Cryptographie et Protection de la Vie Privée

Contents

Note : Ce texte a été écrit en début 2008, et n'a pas été mis à jour depuis. Je ne pense plus aujourd'hui que son contenu soit particulièrement utile, il vaut mieux consulter directement les Références (section 5).

1 Introduction

Cette page est encore une autre tentative pour expliquer ce qu'est la cryptographie, et pourquoi elle est utile. Beaucoup de pages comme celle là existent déjà (voire les références (section 5)), mais il me semble qu'ajouter un peu de bruit peut aider.

2 Qu'est-ce que la cryptographie ?

De l'article Wikipedia [1] :

> La cryptographie est une des disciplines de la cryptologie s'attachant à protéger des messages (assurant confidentialité, authenticité et intégrité) en s'aidant souvent de secrets ou clés.

1. `http://fr.wikipedia.org/wiki/Cryptographie`

"Cacher" l'information (en l'encryptant) est l'un des buts bien connus de la cryptographie, mais *l'authenticité* à l'aide des signatures numériques [2] est un autre qui n'est pas moins important : pourquoi envoyer des informations encryptées si l'on est pas sûr qu'on les envoient à la bonne personne ?

Vous utilisez la cryptographie quand vous vous connectez à votre site d'e-banking, ou quand vous donnez votre numéro de carte de crédit à un site d'achat. Cela empêche que quelqu'un lise votre numéro de carte de crédit pendant qu'il est transmit sur le réseau.

Bien sûr, SSH [3] utilise aussi la cryptographie pour éviter l'interception de mot de passe. Beaucoup de programmes, libre ou pas, utilisent la cryptographie.

3 En quoi est-ce utile ?

La cryptographie est utile pour communiquer de façon sécurisée à travers un cannal non-sécurisé comme l'Internet. En bref : si A et B communiquent en uttilisant des protocoles cryptographiques sécurisés, ils sont sûrs qu'ils communiquent avec la bonne personne, et personne ne peut comprendre ce qu'ils se racontent.

Certaines personnes sont sceptiques sur les usages pratiques d'une telle réalisation. Voici les réactions les plus communes.

3.1 L'encryption est uniquement pour les militaires

Bien sûr que non : des applications civiles ont déjà été données en exemple çi-dessus. L'armée n'est pas la seule entitée qui a besoin de secret : les entreprises gardent des secrets, et les gens égalemment. Lorsque ces secrets ont besoin d'être transmit à travers un cannal non sécurisé, l'encryption est un must.

3.2 L'encryption est utilisée par les criminels

Bien sûr, et alors ? Les criminels utilisent aussi des voitures et des cartes de crédit pour commettre leurs méfaits, et nous utilisons égalemment ces objets ! Ce n'est pas parce que les criminels utilisent `x` que `x` devrait être interdit. Voici une citation intéressante :

> Crime ? If you are not a politician, research scientist, investor, CEO, lawyer, celebrity, libertarian in a repressive society, investor, or person having too much fun, and you do not send e-mail about your private sex life, financial/political/legal/scientific plans, or gossip then maybe you don't need PGP, but at least realize that privacy has nothing to do with crime and is in fact what keeps the world from falling apart. Besides, PGP is FUN. You never had a secret decoder ring ? Boo !
>
> —Xenon `<an48138 at anon.penet.fi>` (Copyright 1993, Xenon)

3.3 Mais je n'ai rien à cacher !

C'est l'argument le plus commun. La première réponse serait : même si vous n'avez rien à cacher, vous avez quand même besoin d'utiliser la cryptographie *pour l'authenticité*. Il est

2. `http://fr.wikipedia.org/wiki/Signature_numérique`
3. `http://www.openssh.org/`

trivial, par exemple, d'envoyer un email en se faisant passer pour vous [4] (en anglais). Les signatures numériques peuvent résoudre ce problème.

La deuxième réponse est que même si vous n'avez rien fait d'illégal, vous avez quand même des choses à cacher : autoriseriez-vous quelqu'un à s'asseoir juste derrière vous et à regarder votre moniteur toute la journée ? La protection de la vie privée est un droit fondamental, et c'est ce que l'encryption protège.

Une fois que l'on admet que l'on envoie parfois des informations privées, tout encrypter est une bonne idée : si vous n'encryptez que les informations réellement privées, les gens sauront que vous envoyez du contenu sensitif et pourraient essayer de casser votre chiffrage ou de vous empêcher d'utiliser l'encryption. Cependant si vous encryptez absolument tout ce que vous envoyez, personne ne peut savoir si ou quand vous avez envoyez des informations secrètes.

Phil Zimmermann, l'auteur de PGP [5], explique tout cela bien mieux que moi dans Pourquoi j'ai écrit PGP [6]

3.4 Personne ne lit / se soucie des données de toute facon

Peut-être, mais alors seriez vous prêt à écrire votre message sur votre page web, ou l'envoyer sur une carte postale ?

