INTRODUCTION À UNE MEILLEURE SÉCURITÉ INFORMATIQUE

AOÛT 2012

Table des matières

I. INTRODUCTION

Pourquoi adopter une attitude sécuritaire

De nos jours les ordinateurs sont de plus en plus omniprésents. Ils contiennent toutes sortes d'informations confidentielles, des numéros de carte de crédit aux listes de contacts. Il convient donc de tenter de sécuriser ces informations de la façon la plus efficace possible contre de possibles attaques.

Cette question prend également un sens plus lourd quand elle est abordée dans une organisation militante. Certaines personnes l'ont découvert avec la grève : l'État n'est pas de notre côté et utilise une panoplie de moyens légaux et extra-légaux pour mieux tenter de nous contrôler. La surveillance informatique fait malheureusement parti de ces moyens.

Pourquoi "attitude sécuritaire" et non sécurité informatique?

Vous vous êtes peut-être posé cette question : pourquoi parle-t-on ici d'attitude sécuritaire et non de sécurité informatique? La réponse est bien simple. La sécurité informatique n'existe tout simplement pas. Tout appareil informatique qui contient des informations sensibles sera toujours sujet à une quelconque faiblesse qui pourra - avec assez de moyens - être exploitée par des forces malveillantes.

Le but est donc d'adopter une attitude sécuritaire adaptée à ses besoins pour mettre des bâtons dans les roues des personnes qui nous voudraient du mal.

Nous mettrons donc beaucoup d'emphase sur les notions d'ensembles de mesures (comparé à des mesures isolées) et de réponses adaptées aux menaces.

II. HORS CONNEXION

a) Comprendre

Pour adopter une attitude sécuritaire, il est important de *comprendre* comment fonctionne les techniques que l'on applique. Malheureusement, certaines personnes veulent tout, tout de suite, recherchent LA solution à leurs problèmes de sécurité. Cela implique cependant trop souvent de faire confiance à de distants "experts" que l'on croit sur parole.

Tenez-le vous pour dit, tenter de sécuriser son ordinateur prends du temps et ne se résume pas à télécharger un programme.

1 - Quelques bases

Qu'est-ce que l'information?

Toute information sur un ordinateur circule sous forme d'impulsions électriques. Elle est représentée par le code binaire, composé de 0 et de 1, qui signifient respectivement l’absence de courant et la présence de courant.

Ainsi, la lettre a en code binaire se traduit par : 01100001

Comment est-elle stockée?

Toute cette information est stockée sous deux grandes formes : dans la mémoire vive (RAM - pour Random Access Memory) et dans des disques durs.

La mémoire vive sert à stocker tous les logiciels et les documents ouverts. C’est à cet endroit que l'ordinateur va chercher les données à traiter et entreposer le résultat des opérations.

L’accès à la mémoire vive est très rapide : il suffit du temps nécessaire pour basculer les interrupteurs qui vont relier le processeur à la case de la mémoire à lire (ou à écrire).

Lorsque la mémoire vive n’est plus alimentée en électricité, les données qu’elle contient deviennent illisibles après quelques minutes ou quelques heures, selon les modèles.

Étant donné que la mémoire vive s’efface à partir du moment où elle n’a plus de courant, l’ordinateur a besoin d’un autre endroit où stocker données et programmes entre chaque allumage. Pour ce faire, on utilise en général un *disque dur*.

Ce mécanisme est *beaucoup plus lent* - 50 fois environ - que l'accès à la mémoire vive. Par contre, c'est plus simple d'y mettre *beaucoup plus d'informations*.

Les informations que l'on met donc généralement sur un disque dur sont, bien entendu, des documents, mais aussi les programmes et toutes les données qu'ils utilisent pour fonctionner, comme des fichiers temporaires, des journaux de bord, des fichiers de sauvegarde, des fichiers de configuration, *etc*.

Le disque dur conserve donc une mémoire quasi-permanente et quasi-exhaustive pour toutes sortes de traces qui parlent de nous, de ce que nous faisons, avec qui et comment, dès qu'on utilise un ordinateur.

2 - Les traces

Mémoire vive

On vient de voir que le premier lieu de stockage des informations sur l'ordinateur est la mémoire vive.

Tant que l'ordinateur est sous tension électrique, elle contient toutes les informations dont le système a besoin. Elle conserve donc nécessairement de nombreuses traces : frappes au clavier (y compris les mots de passe), fichiers ouverts, événements divers qui ont rythmé la phase d'éveil de l'ordinateur.

En prenant le contrôle d'un ordinateur qui est allumé, il n'est pas très difficile de lui faire cracher l'ensemble des informations contenues dans la mémoire vive, par exemple vers une clé USB ou vers un autre ordinateur à travers le réseau. Et prendre le contrôle d'un ordinateur peut être aussi simple qu'y brancher un *iPod* quand on a le dos tourné. Une fois récupérées, les nombreuses informations que contient la mémoire vive sur l'ordinateur et les personnes qui l'utilisent pourront alors être exploitées…

Par ailleurs, si ces données deviennent illisibles lors de la mise hors tension, cela prend néanmoins du temps, ce qui peut suffire pour qu'une personne mal intentionnée ait le temps de récupérer ce qui s'y trouve.

La *veille* (en anglais *suspend to ram*) consiste à éteindre le maximum de composants de l'ordinateur tout en gardant sous tension de quoi pouvoir le rallumer rapidement.

Au minimum, la mémoire vive continuera d'être alimentée pour conserver l'intégralité des données sur lesquelles on travaillait - c'est-à-dire notamment les mots de passe et les clés de chiffrement.

