Atelier 1 : Enjeux

Cycle d'ateliers Internet et vie privée

27 juin 2009

Rien à cacher ?

« *Mais pourquoi aurai-je besoin d'être parano ? Je n'ai rien à cacher.* » pourrait-on entendre en réponse au conseil précédent...

Et le code secret de votre carte bleue ? Son numéro et sa date d'expiration ? Aucun soucis à ce qu'on utilise l'argent sur votre compte bancaire ? Tout le monde a quelque chose à cacher...

Et encore, vous avez quelque chose à cacher *maintenant*. Mais qu'en sera-t-il plus tard ? Les lois et les gouvernements changent. Votre situation personnelle peut changer. Ce qui n'était pas important avant (comme cette fois où vous avez sauté la barrière de votre lycée pour aller manifester avec les copains et copines) peut devenir important (si vous postulez auprès du Ministère de l'Intérieur[1]).

Des ordinateurs ?

Les ordinateurs sont des machines conçues pour s'occuper d'informations. Malheureusement. Ces machines savent précisemment enregistrer, traiter, analyser, classer de l'information. Et c'est par ces machines que passe une partie de plus en plus grande de nos existences... que ce soit dans les bases de données de producteurs, d'exploitants, de marchands ou dans l'intimité de nos courriers.

Et comme dans les ordinateurs, la copie ne vaut que quelques micro-volts, on peut considérer que *mettre une information sur un ordinateur*, surtout quand il est sur un réseau, *c'est accepter qu'elle peut nous échapper*.

Note : Ceci n'est pas un jugement moral sur ces technologies simplement un rappel de faits. Internet et les ordinateurs sont là ; on peut choisir de les utiliser plus ou moins, mais en restant dans le monde occidental, on n'y échappe jamais vraiment totalement, alors autant essayer de comprendre ce que ça implique.

L'essentiel sur Internet

Internet est un « réseau à connectivité globale ». Toutes les machines peuvent parler à toutes les autres machines. Donc toutes les machines connectées ont une adresse, qu'on appelle une adresse IP. Tout comme on a une adresse pour que La Poste amène du courier.

Genre : `80.67.172.39` (`webmail.no-log.org`)

Internet est un réseau *a-centré* : il n'y a pas de centre. Les informations transitent à travers une multitude de machines (des *routeurs*) qui tentent d'acheminer ce qu'elles reçoivent vers leur destination.

Internet fonctionne en découpant les données échangées en petits morceaux qu'on appelle des paquets. Ces paquets sont indépendants, peuvent être perdus, prendre plusieurs chemins différents... Contrairement au téléphone pour lequel on établie d'abord un circuit entre les « centraux » qui ne change pas du début à la fin de la communication.

99% des paquets acheminés par Internet contiennent une adresse d'expédition et une adresse de destination. L'adresse d'expédition permet de faire parvenir un ou pluiseurs paquets en réponse. Ça peut être un routeur qui

[1] L'anecdote vient du livre « Sous surveillance ! » de T. Rousselin et F. De Blomac.

dit « machine injoignable » ou les données qu'on a pu demander à un serveur.

Les « logs »

Quand on envoi des paquets de données vers Internet, on ne sait pas ce que les machines qui le transmettent en font, ni ce qu'en fait concrêtement la destination.

Dans la majorité des cas, si on s'adresse à un serveur, ce dernier va enregistrer la requête dans un journal avec l'heure, l'adresse ayant effectué la demande et la nature de cette dernière. Cela est valable pour le web, le mail, et la plupart des autres services.

En France, le décrêt du 24 mars 2006 stipule que les « opérateurs de communications électroniques conservent [...] » :

1. Les informations permettant d'identifier l'utilisateur ;
2. Les données relatives aux équipements terminaux de communication utilisés ;
3. Les caractéristiques techniques ainsi que la date, l'horaire et la durée de chaque communication ;
4. Les données relatives aux services complémentaires demandés ou utilisés et leurs fournisseurs ;
5. Les données permettant d'identifier le ou les destinataires de la communication.
6. Pour les activités de téléphonie [...] celles permettant d'identifier l'origine et la localisation de la communication.

Et celà pour une « durée de conservation des données [...] d'un an à compter du jour de l'enregistrement. »

Ces informations doivent être transmises à la suite d'une *réquisition judiciaire* émise par un juge d'instruction dans le cadre d'une enquête. Néanmoins, la loi « Antiterroriste » du 3 janvier 2007 permet aux membres des brigades anti-terroristes d'effectuer ces requêtes sans intermédiaire.

L'essentiel des lois concernant la responsabilité des fournisseurs de service à ce jour est rassemblé sur le site de l'association Globenet[2] .

Sans qu'on le sache non plus, il est aussi possible pour tous les intermédiaires d'analyser les données qui sont transités. Ou de les enregistrer quelque part. Voir de les modifier sur le chemin.

