SYNTHÈSE DE L'ATELIER DE RÉFLEXION
« SÉCURITÉ SUR INTERNET (navigation & données) »

atelier du 14 novembre 2016

Sylvain Steer a été chargé pour le CECIL (Centre d'Études sur la Citoyenneté, l'Informatisation et les Libertés) d'élaborer les fiches pour « *protéger ses libertés en milieu numérique 'hostile'* ». Un exemplaire du fascicule regroupant ces douze fiches (édité par le CECIL et la LDH – Ligue des Droits de l'Homme) a été donné aux participant-e-s à cet atelier.
Sylvain est venu ce soir pour partager sur ces sujets. Les thèmes abordés sont amenés par toutes et tous les présent-e-s.

Utilisation de chiffrement, de fait, et de manière 'passive' grâce aux sites certifiés

Les communications entre un ordinateur et un serveur, via les sites sous https:// sont chiffrées.

Les sites sous http:// (avec cadenas ouvert), ne proposent qu'une navigation 'en clair' : tout 'sniffeur' / renifleur pourra pister et voir les informations qui transitent par ce site ET même voir les informations que chaque ordinateur laisse transparaître. Soit à l'émission soit à la réception.

Si on ne saisit pas de données, rien de grave a priori (sauf traçage de circulation) ; par contre si on a des données à saisir : bien veiller à maîtriser ce qu'on donne comme informations …

Les certificats pour les sites sont faits pour donner de la transparence sur les risques de compromissions des communications / relations entre serveurs et ordinateurs, et éviter les détournements de données.
Jusqu'à présent, obtenir un tel certificat fourni par des autorités de certification, était payant, cher et cela empêchait les sites d'y recourir. Désormais il existe http://letsencrypt.fr/ (let us encrypt) qui permet cet 'encryptage' gratuitement.
Certains sites s'auto-signent avec des preuves internes de non compromission. Ceux-là peuvent être sous https ou pas.

Transport Layer Security (TLS), et son prédécesseur *Secure Sockets Layer* (SSL), sont des protocoles de sécurisation des échanges sur Internet. Ce sont des protocoles libres.
Https Everywhere est une extension pour les navigateurs (Mozilla Firefox mais les autres aussi !) qui permet d'étendre l'usage du SSL/TLS sur certains sites. Elle active le SSL sur les pages où ce protocole est normalement désactivé. L'extension est maintenue par le projet TOR depuis 2010.

ANTANAK

Utilisation active de chiffrement

- Régir le transfert d'une archive ou d'un document avec mot de passe : mode de chiffrement symétrique (c.à.d que la clef de fermeture et d'ouverture d'accès est identique : c'est un code qu'on se transmet entre partageurs).

- Différencier les sites sur lesquels il n'y a pas d'incidence à oublier le mot de passe et à en redemander un nouveau (genre 1 site sur lequel on va 2 fois par an), de ceux sur lesquels l'accès doit être bien protégé (courriel, banque, administration, ...).

- Mettre des mots de passe forts sur ses connexions importantes : plutôt 12 caractères ; pas partout le même mot de passe ; pas avec des signes facilement détectables ou interprétables grâce au login/identifiant qui y est accolé ; pas en faisant 'tourner' les mêmes mots de passe sur les sites utilisés souvent (banque, courriel, …) ; mélanger du numérique, de l'alphanumérique et des caractères spéciaux ; préférer même des phrases ; …

- Utiliser un outil de gestion des mots de passe (car on ne peut pas se souvenir de tous, surtout s'ils sont longs. Par exemple keypass (il y en a d'autres) est un outil de gestion des mots de passe, organisés par dossiers / thèmes, lui-même protégé par un mot de passe global, installé sur son disque dur. L'inconvénient est de devoir se promener avec une clef possédant cet outil et ses codes pour agir à distance de son ordinateur … ce qui n'est pas plus compliqué mais plus sécurisé que le petit carnet que certain-e-s ont dans leur poche !!

Naviguer en « toute » sécurité …. et avec discernement

Tous les participants étaient au clair sur les préférences à mettre en place dans le navigateur (anti-traçage avec disconnect / anti-publicité avec u-block / pas d'enregistrement des mots de passe / …). On trouve des choses claires là-dessus sur les fiches du CECIL.

La question de la sécurité sur Internet se pose différemment selon les contextes et ce que l'on souhaite : jusqu'où on veut se protéger, dans quel cas on laisse plus ouvertes les choses … l'approche peut se faire avec discernement … selon que l'on partage un secret ou qu'on communique des données sensibles ou pas.

