance » les plus serviles des loyalistes.

Voilà des décennies que cela dure, et aujourd'hui nous avons deux membres les plus serviles et pro-NSA du Congrès à la tête de ces comités, qui sont là en réalité pour soutenir et justifier tout et n'importe quoi de la part de la NSA plutôt que de s'engager dans un véritable contrôle. Donc, encore une fois, tout est fait pour embellir le processus sans entamer de véritable réforme.

Ce processus est maintenant en train de se reproduire. Vous voyez le Président nommer une poignée de ses plus proches partisans dans ce « comité indépendant de la Maison Blanche » qui fait semblant de publier un rapport très équilibré et critique sur la surveillance étatique, mais en réalité, propose toute une gamme de mesures qui, au mieux, aboutiraient

tout simplement à rendre ces programmes un peu plus acceptables aux yeux du public, et dans de nombreux cas, accroîtraient encore les capacités de la surveillance étatique, plutôt que de la brider de manière significative.

Alors pour savoir si nous aurons ou non des réformes significatives, il ne faut pas compter sur le processus classique de la responsabilité démocratique que nous avons tous appris à respecter. Il faut chercher ailleurs. Il est possible que des tribunaux imposeront des restrictions significatives en jugeant les programmes de surveillance contraires à la constitution.

Il est beaucoup plus probable que d'autres pays dans le monde qui sont vraiment indignés par les violations de la sécurité de leur vie privée sauront s'unir et créer des alternatives, soit en termes d'infrastructures, soit en termes juridiques pour empêcher les États-Unis d'exercer leur hégémonie sur Internet ou faire en sorte que le prix en soit beaucoup trop élevé. Je pense, c'est encore plus prometteur, que les grandes sociétés privées, les entreprises de l'Internet et bien d'autres commenceront enfin à payer le prix de leur collaboration avec ce régime d'espionnage.

> *…savoir si oui ou non Internet sera réellement cet outil de libération et de démocratisation ou s'il deviendra le pire outil de l'oppression humaine de toute l'histoire de l'humanité.*

Nous avons déjà vu comment cela se passe quand leurs actions sont exposées au grand jour ; c'est alors qu'ils sont obligés de rendre des comptes pour tout ce qu'ils font, et ils prennent conscience que leurs intérêts économiques sont mis en péril par le système d'espionnage. Ils utilisent leur puissance inégalée pour exiger qu'il soit freiné. Je pense que tous ces éléments pourront vraisemblablement imposer de sérieuses limites à la surveillance d'état.

Mais en fin de compte je pense que les plus grands espoirs résident dans les personnes qui sont dans cette salle de conférence et dans les compétences que vous tous possédez. Les technologies de protection de la vie privée qui ont déjà été développées, telles que le navigateur Tor, PGP, OTR et toute une série d'autres applications, constituent autant de réels progrès pour empêcher le gouvernement des USA et ses alliés de faire intrusion dans le sanctuaire de nos communications privées.

Aucune de ces technologies n'est parfaite. Aucune n'est invulnérable, mais elles représentent toutes un sérieux obstacle aux capacités du gouvernement des États-Unis à s'attaquer toujours davantage à notre vie privée. Et en fin de compte, le combat pour la liberté d'Internet, la question qui va se jouer je pense, principalement, sur le terrain de guerre technologique, est de savoir si oui ou non Internet sera réellement cet outil de libération et de démocratisation ou s'il deviendra le pire outil de l'oppression humaine de toute l'histoire de l'humanité.

La NSA et le gouvernement américain le savent certainement. C'est pourquoi Keith Alexander enfile son petit déguisement, ses jeans de papa, son tee-shirt noir de rebelle et va aux conférences de hackers.

Et c'est pour cela que les entreprises de la Silicon Valley, comme Palantir Technologies, déploient tant d'efforts à se dépeindre comme des rebelles luttant pour les libertés civiles, alors qu'elles passent la plupart de leur temps à travailler main dans la main avec les agences de renseignement et la CIA pour accroître leurs capacités. Elles cherchent en effet à attirer les jeunes cerveaux de leur côté, du côté de la destruction de la vie privée et de la mise d'Internet au service des organisations les plus puissantes du monde.

Quelle sera l'issue de ce conflit, que deviendra Internet ? Nous ne pouvons pas encore répondre de façon définitive à ces

questions. Cela dépend beaucoup de ce que nous, en tant qu'êtres humains, pourrons faire. L'une des questions les plus urgentes est de savoir si les personnes comme celles qui sont dans cette pièce – les personnes qui ont les pouvoirs que vous avez maintenant et aurez à l'avenir – succomberont à la tentation et travailleront pour les entités qui tentent de détruire la vie privée dans le monde, ou si vous mettrez vos talents, vos compétences et vos ressources au service de la défense du genre humain contre ces intrusions et continuerez à créer des technologies destinées à protéger notre vie privée. Je suis très optimiste car ce pouvoir est vraiment entre vos mains.

Je veux aborder une autre de mes raisons d'être optimiste : la coalition de ceux qui militent pour la défense de la vie privée est beaucoup plus solide et plus dynamique. Elle est à mon avis beaucoup plus grande et plus forte que beaucoup d'entre nous, même ceux qui en font partie, ne l'estiment ou n'en ont conscience. Plus encore, elle est en croissance rapide. Et je pense que cette croissance est inexorable.

Laura Poitras, image de Kris Krug via Wikimedia (CC-BY-SA)

Je suis conscient, en ce qui me concerne, que tout ce que j'ai pu faire sur tout ce dossier au cours des six derniers mois, toutes les tribunes qu'on m'a offertes, comme ce discours et les honneurs que j'ai reçus, et les éloges que j'ai reçus, je dois le partager entièrement avec deux personnes qui ont été

d’une importance capitale pour tout ce que j’ai fait. L’une d’elles est ma collaboratrice incroyablement courageuse et extrêmement brillante, Laura Poitras.

