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.

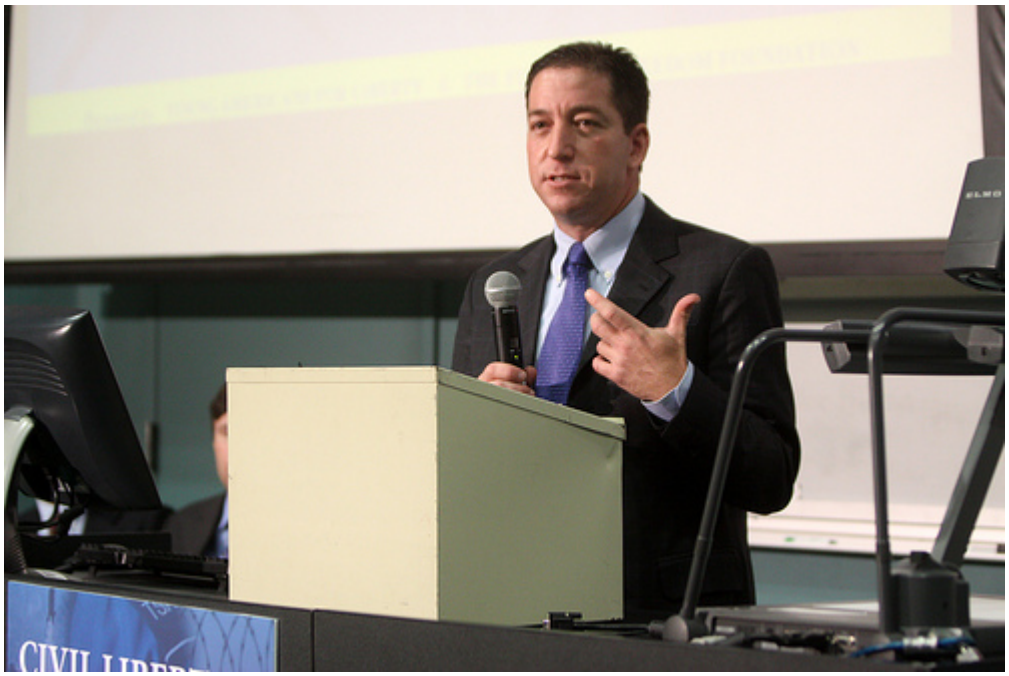
Merci à tous pour cet accueil chaleureux, et merci également aux organisateurs de ce congrès pour m'avoir invité à prendre la parole. Ma réaction, quand j'ai appris qu'on me demandait de faire le discours inaugural de cette conférence, a été la même que celle que vous auriez peut-être eue à ma place, 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 (5)

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

Traduction : Feadurn, Paul, lamessen, goofy

Off-the-Record (OTR) est une couche de chiffrement qui peut être ajoutée à n'importe quel système de messagerie instantanée existant, pourvu que vous puissiez vous connecter à cette messagerie instantanée avec un client qui prend en charge l'OTR, comme Pidgin ou Adium. Avec OTR, il est possible d'avoir des conversations sécurisées, chiffrées de bout en bout, en passant par des services comme Google Talk ou Facebook sans que ni Facebook ni Google n'aient accès au contenu de ces conversations. Notez bien que c'est un système différent de l'option « off the record » de Google, qui n'est pas sécurisée. Et souvenez-vous : bien qu'une connexion HTTPS avec Google ou Facebook offre une très bonne protection à vos messages quand ils circulent, les deux services ont les clés de vos échanges et peuvent donc les communiquer aux autorités.

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

Fournisseurs de services et Jabber

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

Je vous conseille aussi d'utiliser un service XMPP (aussi appelé Jabber). Tout comme le courrier électronique, Jabber

est un protocole ouvert et fédéré. Les utilisateurs d'un service Jabber comme riseup.net peuvent discuter tant avec des utilisateurs du service jabber.ccc.de qu'avec ceux du service jabber.org.

Clients OTR

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

Votre clé

Quand vous commencez à utiliser OTR, votre client de chat génère une clé de chiffrement et la stocke dans un fichier de votre répertoire utilisateur personnel sur votre disque dur. Si votre ordinateur ou votre smartphone est perdu, volé ou rendu inutilisable par un logiciel malveillant, il est possible que l'inviolabilité de votre clé OTR soit compromise. Si c'est le cas, un attaquant aura la possibilité de prendre le contrôle de votre serveur Jabber et de lancer une attaque de l'homme du milieu (MIDTM) contre vous pendant que vous discutez avec des interlocuteurs qui avaient auparavant vérifié votre identité.

Sessions

Si vous souhaitez utiliser OTR pour discuter en privé avec vos amis, ces derniers doivent l'utiliser également. Une session chiffrée entre deux personnes nécessite deux clés de

chiffrement. Par exemple, si vous-même et votre correspondant vous êtes tous deux identifiés sur le chat de Facebook en utilisant Adium ou Pidgin après avoir configuré OTR, vous pourrez discuter en privé. En revanche, si vous vous êtes logué en messagerie instantanée en utilisant Adium ou Pidgin mais que votre interlocuteur discute en utilisant directement facebook.com, vous ne pouvez pas avoir de conversation chiffrée.