Bref, un ordinateur en veille protège aussi peu l'accès aux données qu'un ordinateur allumé.

Mémoire virtuelle (swap)

Normalement, toutes les données auxquelles le processeur doit accéder, et donc tous les programmes et les documents ouverts, devraient se trouver en mémoire vive. Mais pour pouvoir ouvrir plein de programmes et de documents, les systèmes d'exploitation modernes trichent : ils échangent, quand c'est nécessaire, des morceaux de mémoire vive avec un espace du disque dur dédié à cet effet. On parle alors de « mémoire virtuelle », de *swap* en anglais ou encore d'« espace d'échange ».

La conséquence la plus gênante de ce système pourtant bien pratique, c'est que l'ordinateur va écrire sur le disque dur des informations qui se trouvent dans la mémoire vive… informations potentiellement sensibles, donc, *et qui resteront lisibles après avoir éteint l'ordinateur*.

L'*hibernation* ou *mise en veille prolongée*, appelée aussi en anglais *suspend to disk*, consiste à sauvegarder l'intégralité de la mémoire vive sur le disque dur pour ensuite éteindre complètement l'ordinateur. Lors de son prochain démarrage, le système d'exploitation détectera l'hibernation,

recopiera la sauvegarde vers la mémoire vive et recommencera à travailler à partir de là. Vu que c'est le contenu de la mémoire vive qui est écrite sur le disque dur, ça veut dire que tous les programmes et documents ouverts, mots de passe, clés de chiffrement et autres, pourront être retrouvés par quiconque accédera au disque dur.

Journaux

Les systèmes d'exploitation ont une forte tendance à écrire dans leur journal de bord un historique détaillé de ce qu'ils fabriquent.

Ces journaux (aussi appelés *logs*) sont utiles au système d'exploitation pour fonctionner, et permettent de corriger des problèmes de configuration ou des *bugs*.

Cependant leur existence peut parfois être problématique. Les cas de figure existants sont nombreux, mais les quelques exemples suivants devraient être suffisants pour donner une idée de ce risque :

- sous GNU/Linux, le système garde la date, l'heure et le nom de l'utilisateur qui se connecte chaque fois qu'un ordinateur est allumé ;
- toujours sous GNU/Linux, la marque et le modèle de chaque support amovible (disque externe, clé USB…) branché sont habituellement conservés ;
- sous Mac OS X, la date d'une impression et le nombre de pages sont inscrits dans les journaux ;
- sous Windows, le *moniteur d'évènements* enregistre le nom du logiciel, la date et l'heure de l'installation ou de la désinstallation d'une application.

Méta-données

Autour des informations contenues dans un fichier, il existe des informations sur sont contenu. Ces « données sur les données » s'appellent communément des « méta-données ». Elles pourront donc être connues de quiconque aura accès au fichier.

Les méta-données enregistrées dépendent des formats et des logiciels utilisés. La plupart des fichiers audio permettent d'y enregistrer le titre du morceau et l'interprète. Les traitements de texte ou les PDFs enregistreront un nom d'auteur, la date et l'heure de création, et parfois même l'historique des dernières modifications…

La palme revient probablement aux formats d'images comme TIFF ou JPEG : ces fichiers de photo créés par un appareil numérique ou un téléphone portable contiennent un standard de méta-données appelé EXIF. Ce dernier peut contenir la date, l'heure et parfois les coordonnées géographiques de la prise de vue. Ainsi que la marque, le modèle et le numéro de série de l'appareil utilisé, sans oublier une version miniature de l'image. Et toutes ces informations ont tendance à rester après être passées par un logiciel de retouche photo.

Le cas de la miniature est particulièrement intéressant : de nombreuses photos disponibles sur Internet contiennent encore l'intégralité d'une photo recadrée… et des visages ayant été « floutés ».

Impression

On croyait avoir fait le tour des surprises que nous réservent nos ordinateurs… mais même les imprimantes se mettent à avoir leurs petits secrets.

Première chose à savoir : de nombreuses imprimantes haut de gamme signent leur travail. Cette signature stéganographique repose sur de très légers détails d'impression, souvent invisibles à l'œil nu,

et insérés dans chaque document. Ils permettent d'identifier de manière certaine la marque, le modèle et dans certains cas le numéro de série de la machine qui a servi à imprimer un document. On dit bien « de manière certaine », car c'est pour cela que ces détails sont là : afin de pouvoir retrouver la machine à partir de ses travaux.

Elles peuvent également poser des problèmes à un autre niveau, vu qu'elles sont dotées d'une mémoire vive : celle-ci, tout comme celle du PC, gardera la trace des documents qui ont été traités aussi longtemps que la machine est sous tension… ou jusqu'à ce qu'un autre document les recouvre.

La plupart des imprimantes lasers disposent d'une mémoire vive pouvant contenir une dizaine de pages. Les modèles plus récents ou ceux comportant des scanners intégrés peuvent, quant à eux, contenir plusieurs milliers de pages de texte…

Pire encore : certains modèles, souvent utilisés pour les gros tirages comme dans les associations étudiantes, disposent de disques durs internes, auxquels l'utilisateur n'a pas accès, et qui gardent eux aussi des traces - et cette fois, même après la mise hors tension.

3 - Logiciels malveillants

Les logiciels malveillants sont des logiciels qui ont été développés dans le but de nuire : collecte d'informations, hébergement d'informations illégales, *etc*.

Afin de s'installer sur un ordinateur, certains logiciels malveillants exploitent les vulnérabilités du système d'exploitation ou des applications. Ils s'appuient sur des erreurs de conception ou de programmation pour détourner le déroulement des programmes à leur avantage.