Vous savez, Laura n’attire pas énormément l’attention, elle aime qu’il en soit ainsi, mais elle mérite vraiment la plus grande reconnaissance, les plus grands honneurs et les récompenses parce que même si ça sonne cliché, c’est vraiment l’occasion de le dire : sans elle, rien de tout cela n’aurait été possible.

Nous avons pris la parole pratiquement tous les jours, au cours des six derniers mois. Nous avons pris presque toutes les décisions, en tout cas toutes celles qui étaient les plus importantes, en partenariat complet et de façon collaborative. Être capable de travailler avec quelqu’un qui a ce niveau élevé de compréhension de la sécurité sur Internet, sur les stratégies de protection de la vie privée, a été complètement indispensable à la réussite de ce que nous avons pu réaliser.

Et puis, la deuxième personne qui a été tout à fait indispensable et mérite les plus grands éloges, et de partager les plus hautes récompenses, c’est mon héros toutes catégories, Edward Snowden.

Il est vraiment difficile de trouver des mots pour dire à quel point son choix a eu de l’impact sur moi, sur Laura, sur les personnes avec qui nous avons travaillé directement ou indirectement, et encore sur des millions et des millions de personnes à travers le monde. Le courage dont il a fait preuve et les actions qu’il a menées selon des principes dictés par sa conscience vont me façonner et m’inspirer pour le reste de ma vie, et vont inspirer et convaincre des millions et des millions de personnes de prendre toutes sortes d’initiatives qu’elles n’auraient pas prises si elles n’avaient pas vu quel bien un seul individu peut faire au monde entier.

Photo par PM Cheung (CC BY 2.0)

Mais je pense que le plus important est de comprendre, et pour moi, c'est le point décisif, qu'aucun d'entre nous, nous trois, n'a fait ce que nous avons fait à partir de rien. Nous avons tous été inspirés par des gens qui ont fait des choses semblables dans le passé. Je suis absolument certain que Edward Snowden a été inspiré de toutes sortes de façons par l'héroïsme et l'abnégation de Chelsea Manning.

Je suis persuadé que, d'une façon ou d'une autre, elle a été inspirée par toute la cohorte des lanceurs d'alertes et par qui possèdent cette même conscience et l'ont précédée, en dénonçant les niveaux extrêmes de corruption, les méfaits et les illégalités commises par les institutions les plus puissantes de ce monde. Ils ont été inspirés à leur tour, je suis sûr, par l'un de mes plus grands héros politiques, Daniel Ellsberg, qui a fait la même chose quarante ans plus tôt.

Mais au-delà de tout cela, je pense qu'il est réellement important de prendre conscience de ceci : tout ce qu'il nous a été permis de faire tout au long de ces six derniers mois, et je pense, tous ces types de fuites significatives et révélations de documents classés *secret défense* à l'ère du numérique, à la fois dans le passé et le futur, tout cela nous

incite à la plus grande des reconnaissances pour l'organisation qui a donné la première l'exemple à suivre, il s'agit de WikiLeaks.

(…)

Edward Snowden a été sauvé, lorsqu'il était à Hong Kong, du risque d'arrestation et d'emprisonnement aux États-unis pour les trente prochaines années, non par le seul fait de WikiLeaks, mais aussi par une femme d'un courage et d'un héroïsme extraordinaires, Sarah Harrison.

Il existe un vaste réseau de personnes à travers le monde, qui croient en cette cause, et ne se contentent pas d'y croire, mais aussi sont de plus en plus nombreux à vouloir lui vouer leur énergie, leurs ressources, leur temps, et à se sacrifier pour elle. Il y a une raison décisive, et cela m'est apparu au cours d'une conversation téléphonique avec Laura, il y a probablement deux mois. (…) Elle a énuméré une liste de gens qui se sont dévoués personnellement à la transparence et au prix qu'ils ont eu à payer. Elle a dit qu'Edward Snowden était coincé en Russie, sinon il devrait faire face à 30 années de prison, Chelsea Manning est en prison, Aaron Swartz s'est suicidé. D'autres comme Jeremy Hammond et Barrett Brown font l'objet de poursuites judiciaires tellement excessives qu'elles en sont grotesques au nom d'actions de transparence pour lesquelles ils se sont engagés. Même des gens comme Jim Risen, qui appartient à une institution comme le New York Times, doivent affronter le risque d'un emprisonnement pour les informations qu'ils ont publiées.

D'innombrables juristes nous ont informés, Laura et moi, que nous ne serions pas en sécurité en voyageant, même pour retourner dans notre propre pays, et elle a dit : « voilà bien un symptôme de la maladie qui affecte notre avenir politique, quand on voit que pour avoir mis en lumière ce que fait le gouvernement et avoir fait le travail que ni les médias ni le Congrès ne font, le prix à payer est une forme extrême de

punition. »

(…)

Les États-Unis savent que leur seul espoir pour continuer à maintenir le régime du secret, derrière lequel ils s'abritent pour mener des actions radicales et illégales, consiste à intimider, dissuader et menacer les lanceurs d'alerte potentiels et les militants pour la transparence. Il s'agit de les empêcher de se lever pour faire ce qu'ils font, en leur montrant qu'ils seraient soumis aux plus extrêmes châtiments et que personne ne peut rien y faire.

C'est une tactique efficace. Elle fonctionne pour certains, non pas parce qu'ils sont lâches mais parce qu'ils font un calcul rationnel. (…) Il y a donc des activistes qui en concluent rationnellement que le prix à payer pour leur engagement dans ce combat est pour eux trop élevé. Et c'est pourquoi les gouvernements peuvent continuer. Mais le paradoxe c'est qu'il existe un grand nombre de personnes, elle sont même je crois plus nombreuses, qui réagissent de façon totalement inverse.