De plus, on ne parle pas seulement d'humains : des systèmes complétement automatisés existent qui peuvent intercepter des communications et faire une analyse du contenu basée sur des mots clés. Même si ils ne trouvent rien, votre communication sera peut-être archivée pour un examen plus approfondi.

En bref, vous ne savez jamais qui pourrait écouter : utiliser la crypto est un faible prix à payer pour être sûr que vos communications restent privées.

4 Le réseau de confiance

Une fois que vous avez accepté que vous devez utiliser la cryptographie, tout n'est pas magiquement résolu : l'encryption est relativement facile à réaliser, mais pour garantir l'authenticité, on a besoin d'utiliser la confiance. Ce qui suite est une version simplifiée de ce dont on a besoin, et les manières de le réaliser. Si vous voulez rentrer dans les détails techniques, vous pouvez commencer par lire l'article Wikipedia sur la cryptographie assymétrique [7].

En gros, si vous êtes A et que vous voulez être sûr que B est vraiment celui qu'il dit qu'il est, vous avez besoin de faire confiance à quelqu'un qui fait confiance à quelqu'un qui fait confiance à quelqu'un... Qui connaît B et peut certifier qu'il est vraiment celui qu'il prétend être !

Il y a de nombreuses manières de réaliser ceci : le système populaire sur le web en ce moment est centralisé : vous payez certaines grosses compagnies "de confiance" pour qu'ils disent aux autres que vous êtes celui que vous dites être. La faille dans ce système est évidente : il faut faire confiance à ces grosses compagnies !

Un autre système populaire est le réseau de confiance, implémenté par GPG [8]. En gros, vous vérifier manuellement l'identité de certaines personnes (par exemple, vous les rencontrez

4. http://en.wikipedia.org/wiki/E-mail_spoofing
5. http://fr.wikipedia.org/wiki/PGP
6. http://biblioweb.samizdat.net/article4.html
7. http://fr.wikipedia.org/wiki/Cl%C3%A9_publique
8. http://www.gnupg.org/

dans la vraie vie), et vous pouvez ensuite leur faire confiance. Si votre réseau de confiance est suffisament grand, vous pourriez trouver quelqu'un auquel vous faites confiance qui fait confiance à quelqu'un qui ... Qui fait confiance à B.

Bien sûr, c'est trop simplifié : la confiance n'est pas quelque chose de complétement transitif : si vous faites confiance à B, et que B fait confiance à C, vous pourriez bien ne pas faire complétement confiance à C. Plus la chaine devient longue, plus la confiance en est diminuée. C'est pour cela que GPG impose par exemple une longueur de chaine maximale.

Comme ce réseau de confiance me semblait être une meilleure idée que le système centralisée opérant sur le web, j'ai décidé d'essayer d'utiliser activement GPG pour mes communications.

4.1 Comment j'utilise GPG

4.1.1 Signature des releases

Comme vous l'avez peut-être remarqué, je signe toutes mes releases sur `svasey.org` avec ma clé GPG [9]. Si vous avez trouvé une tarball non-signée sur mon site, je ne l'ai pas crée ! (ou j'ai peut-être juste oublié de la signer...). Signalez le moi [10].

Signer une release est utile pour éviter qu'elles soient modifiées durant leur transfert : un attaquant pourrait la remplacer avec un malware, et le pauvre utilisateur l'installerait sans prendre garde, car il croirait qu'il est en train d'installer un innocent programe de `svasey.org`. Des problèmes pourraient égalemment survenir si mon serveur est compromis : encore une fois, l'attaquant pourrait remplacer les tarballs avec des malware.

4.1.2 Signature des emails

Je signe tous mes emails sortant. Si vous recevez un mail non-signé, il ne vient pas de moi !

4.1.3 Encryption des emails

Malheureusement, pas tout le monde à qui j'envoie des mails a une clé GPG. Cependant, j'encrypte systématiquement tous les mails vers mon réseau de confiance. Si quelqu'un d'autre a une clé GPG et me demande de lui envoyer des informations de manière cryptée, je le ferai : cela ne peut pas abaisser le niveau de sécurité !

4.1.4 TLS

Il est toujours possible d'utiliser TLS [11] avec mes sites web. Mon certificat est signé en utilisant GPG. Voir ma documentation TLS pour svasey.org [12] pour plus d'information.

5 Références

– The comp.security.pgp FAQ [13] (EN) est un bon point de départ sur PGP

9. `http://certs.svasey.org/gpg-svasey-pubkey.asc`
10. `http://svasey.org/about_en.html#contact`
11. `http://fr.wikipedia.org/wiki/Transport_Layer_Security`
12. `http://svasey.org/tls-user_en.html`
13. `http://www.cam.ac.uk.pgp.net/pgpnet/pgp-faq/`

– André Bacard's "Non-Technical PGP FAQ"[14] (EN) répond à "je n'ai rien à cacher et à d'autres argumeents contre la crypto
– Pourquoi j'ai écrit PGP[15] est un excellent article par l'auteur de PGP

14. http://www.andrebacard.com/pgp.html
15. http://biblioweb.samizdat.net/article4.html