4 - Quelques illusions de sécurité

Propriétaire Vs Open Source

Un logiciel peut faire plein de choses qu'on n'as pas du tout envie qu'il fasse. Dès lors, il est indispensable de faire ce que l'on peut pour réduire ce problème autant que possible. De ce point de vue, les logiciels libres sont dignes d'une confiance bien plus grande que les logiciels dits « propriétaires » .

Pour comprendre la différence entre ces deux types de logiciels, on utilise souvent la métaphore du gâteau. Pour faire un gâteau, il faut une recette.. De la même façon, la recette d'un logiciel est appelée « code source ».

Cette recette est ensuite transformée en un code compréhensible par l'ordinateur, un peu comme la cuisson d'un gâteau nous donne ensuite la possibilité de le manger. Les logiciels propriétaires ne sont disponibles que « prêts à consommer », comme un gâteau industriel, sans la recette. Il est donc très difficile de s'assurer de ses ingrédients.

Les logiciels libres, au contraire, livrent la recette pour quiconque veut comprendre ou modifier le fonctionnement du programme. Il est donc plus facile de savoir ce qu'on donne à manger à notre ordinateur, et donc ce qui va arriver à nos données.

Mots de passe

Tous les systèmes d'exploitation récents offrent la possibilité d'avoir différents utilisateurs sur un même ordinateur. Il faut bien savoir que les mots de passe qui protègent parfois ces utilisateurs ne garantissent pas du tout la confidentialité des données.

Certes il peut être pratique d'avoir son espace à soi, avec ses propres réglages (marque-pages, fond d'écran…), mais une personne qui souhaiterait avoir accès à toutes les données qu'il y a sur l'ordinateur n'aurait aucun mal à y parvenir : il suffit de rebrancher le disque dur sur un autre ordinateur.

Aussi, si utiliser des comptes séparés et des mots de passe peut avoir quelques avantages (comme la possibilité de verrouiller l'écran quand on s'éloigne quelques minutes), il est nécessaire de garder en tête que cela ne protège pas réellement les données.

Supprimer des fichiers

La suppression d'un fichier n'en supprime pas le contenu et ça peut être très facile de le retrouver.

En effet, lorsqu'on « supprime » un fichier - en le plaçant par exemple dans la *Corbeille* puis en la vidant - on ne fait que dire au système d'exploitation que le contenu de ce fichier ne nous intéresse plus. Il supprime alors son entrée dans l'index des fichiers existants. Il a ensuite le loisir de réutiliser l'espace que prenaient ces données pour y inscrire autre chose.

Mais il faudra peut-être des semaines, des mois ou des années avant que cet espace soit *effectivement* utilisé pour de nouveaux fichiers, et que les anciennes données disparaissent réellement. En attendant, si on regarde directement ce qui est inscrit sur le disque dur, on retrouve le contenu des fichiers.

b) Choisir des réponses adaptées

1 - Évaluer les risques

Protéger quoi?

Le mot « protéger » recouvre différents besoins :

- **confidentialité** : cacher des informations aux yeux indésirables ;
- **intégrité** : conserver des informations en bon état, et éviter qu'elles ne soient modifiées sans qu'on s'en rende compte ;
- **accessibilité** : faire en sorte que des informations restent accessibles aux personnes qui en ont besoin.

Il s'agit donc de définir, pour chaque ensemble d'informations à protéger, les besoins de confidentialité, d'intégrité et d'accessibilité. Sachant que ces besoins entrent généralement en conflit, on réalise dès maintenant qu'il faudra, par la suite, poser des priorités et trouver des compromis entre eux : en matière de sécurité informatique, on a rarement le beurre et l'argent du beurre.

Contre qui?

Rapidement se pose la question des capacités des personnes qui en auraient après ce que l'on veut protéger. Et là, ça se corse, parce qu'il n'est par exemple pas facile de savoir ce que les personnes les plus qualifiées peuvent réellement faire, et de quels moyens et de quels budgets elles bénéficient. En

suivant l'actualité, et par divers autres biais, on peut se rendre compte que cela varie beaucoup selon à qui on a affaire. Entre le flic du coin et la *National Security Agency* américaine, il y a tout un fossé sur les possibilités d'actions, de moyens et de techniques employées.

Un facteur important est aussi à prendre en compte : le coût. En effet, plus les moyens mis en place sont importants, plus les technologies utilisées sont complexes, et plus leur coût est élevé ; ça signifie qu'ils ne seront utilisés que dans des cas précis et tout aussi importants aux yeux des personnes concernées. Par exemple, il y a peu de chances de voir un ordinateur soumis à d'intenses tests dans de coûteuses expertises pour une affaire de vol à l'étalage.

Dès lors, avant même de chercher une solution, la question est de savoir qui pourrait tenter d'accéder à nos informations sensibles, afin de discerner s'il est nécessaire de chercher des solutions compliquées ou pas. Sécuriser complètement un ordinateur est de toutes façons de l'ordre de l'impossible, et dans cette histoire, il s'agit plutôt de mettre des bâtons dans les roues de celles et ceux qui pourraient en avoir après ce que l'on veut protéger. Plus l'on pense grands les moyens de ces personnes, plus les bâtons doivent être nombreux et solides.

Évaluer les risques, c'est donc avant tout se poser la question de quelles sont les données que l'on veut protéger, et de qui peut être intéressé par ces données. À partir de là, on peut avoir une vision de quels moyens ils disposent (ou en tout cas, dans la mesure du possible, essayer de se renseigner) et en conséquence, définir une *politique de sécurité* adaptée.