> *les États-Unis et leurs plus proches alliés sèment malgré eux les germes de l'opposition, et nourrissent eux-mêmes la flamme de l'activisme à cause de leur propre comportement abusif.*

Quand ils voient que les gouvernements britannique et états-unien révèlent leur véritable visage, en montrant à quel point ils sont déterminés à abuser de leurs pouvoirs, ils ne sont pas effrayés ni dissuadés, leur courage en est même au contraire renforcé. En voici la raison : quand vous voyez que ces gouvernements sont réellement capables d'un tel niveau d'abus de pouvoir, vous prenez conscience que vous ne pouvez plus en toute conscience rester là sans rien faire. Il devient pour vous encore plus impératif de mettre en pleine lumière ce que font les gouvernements, et si vous écoutez tous ces

lanceurs d’alerte ou activistes, ils vous diront la même chose.

Il a fallu un long processus pour prendre conscience que les actions qu’ils entreprenaient étaient justifiées, mais en définitive ce sont les actions de ces gouvernements qui les ont convaincus. C’est d’une ironie savoureuse, et je pense que ça peut rendre vraiment optimiste, de savoir que les États-Unis et leurs plus proches alliés sèment malgré eux les germes de l’opposition, et nourrissent eux-mêmes la flamme de l’activisme à cause de leur propre comportement abusif.

Maintenant, à propos de tentatives d’intimidation et de dissuasion, et autres manœuvres, je voudrais simplement passer quelques minutes à parler de l’attitude actuelle du gouvernement des États-Unis envers Edward Snowden. Il est devenu très clair, à ce stade, que le gouvernement des États-Unis, du plus haut niveau jusqu’au plus bas, est totalement déterminé à poursuivre un seul résultat. Ce résultat est qu’Edward Snowden finisse par passer plusieurs décennies, sinon le reste de sa vie, dans une petite cage, probablement coupée, en termes de communication, du reste du monde.

Et la raison pour laquelle ils ont cette intention n’est pas difficile à comprendre. Ce n’est pas parce qu’ils sont furieux, ou parce que la société doit être protégée d’Edward Snowden, ou pour l’empêcher de recommencer. Je crois qu’on peut parier à coup sûr que le niveau de sécurité d’Edward Snowden est révoqué de façon plus ou moins permanente.

La raison pour laquelle ils sont tellement résolus c’est qu’ils ne peuvent pas laisser Edward Snowden mener la moindre vie décente et libre parce qu’ils sont tétanisés à l’idée que cela va inciter d’autres personnes à suivre son exemple, et à ne plus vouloir garder le secret qui les lie et qui ne sert à rien d’autre que dissimuler leur conduite illégale et dommageable à ceux qui en sont les plus victimes.

Et ce que je trouve le plus étonnant à ce sujet n'est pas que le gouvernement des États-Unis soit en train de faire ça, car ils le font. C'est ce qu'ils *sont*. Ce que je trouve étonnant, c'est qu'il y ait de si nombreux gouvernements à travers le monde, y compris ceux qui sont en mesure de protéger les droits de l'homme, et qui ont été les plus grands bénéficiaires des révélations héroïques de Snowden, qui sont pourtant prêts à rester là à regarder ses droits individuels être foulés aux pieds, à le laisser emprisonner pour avoir commis le crime de dévoiler aux gens du monde entier ce qu'on fait de leur vie privée.

C'était vraiment surprenant d'observer les gouvernements, y compris certains des plus grands en Europe, et leurs dirigeants, exprimer en public une intense indignation parce que la vie privée de leurs citoyens est systématiquement violée, et une véritable indignation quand ils apprennent que leur propre vie privée a également été pris pour cible[2].

Pourtant, dans le même temps, la personne qui s'est sacrifiée pour défendre leurs droits fondamentaux, leur droit à la vie privée, voit maintenant ses propres droits visés et menacés en rétorsion. Et je me rends compte que pour un pays comme l'Allemagne ou la France, ou le Brésil, ou tout autre pays dans le monde, défier les diktats des États-Unis, ça coûte relativement cher. Mais le prix à payer était bien plus élevé pour Edward Snowden quand il a choisi de se manifester et de faire ce qu'il a fait pour la défense de vos droits, et pourtant il l'a fait malgré tout.

Je pense qu'il est réellement important de prendre conscience que les pays ont les obligations légales et internationales, en vertu des traités qu'ils ont signés, qui leur rend difficile de défendre Edward Snowden des poursuites judiciaires, de l'empêcher d'être en cage pour le restant de ses jours, pour avoir fait la lumière sur les atteintes systématiques à la vie privée, et d'autres formes d'abus

relatifs au secret. Mais ces pays ont également les obligations morales et éthiques en tant que bénéficiaires de ses actions, de ce qu'il a fait pour eux, et cela consiste à protéger ses droits en retour.

Je veux prendre une petite minute pour parler de l'un de mes thèmes favoris, le journalisme. Quand j'étais à Hong Kong, avec Laura et Edward Snowden, et que j'ai eu pas mal à réfléchir à ce sujet pour l'écriture d'un livre sur les évènements des derniers mois, une des choses dont j'ai pris conscience avec le recul et aussi en discutant avec Laura, était que nous avions passé au moins autant de temps à aborder des questions de journalisme et de presse libre que la question de la surveillance. Car nous savions que ce que nous étions en train de faire déclencherait autant de débats sur le rôle propre du journaliste vis-à-vis de l'état et d'autres puissantes institutions qu'il y en aurait sur l'importance de la liberté et de la vie privée sur Internet et les menaces de la surveillance d'état.