Un petit tour par WEBKAY *pour* « *What Every Browser Knows About You* », permet de voir toutes les données qui 'sortent' de son ordinateur (localisation, nature du système d'exploitation, niveau de sa batterie, sites visités, …) si on n'a pas de blocage mis en place.
Juste après ces constats, on a vite envie de se munir de 'NOSCRIPT' … certes cela oblige à désactiver le blocage sur certains sites qu'on veut malgré tout aller voir et qui utilise du javascript, mais au moins sait-on ainsi ce qui se passe. On autorise un par un, tout le temps ou temporairement le temps d'une connexion, les sites qui sont sinon bloqués par Noscript car ils œuvrent au traçage de notre activité sur internet.
Une fois installé, la géolocalisation disparaît, et toutes les autres informations aussi :)

ANTANAK

La cryptographie, c'est quoi et pour quels usages

L'outil PGP *pour "Pretty Good Privacy"* (*="Plutôt bonne intimité"*) est un **logiciel de cryptographie** renforcée qui est particulièrement bien adapté à l'utilisation sur Internet, gratuit et très sûr. Lorsqu'il est correctement utilisé, la lecture des messages que ce logiciel a chiffrés est impossible sans posséder la clef de déchiffrement.
En effet, il sert à fournir deux serrures de clefs : 1 clef privée qui a 1 unique propriétaire déclaré et qui est elle-même protégée par une phrase de passe (20 caractères au moins), et 1 clef publique qui peut être fournie à tout un chacun, pour pouvoir communiquer avec cette personne. C'est un chiffrement asymétrique.

Le logiciel libre GPG (pour Gnu Privacy Guard) s'installe en local sur son ordinateur. Il est autorisé depuis 1999 en France.

Il existe des serveurs de clefs publiques, sur lesquels on peut retrouver la clef de quelqu'un-e qu'on ne connaît pas mais à qui on va pouvoir ainsi écrire de manière confidentielle.
À l'inverse, seul le propriétaire de la clef privée va pouvoir authentifier la provenance du document qu'il émet, laquelle sera attestée par la clef publique de recevant. La clef publique et la clef privée sont liées.

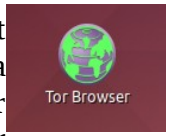
Il y a d'autres outils de même nature, tel que OMIT et SKS.

Tous les usages sont certes imaginables : en l'occurrence, il suffit qu'un collectif ait besoin de s'écrire des choses complètement non déchiffrables par des tiers externes, pour que ce système soit judicieusement utilisé sur internet.

Utiliser un réseau libre alternatif : Tor

Sans aller jusqu'à utiliser des outils de cryptographie de ces messages, si on n'estime pas en avoir besoin en terme de contenu, il peut être intéressant d'utiliser un réseau différent.

Tor est un réseau informatique superposé mondial et décentralisé, permettant un routage en oignon. Il se compose en effet d'un certain nombre de serveurs, appelés nœuds du réseau et dont la liste est publique. Ce réseau permet d'anonymiser l'origine des connexions : cela peut entre autres servir à anonymiser la source d'une session de navigation ou de messagerie instantanée (chat). Les informations passent de l'un à l'autre, déroutant les pisteurs ...



Cependant, l'anonymisation du flux n'est pas suffisante, car l'application peut potentiellement transmettre des informations annexes permettant d'identifier la personne : c'est pourquoi le projet Tor développe également un navigateur Web basé sur Firefox : Tor Browser, ainsi que d'autres applications spécialement modifiées pour préserver l'anonymat de leurs usagers. C'est un logiciel libre. Très facile à installer.

Et si on ne s'en sert pas « pour soi », servons-nous-en pour protéger, par le nombre d'utilisateurs et trices qu'on sera, ceux et celles qui en ont vraiment besoin — de se protéger et d'être protégé-e-s ...

ANTANAK

Quelques problèmes soulevés ...

- ✗ Sur Thunderbird, il n'y a pas de protection directe sur le logiciel, mais on peut chiffrer ses courriels (clefs publique et privée)

- ✗ Les bases de données « identifiants / mots de passe » se font régulièrement attaquées : Linked'In, Yahoo, … et bien d'autres.

- ✗ Démarrer sur sa propre clef, avec un système installé, nécessité d'avoir accès au démarrage de l'ordinateur (pas toujours possible dans les lieux publics). Du coup, on peut préférer utiliser le mode de navigation privée permet d'empêcher l'ordinateur sur lequel on travaille momentanément de se souvenir des connexions / sites visités.

- ✗ Flash Player sera bientôt terminé – déjà on ne forme plus dans les écoles à son développement ; tout se fera bientôt sous HTLM5.

- ✗ On peut aussi chiffrer ses données stockées sur son ordinateur. A minima les données personnelles.

- ✗ On n'a pas eu le temps de parler du VPN (Virtual Private Network = réseau privé virtuel) … ce sera pour une prochaine fois !

On finit la séance avec d'autres points d'actualité — *dont le TES, ce fichier géant en cours de programmation en France …, ainsi que le prochain colloque organisé par le CECIL, la Quadrature du Net et le Syndicat de la Magistrature* — ou plus lointains – *dont l'initiative en 2015 du 'ni pigeons ni espions', et sur les recherches de Antoinette ROUVRAY sur le bigdata, les travaux sur google, … etc.*