2 - Définir une politique de sécurité

Compromis

On peut toujours *mieux* protéger ses données et ses communications numériques. Il n'y a de limite ni aux possibilités d'attaque et de surveillance, ni aux dispositifs qu'on peut utiliser pour s'en protéger.

Cependant, à chaque protection supplémentaire qu'on veut mettre en place correspond un effort en termes d'apprentissage, de temps ; non seulement un effort initial pour s'y mettre, pour installer la protection, mais aussi, bien souvent, une complexité d'utilisation supplémentaire, du temps passé à taper des phrases de passe, à effectuer des procédures pénibles et répétitives, à porter son attention sur la technique plutôt que sur l'usage qu'on voudrait avoir de l'ordinateur.

Dans chaque situation, il s'agit donc de trouver un compromis convenable entre la facilité d'utilisation et le niveau de protection souhaité.

Comment faire?

Il s'agit de répondre à la question suivante : quel ensemble de pratiques, d'outils me protégeraient de façon suffisante? Vous pouvez par exemple partir de vos pratiques actuelles, et vous mettre dans la peau de l'adversaire pour vous poser les questions suivantes :

1. Face à une telle politique de sécurité, quels sont les angles d'attaque les plus praticables ?
2. Quels sont les moyens à mettre en œuvre pour ce faire ?
3. Croyez-vous que ces moyens puissent être utilisés par les adversaires ?

En cas d'incertitude, il est toujours possible de demander à une personne digne de confiance et plus compétente en la matière de se mettre dans la peau de l'adversaire : elle sera ravie de constater que

vous avez fait vous-mêmes le gros du travail de réflexion, ce qui l'encouragera certainement à vous aider sur les points qui restent hors de votre portée.

Quelques règles

En matière de sécurité, une solution simple doit toujours être préférée à une solution complexe.

Ensuite, parce que plus une solution est complexe, plus il faut de connaissances pour l'imaginer, la mettre en œuvre, la maintenir… mais aussi pour l'examiner, évaluer sa pertinence et ses problèmes. Ce qui fait qu'en règle générale, plus une solution est complexe, moins elle aura subi les regards acérés nécessaires pour établir sa validité.

Par exemple, plutôt que de passer des heures à mettre en place des dispositifs visant à protéger un ordinateur particulièrement sensible contre les intrusions provenant du réseau, autant l'en débrancher. On peut même parfois retirer physiquement la carte réseau…

Une chose à retenir : on n'est pas des robots. Il vaut mieux se donner de solides garde-fous matériels, que de s'imposer une vigilance sans bornes.

Une fois une politique de sécurité définie, il ne faut pas oublier de la revoir de temps en temps! Le monde de la sécurité informatique évolue très vite, et une solution considérée comme raisonnablement sûre à l'heure actuelle peut très bien être aisément attaquable l'an prochain.

c) Un exemple pratique : TAILS

1 - Théorie

Les systèmes *live*

Un système dit *live* est un système d'exploitation qui fonctionne *par-dessus* celui déjà installé *via* un médium extérieur. On peut par exemple faire rouler Ubuntu sur n'importe quel ordinateur grâce à un CD, et ce sans l'installer.

TAILS, un système sécurisé

TAILS - The Amnesic Incognito Live System - est un système *live* basé sur Debian GNU/Linux créé spécialement pour laisser le moins de traces possibles. Par défaut il est configurer pour n'utiliser que la mémoire vive, qui ne garde les informations que quelques heures. Il vient avec certains programmes déjà installés et il n'est pas possible d'en installer d'autre.

2 - Tutoriel

Installation

1. Télécharger le fichier .iso au https://tails.boum.org/
2. Consulter la consultation: https://tails.boum.org/doc/index.fr.html
3. Graver le fichier .iso sur un DVD (graver comme une image de disque). La documentation explique également comment le graver sur une clef USB.

Utilisation

Pour utiliser TAILS, il ne suffit plus que d'insérer le DVD dans l'ordinateur et le redémarrer. Si TAILS ne démarre pas automatiquement, il vous faudra modifier l'ordre d'amorçage de votre BIOS.

Voici un tutoriel montrant comment : http://doc.ubuntu-fr.org/tutoriel/modifier_ordre_amorcage_du_bios

Une chose est importante à retenir : il ne sert à rien d'utiliser TAILS pour créer un tract sensible pour ensuite l'enregistrer sur une clef USB ou alors l'envoyer par son compte e-mail régulier.

Le moyen le plus simple d'utiliser TAILS pour travailler sur des documents sensibles est d'enregistrer ses documents grâce à système *cloud* anonymisé[1].

LA MAJEURE PARTIE DE LA SECTION HORS CONNEXION EST TIRÉE DU *GUIDE D'AUTODÉFENSE NUMÉRIQUE*, DISPONIBLE AU http://guide.boum.org/
SA LECTURE EST FORTEMENT CONSEILLÉE AUX PERSONNES DÉSIRANT APPROFONDIR CES NOTIONS.

III. EN LIGNE

a) Comprendre

Comme expliqué plus tôt, il est important de comprendre comment fonctionne les techniques que l'on applique. Cette partie vise à vulgariser le *comment* du réseautage internet.

1 - Une connexion internet

Quand vous connectez à internet et que vous accédez à un site web, vous n'êtes pas directement en relation avec celui-ci. En fait, vous passez par une série d'étapes assez complexes, mais qui sont heureusement résumé à 6 grands points.