Nous savions, en particulier, que nos plus formidables adversaires n'allaient pas être seulement les agences de renseignements sur lesquelles nous enquêtions, et dont nous tentions de révéler les pratiques, mais aussi leurs plus loyaux et dévoués serviteurs, j'ai nommé : les médias américains et britanniques.

(…)

Une des choses les plus remarquables qui me soit arrivées est l'interview que j'ai livrée, il y a environ trois semaines sur la BBC, c'était pendant ce programme appelé Hard Talk, et personnellement, à un moment donné, j'ai pensé (…) que les officiels de la sécurité nationale mentaient de façon routinière à la population dans le but de protéger leur pouvoir et de faire avancer leur agenda, et que le but et devoir d'un journaliste est d'être le contradicteur de ces gens de pouvoir, que les déclarations que mon intervieweur

énonçait – pour dire à quel point ces programmes gouvernementaux sont essentiels pour empêcher les terroristes de nuire – ne devraient pas être crues à moins qu'il ne produise une preuve tangible de leur véracité.

Lorsque j'ai dit ceal il m'a interrompu (désolé, j'imite mal l'accent britannique, alors vous allez devoir l'imaginer) et a dit : « Je dois vous interrompre, vous venez de dire quelque chose d'étonnant ! » Il était comme un prêtre victorien scandalisé en voyant une femme soulever sa jupe au dessus de ses chevilles.

Il a dit : « J'ai peine à croire que vous suggériez que des hauts fonctionnaires, des généraux des États-Unis et du gouvernement britannique, font en réalité de fausses déclarations au public ! Comment vous est-il possible de dire cela ? »

Et ceci n'est pas aberrant. C'est vraiment le point de vue des grands noms des médias états-uniens et britanniques, particulièrement lorsque des gens avec des tas de médailles épinglées sur la poitrine, qu'on appelle des généraux, mais aussi des officiels hauts placés du gouvernement, font des déclarations, et que leurs affirmations sont à priori traitées comme vraies sans la moindre preuve, et qu'il est presque indécent de les remettre en question, ou de s'interroger sur leur véracité.

Évidemment, nous avons connu la guerre en Irak, sur laquelle deux gouvernements très moraux ont particulièrement et délibérément menti à plusieurs reprises à leur peuple, pendant deux années entières, pour justifier une guerre d'agression qui a détruit un pays de 26 millions de personnes.

Mais nous l'avons vu aussi en permanence au cours des six derniers mois. Le tout premier document qu'Edward Snowden m'a montré contenait une information dont il m'a expliqué qu'elle révélerait le mensonge incontestable d'un responsable du

renseignement national senior du président Obama, le directeur du renseignement national, James Clapper. C'est le document qui a révélé que l'administration Obama a réussi à convaincre un tribunal secret d'obliger les compagnies de téléphone à communiquer à la NSA chaque enregistrement de conversation téléphonique, de chaque appel téléphonique unique, local et international, de chaque Américain.

Et pourtant ce fonctionnaire de la sécurité nationale, James Clapper, devant le Sénat, quelques mois plus tôt, auquel on a demandé : « Est-ce que la NSA recueille des données complètes sur les communications des Américains ? » a répondu : «Non, monsieur » mais nous savons tous maintenant que c'était un parfait mensonge.

La NSA et les hauts responsables du gouvernement américain ont raconté bien d'autres mensonges. Et par « mensonge » je veux dire qu'ils ont menti sciemment, en racontant des choses qu'ils savaient pourtant être fausses pour convaincre les gens de ce qu'ils voulaient leur faire croire. Keith Alexander, le chef de la NSA, a déclaré à maintes reprises qu'ils étaient incapables de rendre compte du nombre exact d'appels et de courriels interceptés sur le système de télécommunications américain, alors même que le programme que nous avons fini par révéler, *Boundless Informant*, dénombre avec une précision mathématique exactement les données qu'il a dit être incapable de fournir.

Autre exemple, la NSA et le GCHQ ont déclaré à plusieurs reprises que le but de ces programmes est de protéger les gens contre le terrorisme, et de protéger la sécurité nationale, et qu'ils ne seraient jamais, contrairement à ce que font ces méchants Chinois, utilisés pour de l'espionnage à des fins économiques.

Et pourtant, au fil des rapports qui nous sont révélés, depuis l'espionnage du géant pétrolier brésilien Petrobas en passant par l'espionnage de l'organisation des états américains et des

sommets économiques où des accords économiques d'envergure ont été négociés, par l'espionnage des sociétés d'énergie à travers le monde ou en Europe, en Asie et en Amérique latine, le gouvernement américain continue de nier toutes ces allégations et les considère comme des mensonges.

Et puis nous avons le président Obama qui a fait à plusieurs reprises des déclarations telles que « Nous ne pouvons pas et n'effectuons pas de surveillance ou d'espionnage sur les communications des Américains sans l'existence d'un mandat » et ceci alors même que la loi de 2008 adoptée par le Congrès dont il faisait partie permet au gouvernement des États-Unis d'intercepter les conversations et les communications des Américains sans mandat.

Et ce que vous voyez ici, c'est un mensonge complet. Pourtant, dans le même temps, les mêmes médias qui le constatent poussent les hauts cris si vous suggérez que leurs déclarations ne doivent pas être prises pour argent comptant, sans preuve, parce que leur rôle n'est pas d'être des contradicteurs. Leur rôle est d'être les porte-paroles fidèles de ces puissantes institutions qui prétendent exercer un contrôle.

Vous pouvez très bien allumer la télévision, à tout moment, ou visiter un site web, et voir de très courageux journalistes qualifier Edward Snowden de criminel et demander qu'il soit extradé aux États-Unis, poursuivi et emprisonné. Ils sont très très courageux quand il s'agit de s'attaquer à des personnes qui sont méprisées à Washington, qui n'ont aucun pouvoir et sont marginalisées. Ils font preuve de beaucoup de courage pour les condamner, se dresser contre eux et exiger que les lois s'appliquent à eux avec rigueur.« Il a transgressé les lois, il doit en payer les conséquences ».