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

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

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

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

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

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

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

Cette propriété est appelée sécurité *itérative*, et c'est une particularité d'OTR dont PGP ne dispose pas. Si votre clé PGP privée (article à venir sur les clés PGP) est compromise et que l'attaquant a eu accès à tous les messages chiffrés que vous avez reçus, il peut les retrouver et en déchiffrer l'intégralité.

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

Vérification d'empreinte OTR

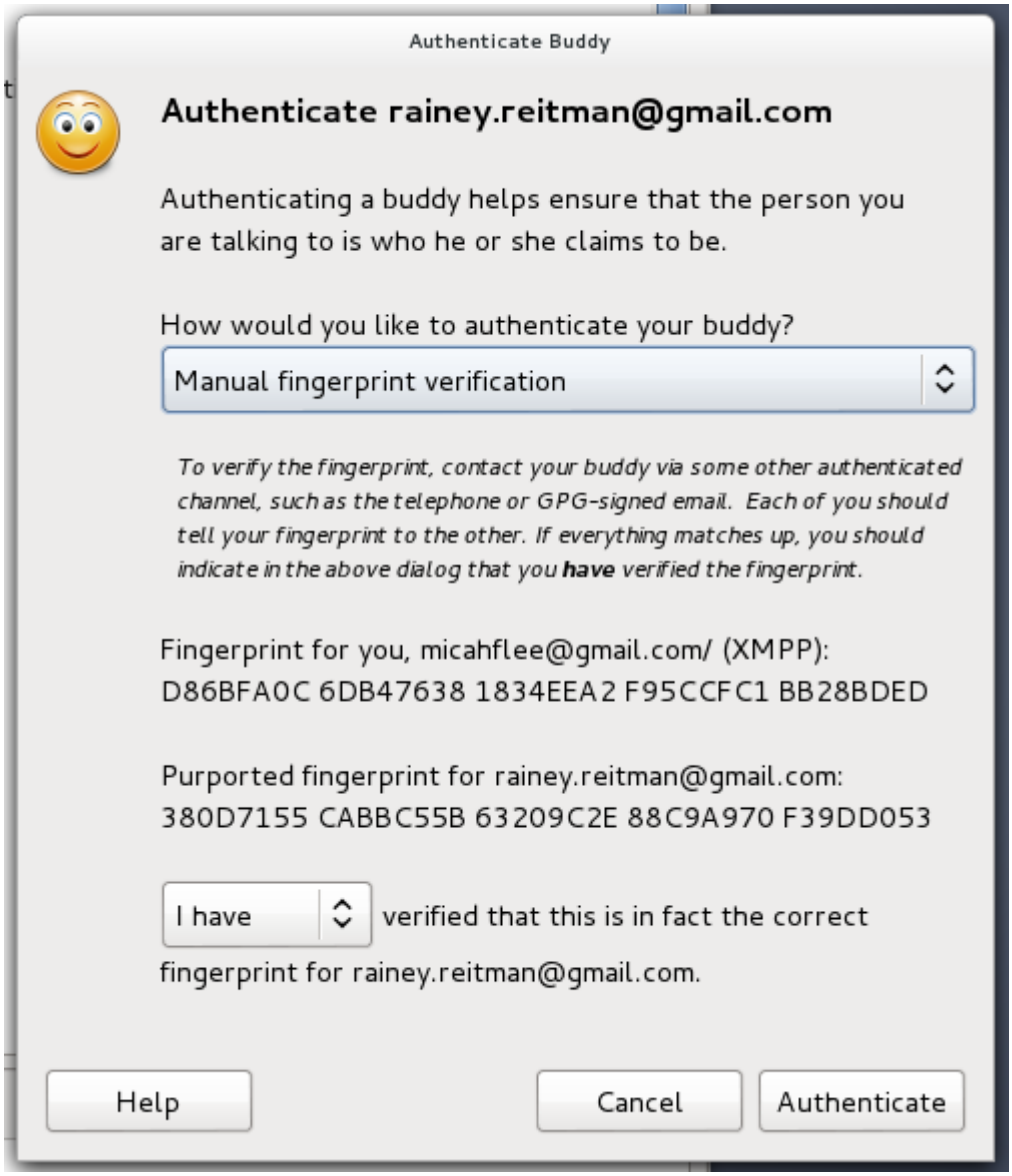
Quand vous commencez une nouvelle session OTR avec quelqu'un, votre logiciel de chat reçoit une empreinte[1] de sa clé de chiffrement et votre logiciel OTR se souvient de cette empreinte. Aussi longtemps que la personne utilise la même clé de chiffrement lorsqu'elle communique avec vous, probablement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

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

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

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

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



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

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

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

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

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

Journaux d'activité

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

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

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

(1:41:12 PM) bradass87: Salut

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

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

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

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

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

(2:17:29 PM) bradass87: ?

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

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

Même s'il peut parfois être utile de garder des journaux de conversations, cela peut aussi gravement mettre en danger votre vie privée. Si Pidgin et Adium ne journalisaient pas les conversations par défaut, il est probable que ces journaux de conversations n'auraient pas fini sur la place publique.

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

(à suivre…)

Notes

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

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