Internet Protocol

Commençons donc au tout début, au niveau de l'ordinateur. Tout ordinateur connecté à internet se voit attribuer une adresse IP, une série de chiffres, qui sert à l'identifier et à savoir où envoyer les données qu'il demande. Elle est donc indispensable pour réaliser une connexion internet.

Grâce à l'adresse IP on peux également identifier le pays, le fournisseur d'accès internet et parfois même la ville où l'ordinateur se trouve. Elle peut donc être utilisée à mauvais escient, soit pour vous localiser physiquement après vous avoir observé de façon numériques, ou alors pour vous localiser numériquement lorsque l'on veut suivre vos connexions.

Routeur

Le routeur est la machine qui reçoit les données de votre ordinateur, par un câble Ethernet ou par wi-fi, et les redirige vers votre fournisseur d'accès internet. Il dispose d'une "banque" d'adresses IP disponibles qu'il répartit en fonction des personnes connectées en même temps.

1 Voir la partie dédiée à ce sujet dans la section En Ligne

Si vous communiquer par Wi-Fi avec votre routeur, il est très facile pour quiconque qui se connecte à ce réseau de voir vos activités sur internet et d'en prendre le contrôle. Il est donc particulièrement important de sécuriser son réseau sans-fil du mieux possible en utilisant le processus d'encryptage WPA2.

Internet Service Provider

Le fournisseur d'accès internet (ISP) est la compagnie qui vous vend une connexion à internet. En fait, elle achète une connexion à très haute capacité qu'elle divise et revend aux particuliers. Quand vous vous connectez sur un site web, vous demandez donc à votre ISP de se connecter pour vous et de vous renvoyer les données.

Si votre connexion n'est pas encryptée votre ISP peut voir tout ce que vous faîtes sur internet. Il peut aussi servir d'outil de censure, comme dans certains pays du Moyen-Orient ou en Chine où le gouvernement interdit aux ISP de donner accès à certains sites web.

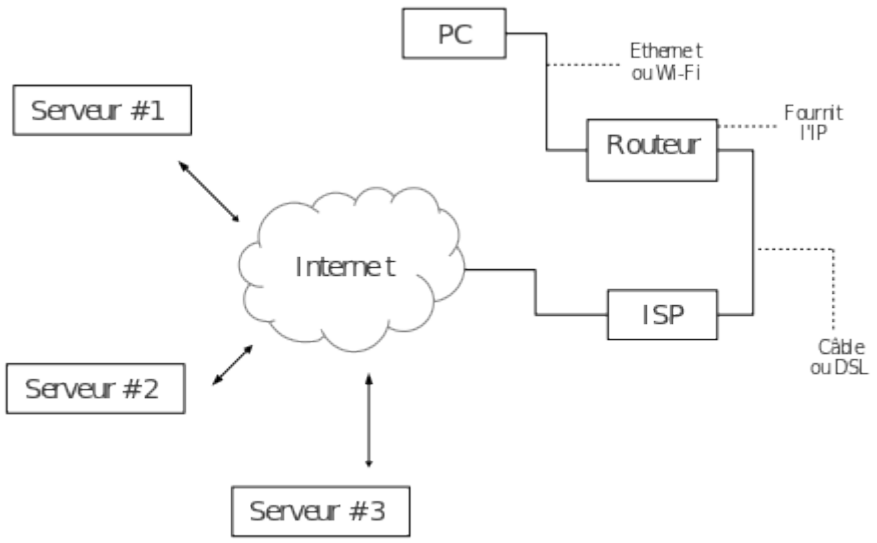
Avec un mandat, la police ou le gouvernement peut demander à avoir la liste des sites web que vous avez visités et plus encore. Certaines informations portent même à croire que, de plus en plus, les ISP donnent ces informations à la police sans mandat, car elles considèrent qu'elles sont les leurs et non les vôtres...

Internet

Dû à la très grande complexité de la structure interne d'internet, nous ne la décrirons pas ici. Il est néanmoins bien de savoir que globalement, elle est faite de serveurs qui se connectent à des serveurs qui se connectent à des serveurs qui...

Serveur

Finalement, après avoir passé à travers toute la chaîne, on arrive au serveur où est hébergé le site web que l'on souhaitait consulter. Pour que l'information se rende à votre ordinateur, elle devra refaire tout le chemin inverse.



2 - Les médias sociaux

La grande popularité des réseau sociaux est en parti attribuable au fait qu'il y est facile d'y partager une tonne d'informations personnelles avec une multitude de personnes. C'est également ce qui fait qu'ils ne sont pas sécuritaire.

Facebook

Mis à part le fait que toute l'information que vous mettez sur votre compte appartient à Facebook et qu'ils peuvent faire ce qu'ils veulent avec cette dernière, Facebook sert de plus en plus d'outil de surveillance par les forces de l'ordre.

Vous êtes-vous déjà demandé pourquoi Facebook était gratuit? Rien n'est jamais réellement gratuit, sauf peut-être les logiciels libre. Pour se faire de l'argent, Facebook regarde ce que vous aimez et construit des profils type qu'il va vendre aux compagnies de publicité. Ces profils serviront à faire de la publicité ciblée, également présente sur Facebook. Ce processus se nomme le *data-mining*, textuelle miner de l'information.

Après avoir utilisé Facebook pendant un an, un homme en Allemagne à demandé à la compagnie de lui envoyer l'ensemble des données qu'ils avaient récolté sur lui. Il a reçu 3 DVD complet de document texte, incluant des statistiques et des analyses retraçant sa semaine type.

Le plus dangereux avec ce média social, c'est la fausse impression de sécurité qu'il fournit. Parce que seul nos amis ont accès à notre compte, on à l'impression que les personnes qui nous veulent du mal doivent fonctionner selon les même règles. Seules quelques notions de base suffisent pour pirater un compte Facebook à l'insu de son propriétaire.