Et pourtant, le responsable de la sécurité nationale au plus haut niveau du gouvernement états-unien est allé au Sénat et leur a menti les yeux dans les yeux, chacun le sait

maintenant, ce qui constitue au moins un crime aussi grave que n'importe quel délit dont Edward Snowden est accusé.

Vous serez bien en peine de trouver ne serait-ce qu'un seul de ces intrépides et résolus journalistes, pour oser imaginer et encore moins exprimer l'idée que le directeur du renseignement national James Clapper devrait être soumis à la rigueur de la loi, poursuivi et emprisonné pour les crimes qu'il a commis, parce que le rôle des médias américains et de leurs homologues britanniques est d'être la voix de ceux qui ont le plus de pouvoir, de protéger leurs intérêts et de les servir.

Tout ce que nous avons fait au cours des six derniers mois, et tout ce que nous avons décidé le mois dernier pour fonder une nouvelle organisation médiatique, consiste à essayer de renverser ce processus et à ranimer la démarche journalistique pour ce qu'elle était censé être, c'est-à-dire une véritable force de contradiction, de contrôle de ceux qui ont le plus grand pouvoir.

> *le but de la NSA, et de ses complices anglo-saxons, le Canada, la Nouvelle Zélande, l'Australie et plus spécialement le Royaume-Uni, c'est d'éliminer la vie privée de la surface du globe.*

Je veux simplement terminer par un dernier point, il s'agit de la nature de cet état de surveillance que nous avons dévoilé ces six derniers mois. Dès que je donne une interview, les gens me posent des questions comme : quelle est l'histoire la plus importante que j'ai eu à révéler, ou que nous apprend la dernière histoire que je viens de publier. Et ce que j'ai commencé à répondre pour de bon, c'est qu'il n'y a véritablement qu'un seul point primordial que toutes ces histoires ont révélé.

Et voici ce qu'il en est, je l'affirme sans la moindre hyperbole ni dramatiser, ce n'est ni métaphorique ni caricatural, c'est littéralement la vérité : le but de la NSA,

et de ses complices anglo-saxons, le Canada, la Nouvelle Zélande, l'Australie et plus spécialement le Royaume-Uni, c'est d'éliminer la vie privée de la surface du globe. Pour s'assurer qu'il ne subsiste aucune communication numérique humaine qui échappe à leur réseau de surveillance.

Ils veulent s'assurer que toute forme humaine de communication, que cela soit par téléphone ou Internet ou toute activité en ligne, puisse être collectée, contrôlée, enregistrée, et analysée par cette agence, et par leurs alliés. Décrire cela revient à décrire une omniprésence de l'état de surveillance. Il n'est pas nécessaire d'user d'hyperboles pour évoquer ce point, et vous n'avez pas besoin de me croire quant je dis que c'est leur but. Document après document, les archives livrées par Edward Snowden affirment que tel est bien leur objectif. Ils sont obsédés par la recherche de la plus petite faille sur cette terre par laquelle pourrait passer une communication échappant à leur interception.

(…) la NSA et la GCHQ enragent à l'idée que vous pouvez monter dans un avion et faire l'usage de certains téléphones portables ou services internet tout en étant à l'abri de leur regards indiscrets pour quelques heures d'affilée. Ils s'obstinent à chercher des moyens de s'introduire dans les systèmes embarqués dédiés aux services mobiles et internet. La simple idée que les êtres humains puissent communiquer, même pour un court instant, sans qu'il puisse y avoir de collecte, de stockage, d'analyses et de surveillance sur ce que nous disons, leur est tout simplement intolérable. Les institutions les ont mandatés pour ça.

> *Quand vous réfléchissez sur le monde dans lequel on a le droit d'éliminer la vie privée, vous parlez en réalité d'éliminer tout ce qui donne sa valeur à la liberté individuelle.*

Et quand on me pose des questions, quand je donne des interviews dans différents pays, eh bien c'est du genre : « Pourquoi voudraient-ils espionner cet officiel ? » ou « Pourquoi voudraient-ils espionner la Suède ? » ou « Pourquoi voudraient-ils cibler cette entreprise-là ? ». Le postulat de cette question est vraiment erroné. Le postulat de cette question est que la NSA et le GCHQ ont besoin d'une raison spécifique pour cibler quelqu'un pour le surveiller. Or ce n'est pas comme cela qu'ils pensent. Ils ciblent chaque forme de communication sur laquelle ils peuvent mettre la main. Et si vous pensez à l'utilité de la vie privée pour nous, en tant qu'êtres humains, sans même aborder son utilité au plan politique, c'est vraiment ce qui nous permet d'explorer les limites et de nous engager dans la créativité, et utiliser les mécanismes de dissidence sans crainte. Quand vous réfléchissez sur le monde dans lequel on a le droit d'éliminer la vie privée, vous parlez en réalité d'éliminer tout ce qui donne sa valeur à la liberté individuelle.

L'état de surveillance, est nécessairement, par son existence même, un générateur de conformisme, car lorsque des êtres humains savent qu'ils sont toujours susceptibles d'être observés, même s'ils ne sont pas systématiquement surveillés, les choix qu'ils font sont de loin beaucoup plus contraints, beaucoup plus limités, se coulent plus étroitement dans le moule de l'orthodoxie qu'ils ne le feraient dans leur véritable vie privée.

Voilà précisément pourquoi la NSA et la GCHQ , et les tyrannies les plus puissantes de ce monde, actuellement et tout au long de l'histoire, ont toujours eu comme premier objectif en haut de leur agenda, l'éradication de la vie privée : cela leur garantit que les individus ne pourront plus résister longtemps aux diktats qu'ils leur imposent.