Spoofing

Le « spoofing », c'est le nom anglais de la technique permettant de se faire passer pour ce qu'on est pas.

Internet, au début, y avait une dizaine de facs aux États-Unis, soit un environnement ou les gens se font confiance. Or maintenant, c'est beaucoup plus grand mais la plupart des protocoles inventés à l'époque n'ont pas changé.

Du coup, il existe des techniques permettant de mentir entre autre sur le contenu de l'annuaire (DNS), l'adresse d'émission d'un paquet, les systèmes coordination des routeurs, et bien entendu l'email.

Sniffage

N'importe quel intermédiaire dans le réseau peut examiner le contenu des données qui transitent. Mais c'est aussi possible par ailleurs : un ordinateur peut se faire passer pour un intermédiaire (*spoofing*), sur le Wi-Fi, il suffit d'être à côté ou d'avoir une bonne antenne, sur le cable ou l'ADSL, il existe également des techniques... Bref, le plus simple est de partir du principe que tout ce qui sort d'un ordinateur à destination du reste d'Internet peut être observé.

Donc on utilise des techniques cryptographiques pour chiffrer les échanges afin que seul les interlocuteurs auxquels ils sont destinés puissent les lire. Mais ce n'est pas aussi simple. Par exemple, avec le *webmail* de GMail ou Yahoo !, seul la phase de connexion (où l'on entre le mot de passe) est chiffrée. Le reste des pages (et donc des messages personnels) ne l'est pas,

[2] `http://www.globenet.org/Le-Tombeau-de-la-Liberte.html`

les messages sont donc envoyé « en clair » et lisible par tout le monde. C'est un exemple parmis tant d'autre...

Man-in-the-middle

Il faut aussi s'assurer qu'on chiffre pour le bon interlocuteur. L'utilisation du protocole « sécurisé » d'accès au web, `HTTPS`, utilise pour cela des certificats. Il est *nécessaire* d'y porter attention, sans cela, il est facile de se faire passer pour le serveur auquel on croit se connecter de façon « sûre », alors qu'en fait tout le chiffrage ne sert à rien ; vu que l'intégralité des échanges est intercepté.

Ce qu'on donne (trop) volontairement

On pourrait continuer à démontrer tout ce qui fait que la « sécurité informatique » est un mythe pendant longtemps, mais peut-être est-ce plus intéressant de regarder à quel point on peut aussi avoir tendance à diffuser nous-mêmes des informations de notre vie privée.

Les journalistes de la revue *Le Tigre* ont publié dans le volume 28 de leur revue ce qu'ils ont appelé un « portrait Google », une idée « tout simple : on prend un anonyme et on raconte sa vie grâce à toutes les traces qu'il a laissées, volontairement ou non sur Internet. » Ce premier portrait, de Marc L *[3] , a ensuite fait pas mal de bruit dans la presse[4] .

En effet, ce portrait, réalisé à partir de *Google*, *Facebook* et *Flickr*, surtout, contenait le lieu de résidence, les voyages, l'employeur, et des descriptions physiques des ami·e·s de Marc L *. Et beaucoup de journalistes ont crié « au scandale », alors que toutes ses informations étaient visibles par (quasiment) tout le monde sur Internet ; vu qu'elles y avaient été généreuseument mises en ligne par l'intéressé.

L'exemple est suffisament parlant : on laisse des traces indélébiles[5] de nos intimités, souvent bien trop volontairement. Et sans trop savoir à qui ni à quoi elles pourraient servir.

Et si certaines personnes en doutaient, ces informations sont *déjà* exploité par la police, comme en témoigne un article du Figaro du 2 avril 2009[6] . Et vous pouvez toujours vous dire que vous n'avez rien à vous reprocher, mais « pour de simples vérifications d'environnement, comme les fréquentations d'un suspect, les enquêteurs accèdent aux informations au même titre que n'importe quel surfeur puisqu'elles sont publiques. »

Vous êtes sûr·e que vous n'allez pas faire vos courses dans une épicerie quelque part en Corrèze ?

L'espoir fait vivre

L'informatique et les outils de communications éléctroniques sont là. On peut lutter contre, refuser de s'en servir, mais cela n'empêchera pas d'autres de s'en servir *malgré* nos volontés... la *vie privée* est rarement une affaire solitaire. Alors *soyons parano*, prenons l'habitude de nous interroger sur ce que deviennent les informations nous conçernant, et réapproprions-nous l'usage (ou le non-usage) de ces outils.

[3] `http://www.le-tigre.net/Marc-L.html`

[4] `http://www.le-tigre.net/Volume-30.html#page_12`

[5] Le projet *Internet Archive* passe justement son temps à archiver toutes les pages web disponibles sur Internet : `http://www.archive.org/`

[6] `http ://www.lefigaro.fr/actualite-france/2009/04/03/01016-20090403ARTFIG00007-facebook-ou-myspace-une-mine-d-or-pour-la-police-.php`