Pour les personnes qui souhaiteraient tout de même continuer à utiliser Facebook, nous ne pouvons que vous conseiller de mettre le moins d'informations personnelles possibles et de bien séparer vie militante et vie personnelle.

Twitter

De par son utilisation, Twitter est peut-être bien le média social le plus sécuritaire. En effet, il sert plus souvent pour relater des événements – dans des manifs par exemple – et exprimer des opinions qu'à expliquer de long en large qui sont nos amis.

Il est néanmoins important de rester vigilant-e : toute information mise sur Twitter est encore plus facilement accessible que sur Facebook. Il y a donc là un potentiel de risque énorme. Le mot d'ordre, comme partout, est de de choisir précautionneusement se que l'on y met.

Foursquare !!!!

Si jamais il vous est venu la bonne idée de vous abonner à un site qui indique votre position en tout temps à vos amis comme Foursquare, et bien détruisez votre compte. Avec ce genre de fonctions, il est possible de retracer ce que vous avez fait, quand et avec qui, depuis l'activation de votre compte. Et bien entendu, ces sites ne se gênent pas à revendre ces informations.

Si vous ne voyez aucun problème à cela, nous vous conseillons *1984*, un excellent livre de George Orwells.

3 - Les comptes e-mails

Mise à part certains groupes qui fournissent des comptes e-mails sécurisés (comme Koumbit ou alors Riseup), il faut savoir qu'il est aussi peu sécuritaire d'envoyer de l'information par e-mail que d'envoyer une copie conforme à votre poste de police préféré.

En effet, la facilité avec laquelle les compagnies de e-mails donnent de l'information aux forces de l'ordre est assez stupéfiante. Il suffit à la police – même sans mandat – de demander à un fournisseur de compte e-mail l'ensemble des e-mails d'un compte pour que ces dernières obtempèrent.

De plus elles sont parmi celles qui profitent le plus du *data-mining*. Ainsi, Google et autres - exactement comme Facebook - analysent l'ensemble de vos courriels, créent des profils et font de publicité ciblée.

b) Choisir des réponses adaptées

Il convient d'appliquer le même type de raisonnement pour définir une politique de sécurité lorsque l'on se connecte sur internet que lorsque que l'on est hors-connexion[2].

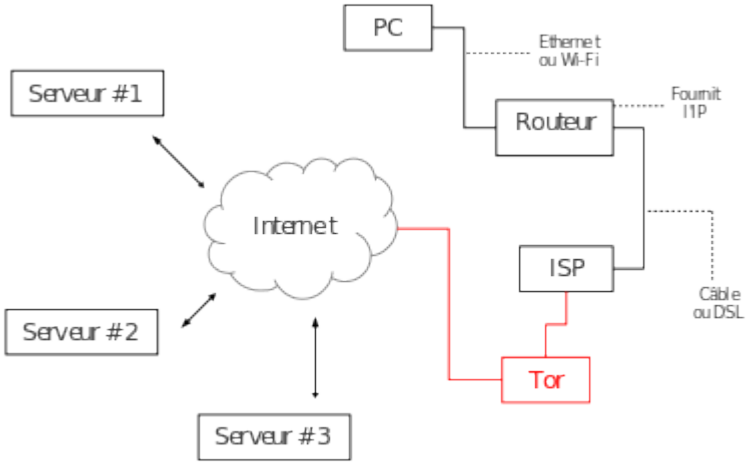
Il ne faut cependant pas oublier de considérer ces pratiques dans son ensemble : une attitude sécuritaire sur internet ne sert à rien si on applique pas le même genre de pratiques à l'ensemble de son ordinateur.

c) Un exemple pratique : anonymiser une connexion

1 - Théorie

Tor

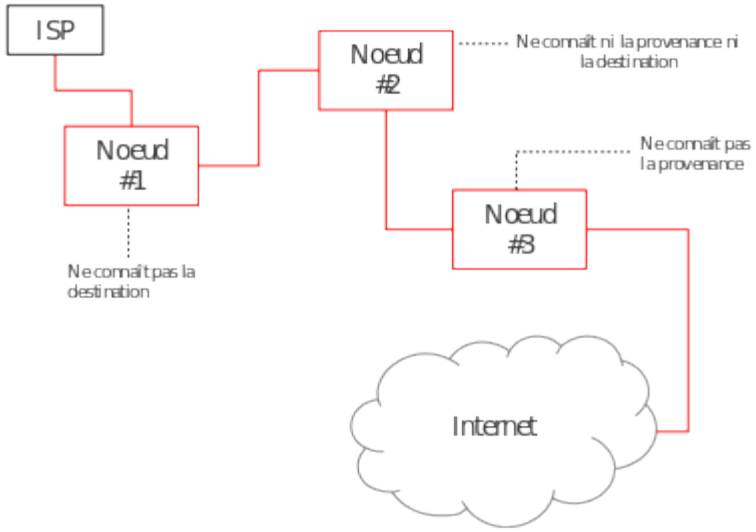
Tor (The Onion Routeur) est un programme libre qui permet d'anonymiser sa connexion internet. Pour ce faire, il vient "s'insérer" entre votre ISP et internet. Vous demandez donc à votre ISP de se connecter à Tor, qui lui se connecte à internet. Résultat : votre ISP ne peux plus savoir à quel site vous vous connectez, il sait seulement que vous vous connectez à Tor.