Eh bien, encore une fois, merci beaucoup.

* * * * *

À voir aussi :

- la fort intéressante intervention de Jacob Appelbaum au 30c3 https://www.youtube.com/watch?v=b0w36GAyZIA
- un appel d'Assange aux administrateurs système pour qu'ils investissent les services de renseignement et fuitent les informations

Notes

[1] Un moment de recyclage très troublant rétrospectivement est le clip promotionnel d'Apple en 1984 (une minute à regarder sur YouTube) qui s'achevait par « vous allez voir pourquoi 1984 ne ressemblera pas à "*1984*" »

[2] [Note de l'éditeur] On ne peut s'empêcher d'opérer un rapprochement avec un élément d'actualité récente : le président Hollande réclamant (à juste titre) le respect de sa vie privée, tandis qu'il y a quelques semaines à peine le parlement votait pour une loi de programmation militaire dont un des articles faisait bien peu de cas de la vie privée des citoyens ordinaires

---

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.

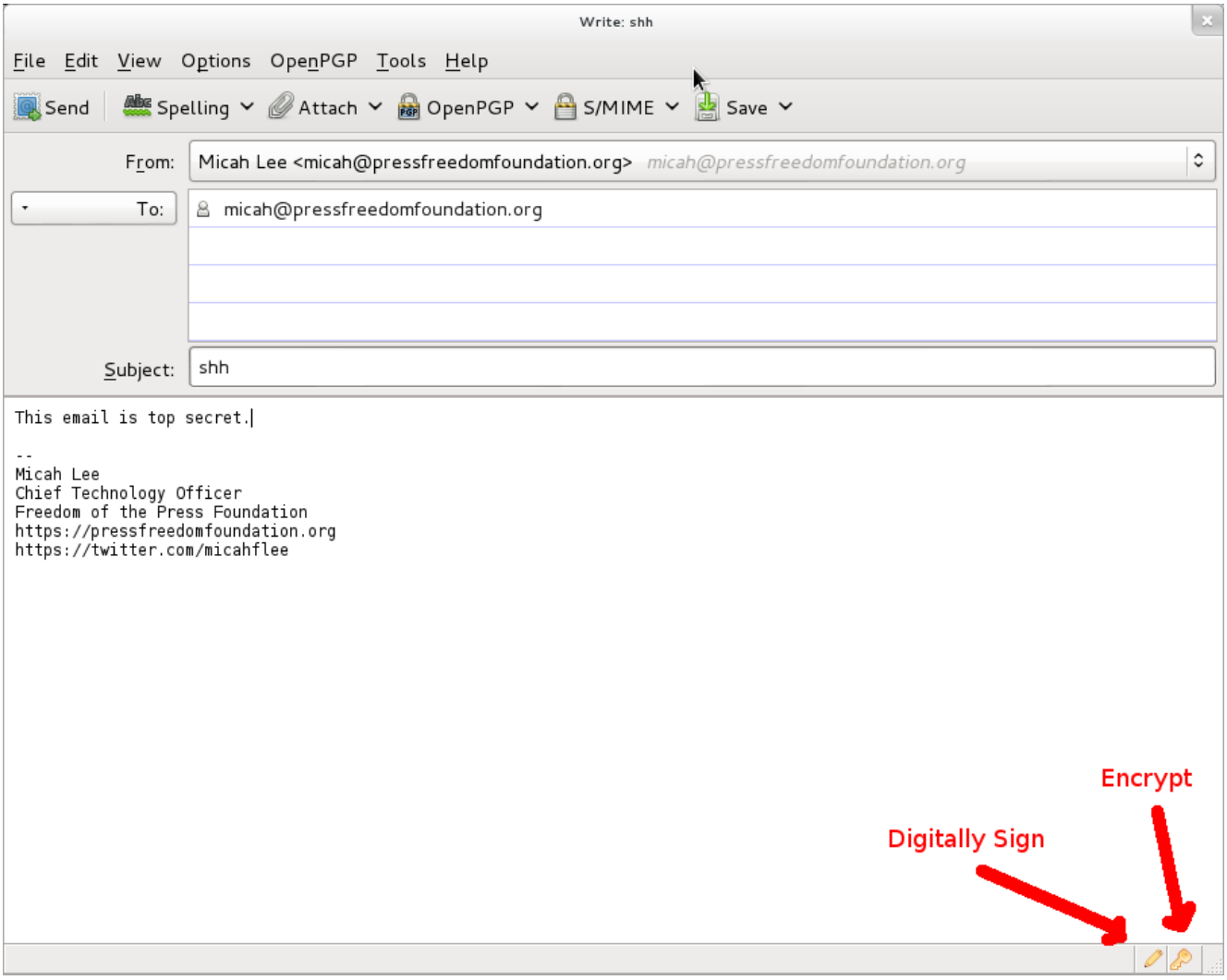
Vous devrez télécharger un client messagerie pour utiliser PGP correctement. Un client de messagerie est un programme sur votre ordinateur que vous ouvrez pour vérifier vos courriels, contrairement à l'utilisation de votre navigateur web. La configuration PGP la plus populaire est le client de messagerie 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.

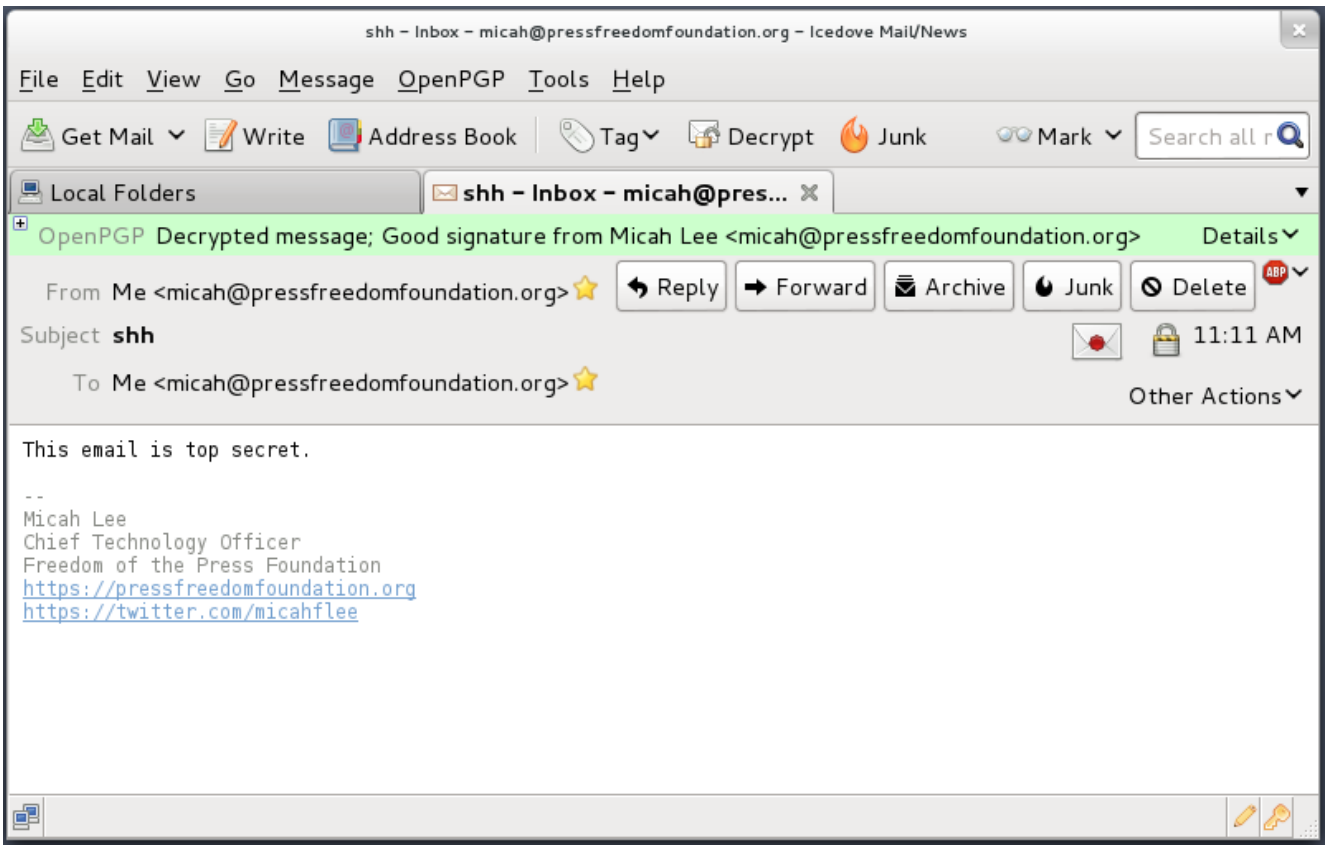
Il est possible d'utiliser un chiffrement PGP avec Gmail, mais la façon la plus simple est de passer par un client de messagerie comme Thunderbird et de configurer votre compte Gmail à travers lui.

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

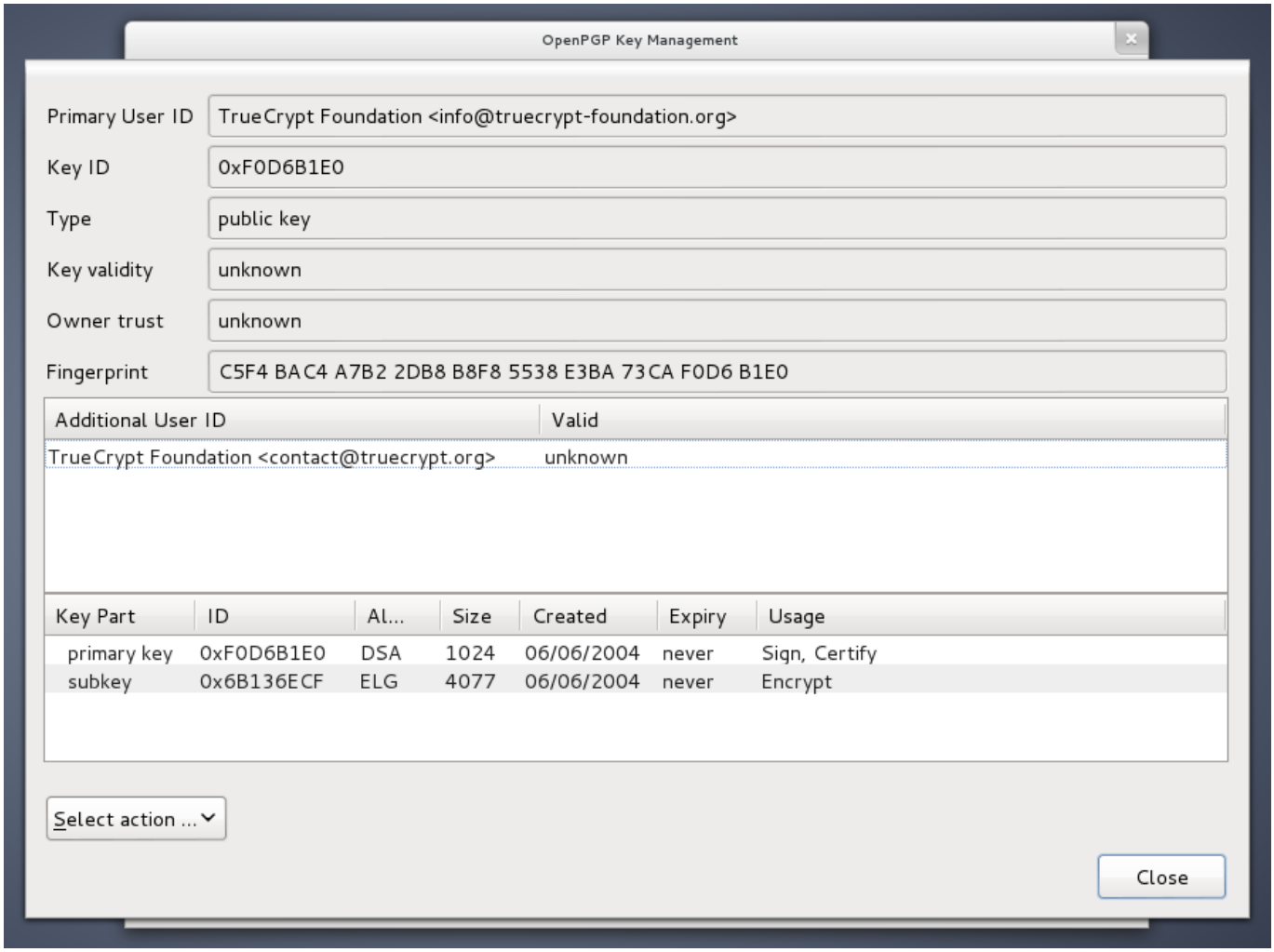
Comme avec l’OTR, il est important de vérifier les clés PGP