2 Nous vous référons donc à la partie *Choisir des réponses adaptées* de la section Hors-connexion

Tor fonctionne grâce à une série de nœuds. Ces nœuds sont en fait des serveurs fournis bénévolement par des personnes à travers le monde qui retransmettent la connexion.

Plutôt que de se connecter directement à internet, le PC se connecte tout d'abord au premier nœud. Ce dernier ne connaît pas la destination de la connexion. Il le retransmet au deuxième nœud, qui lui ne sait pas d'où provient la connexion ni où elle va. Finalement, la connexion passe par un troisième nœud, qui lui se connecte à internet. Celui-ci ne sait pas d'où provient la connexion.



On peut ainsi faire en sorte d'anonymiser sa connexion et d'empêcher les nœuds, même s'ils sont malveillants, de savoir qui l'on est.

Tor n'est cependant pas la solution miracle à tous vos problèmes. En effet, il ne fait qu'anonymiser vos connexions : il ne cache pas ce que vous faîtes. De plus, si vous vous connectez sur votre compte e-mail personnel ou sur Facebook via Tor, vous venez de montrer à tout le monde qui vous êtes!

Un *cloud* anonymisé

Le problème avec le fait d'utiliser TAILS pour ne pas laisser de traces sur votre ordinateur est justement le fait que vous ne voulez pas laisser de traces. Il est ainsi assez difficile de sauvegarder un travail.

Il est cependant possible d'utiliser Tor à l'intérieur de TAILS pour stocker ses documents sur internet (dans le *cloud*) d'une manière anonyme. Ainsi, on peut de se créer un compte e-mail sur lequel on va s'envoyer à soi-même les documents que l'on souhaite stocker. Un compte Dropbox réservé à une utilisation anonyme peut également être une solution.

ATTENTION : ces comptes ne doivent être accédés que par Tor à l'intérieur de TAILS!! Si vous utilisez une connexion qui n'est pas anonyme pour vous connecter, votre compte n'est plus anonyme!

2 - Tutoriel

Installation

1. Télécharger le Tor Browser Bundle : https://www.torproject.org/
2. Consulter la consultation: https://www.torproject.org/docs/documentation.html.en

Tor est installé par défaut sur TAILS. Il ne vous suffit que d'ouvrir un navigateur web et vous serez automatiquement connecté grâce à Tor.

Utilisation

1. Ouvrir le Tor Bundle et cliquer sur le fichier start-tor-browser
2. Vous assurer que la page principale indique bien que vous êtes connecté à Tor

Sur TAILS :

1. Ouvrir IceWeasel, le navigateur web par défaut.
2. Vous assurer que la page principale indique bien que vous êtes connecté à Tor

IV. LES CELLULAIRES

a) L'appareil

Si nous avons inclus la question des téléphones cellulaires à notre atelier sur la sécurité informatique c'est parce qu'ils sont de plus en plus des ordinateurs à part entière. Ainsi, l'ensemble des mises en gardes que nous avons fait précédemment s'appliquent aussi aux cellulaires.

Le plus grand danger avec les cellulaire est le fait qu'ils sont conçus pour qu'ils nous suivent partout, des toilettes aux réunions les plus sensibles.

L'alimentation électrique

Commençons donc par déconstruire un premier mythe : la question de l'alimentation électrique et des batteries.

Ce n'est pas parce que vous fermez votre cellulaire (bouton *off*) que ce dernier est réellement éteint. Mon cellulaire, par exemple, me sert de réveil-matin. Tous les soirs je règle un heure et je l'éteint. Mon cellulaire est donc "fermé". Pourtant, à l'heure programmée, le téléphone s'allume et me réveille. Il n'était donc pas réellement fermé...

En fait, lorsque vous fermez votre cellulaire, celui-ci ne fait que désactiver certaines fonctions, comme l'écran ou le fait de recevoir des appels pour sauver de l'énergie.

Un téléphone programmé correctement pourrait donc continuer à émettre (votre position, ce que vous dîtes, etc) même si vous l'avez "fermé". Cela peut donc poser de graves problèmes de sécurité.

Un moyen de régler le problème est de couper toute alimentation électrique à l'appareil. On peut ainsi encore enlever la batterie sur de vieux modèles.

Un bémol survient quand on arrive aux modèles dit"intelligents". En effet, il est souvent difficile, voir

même impossible comme sur les *iPhones*, de retirer la batterie principale. La deuxième chose à savoir avec ceux-ci est le fait qu'ils ont parfois une pile secondaire. Elle est placée là au cas où la batterie principale ferait défaut pour garder en mémoire des choses comme l'heure, la date ou alors des informations comme le début d'un texto que l'on aurait pas eu le temps d'envoyer. Ces piles sont presque tout le temps impossible à enlever sans démonter intégralement le téléphone. Il y a donc toujours un risque qu'un cellulaire puisse servir d'outil malveillant même si la batterie principale a été enlevée.

Les micro-ondes

La meilleure solution pour se protéger est donc de retirer la batterie principale (quand c'est possible) et mettre son cellulaire dans un four à micro-ondes.

En effet, ces derniers sont conçus pour ne pas laisser passer les rayonnements nocifs émit par leurs utilisation. Ils peuvent donc servir de chambre d'isolement.

Un bon moyen de voir si son four à micro-ondes bloque bel et bien les ondes cellulaires est de placer le téléphone à l'intérieur et tenter de l'appeler grâce à un autre appareil. Si vous tombez sur la boîte vocale sans que le téléphone ait sonné, on peut considérer le micro-onde sécuritaire.