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.

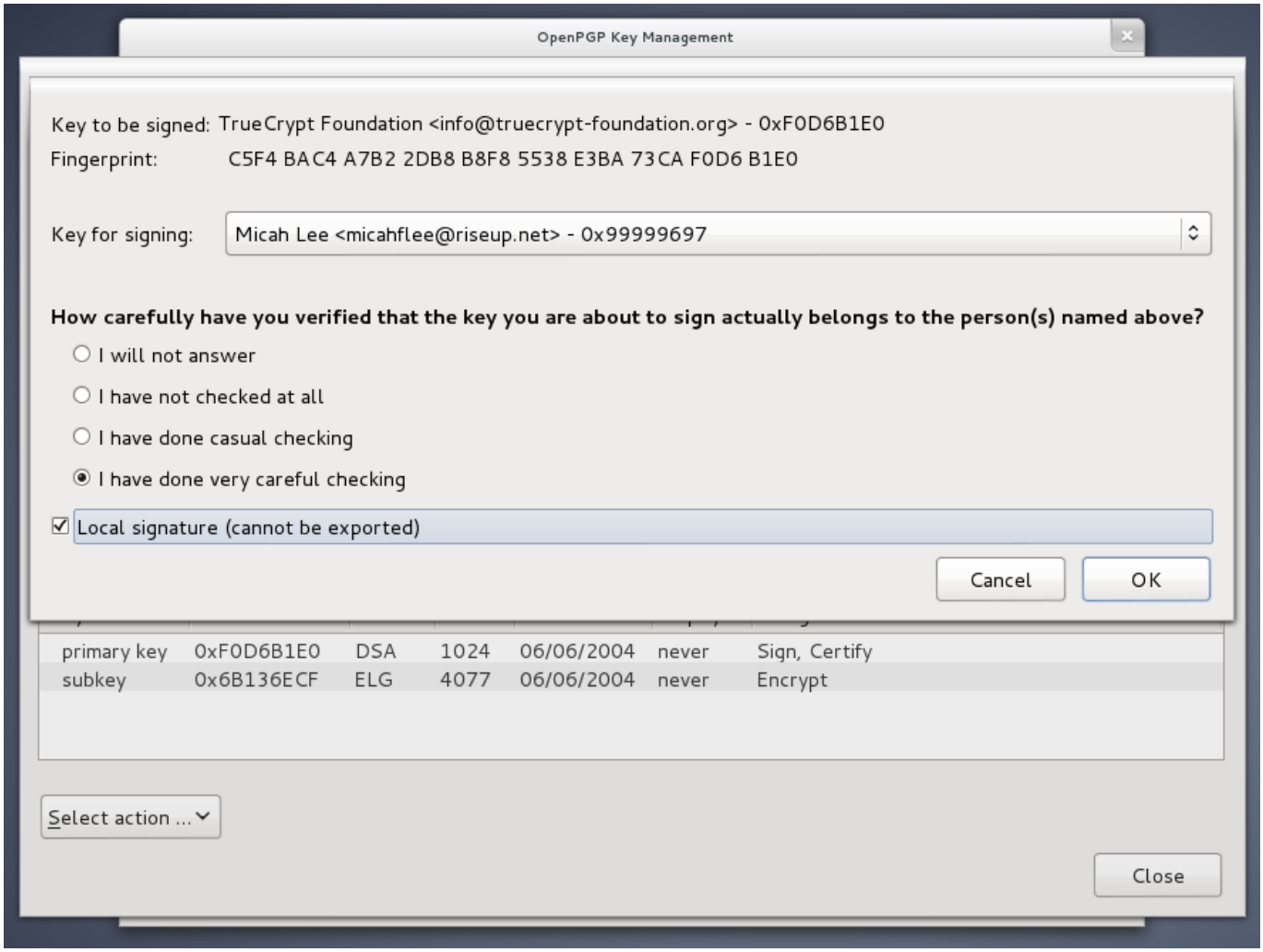
Comme avec les clés OTR, chaque clé PGP a une empreinte unique. Et comme pour OTR, vous avez besoin d'afficher l'intégralité de l'empreinte pour être sûr que la clé publique que vous êtes en train de regarder est bien celle de la personne à qui vous pensez qu'elle appartient.

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.