Les réfrigérateurs ne produisent cependant pas le même effet et endommageront vos appareils.

b) Ses fonctions

Maintenant que l'on sait à quel point un cellulaire peut-être dangereux, il est important de s'attarder aux fonctions d'un tel appareil qui peuvent s'avérer utile pour les forces de l'ordre et de l'injustice.

1 - Positionnement

GPS

Il est évident qu'avec un GPS dans votre téléphone, il est possible de vois localiser. Et bien entendu, comme l'extrême grande majorité des cellulaires fonctionnent avec des logiciels propriétaires, vous ne serez jamais vraiment sûr de ce qu'ils font réellement. Même si vous désactivez la fonction GPS de votre téléphone vous ne pouvez pas être sûr que cette dernière ne fonctionne pas et ne retransmet pas votre position.

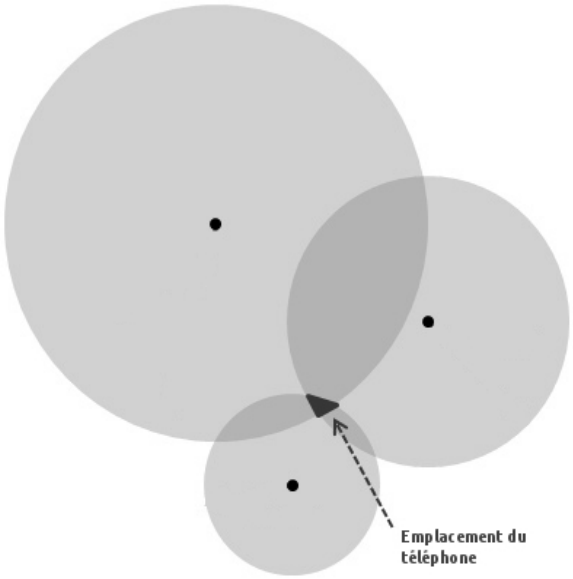
Ondes cellulaires

Vous direz alors : « HAHA, je n'ai pas de GPS dans mon cellulaire, victoire et sécurité! ». Soit, réjouissez-vous de ne pas avoir cette fonction ma fois bien utile, mais cela n'empêche pas quiconque qui dispose d'assez de moyens de vous localiser quand même.

Votre téléphone reçoit et émet des appels et des textos grâce aux ondes cellulaire. Le "3G" ou tout autre forme d'internet à distance fonctionne également de la même manière.

Grâce à ces ondes, il est très facile de vous localiser. En ville ce moyen est même plus efficace que le GPS à cause de l'abondance des tours de relais.

Pour ce faire, on utilise la méthode de la triangulation :



Par des calculs relativement simple, on peut connaître la position d'un cellulaire grâce au délai que le signal met à parcourir la distance entre des antennes et l'appareil. Avec trois antennes, il est possible de connaître les coordonnées géographiques d'un cellulaire.

Il faut de plus savoir que les compagnies de téléphone donnent volontiers ces informations à la police ou au gouvernement lorsqu'ils le demande...

Wi-fi

La troisième façons de connaître votre position est par une connexion Wi-Fi. Comme expliqué plutôt, tout appareil qui se connecte sur internet se voit attribuer une adresse IP. Grâce à cette adresse, il est possible de savoir où vous êtes. De plus, il est beaucoup plus difficile d'anonymiser sa connexion avec un téléphone intelligent qu'avec un ordinateur. Cela est toute fois possible grâce à Orbot, une application Tor sur Android[3].

2 - Écoute électronique

Écoute active et écoute passive

L'écoute active se distingue par le fait qu'on vous écoute en temps réel. Ainsi, vos appels ou vos textos sont mis sous surveillance intensive. Par exemple, la police a eu vent du fait que vous prépariez une action le 8 août à 11h30 et décide de faire de l'écoute active durant deux jours avant la date prévue dans le but de vous empêcher de la mener à bien.

Il est également possible de faire de l'écoute passive, c'est-à-dire enregistrer vos conversations pour les analyser d'un bloc par la suite. Contrairement à l'écoute active, cette méthode demande moins de ressources. Elle a souvent comme but de ramasser des preuves en vue d'un procès ou dans le cadre d'une enquête.

3 https://guardianproject.info/apps/orbot/

Textos vs appels

Est-il plus sécuritaire de communiquer par textos ou de faire un appel? En fait, ni l'un ni l'autre n'est sécuritaire. Les textos ne sont que du texte : il est extrêmement facile de les analyser à l'aide de mots-clefs pour trouver ce que l'on cherche.

Pour ce qui est des appels, les programmes de transcription de la voix sont tellement rendus perfectionnés qu'ils peuvent être mis sous forme de texte et soumis aux mêmes traitements que les textos. De nos jours même *Youtube* offre de transcrire automatique le son d'un vidéo en sous-titre d'une manière très décente. Et si Google le fait, imaginez un peu ce que l'armée ou la NSA peut faire...

La solution miracle

Il n'y a pas de solution miracle. Quand on peut, on évite le plus possible d'utiliser les technologies informatiques et quand cela s’avère impossible, on utilise un code sur lequel on s'est entendu préalablement de vive voix. Ainsi : « Groupe #1 go! » peut devenir « J'ai 1 [G-1] canard ».

En théorie, pour effectuer de l'écoute électronique la police doit disposer d'un mandat émis par un juge. En pratique, ce mandat n'est nécessaire que pour utiliser les informations recueillies comme preuves. Aucun mandat n'est donc requis pour savoir où et quand envoyer l'anti-émeute pour vous empêcher d'agir. De plus, il est possible de faire de l'écoute sans mandats dans le but de récolter de l'information pour savoir dans quelle direction continuer à creuser.