[Fiche 12] Le chiffrement des communications

Si protéger ses données enregistrées est une bonne pratique, il est tout aussi fondamental de protéger ses communications : courriels, discussions et échanges avec les sites Internet.

Le chiffrement asymétrique

S'agissant des communications, les méthodes de chiffrement sont différentes de celles présentées précédemment dites "*symétriques*" (le même code est utilisé pour chiffrer et déchiffrer).

En effet, il faut que la personne ou le serveur avec qui l'on communique soit capable aussi bien de déchiffrer les messages qui lui sont envoyés que de chiffrer ceux qu'il envoie pour que la communication ne puisse être comprise par quelqu'un qui "écouterait" le réseau.

Une solution est de partager un code entre les deux correspondant·es (*chiffrement symétrique*), mais cela implique une confiance totale et pose de gros problèmes pratiques (transmission du code, besoin d'autant de codes que de correspondants...). Des solutions plus efficaces permettent de ne pas "partager" son code de déchiffrement tout en chiffrant la communication.

Ce sont les méthodes de chiffrement dites "*asymétriques*". De façon simplifiée, chaque correspondant utilise deux clés : une clé publique communicable à tous, servant à chiffrer les messages, et une clé privée nécessaire pour les déchiffrer.

La clé privée, à ne pas communiquer, est protégée par une phrase de passe personnelle.

Cela peut sembler étrange qu'une clé qui permet de "chiffrer" ne puisse pas permettre de "déchiffrer", mais ces méthodes ont fait leurs preuves.
Une image utilisée est que la clé publique correspond à des cadenas ouverts distribués aux correspondant·es, qui une fois refermés par eux ne peuvent être ouverts que par l·a détent·rice de la clé privée (qui a envoyé les cadenas).

Ces méthodes sont aussi utilisables en tant que "signature" pour authentifier une communication ou un document. On signe le document avec sa clé privée, dont l'authenticité peut être vérifiée à la réception grâce à la clé publique.

Chiffrer ses navigations

Une des applications de cette méthode est le protocole TLS (pour *Transport Layer Security* couramment utilisé sans en avoir toujours conscience en naviguant sur Internet. C'est le "s" du "HTTPs" ou le petit cadenas vert qui apparaît dans la barre d'adresse du navigateur. Automatiquement, avant toute transmission d'informations, les deux ordinateurs mis en contact (exemple : le votre et celui de votre banque), génèrent puis se transmettent leurs clés publiques et déchiffreront avec les clés privées correspondantes.

Ce petit "s" a donc une importance considérable. Sans cela, un "espion" connecté à un réseau Wi-Fi ou au réseau filaire du quartier ou du noeud réseau, le propriétaire du noeud TOR de sortie de la communication, etc., pourrait connaitre le contenu des échanges (coordonnées bancaires...).

Le module complémentaire "HTTPs Everywhere" de l'*EFF* permet de tester en permanence s'il est possible d'établir une communication en HTTPs et si oui la force.

Pour l'installer sur Firefox :

> Télécharger le logiciel dans la base de modules de Firefox en cliquant sur "Ajouter à Firefox", cliquer sur "Installer", redémarrer le navigateur.

Attention, si l'HTTPs protège la confidentialité du contenu des échanges, mais l'existence d'une communication entre A. et B. et son horaire restent connus. Pour dissimuler ces informations d'autres protections sont nécessaires.

Chiffrer ses échanges personnels

Une autre application de ce mécanisme de clé privée / clé publique consiste à chiffrer volontairement ses communications personnelles (courriels, messagerie instantanée, SMS et autres communications par ordiphone...).

Pour ce faire, il existe un standard efficace *"OpenPGP"* pour *Pretty Good Privacy* qui est notamment mis en œuvre par un logiciel libre appelé GPG (*Gnu Privacy Guard*).

Même si GPG est moins "automatique" que l'HTTPs, il n'est pas si difficile de chiffrer ses courriels à condition de convaincre ses correspondant·es d'en faire autant.

Chiffrer ses courriels

- Il faut commencer par installer le logiciel GPG, installé par défaut dans la plupart des distributions Gnu-Linux.

  Pour Windows, télécharger et installer (en suivant les consignes) : Gpg4win.

  Pour Mac OS X, télécharger et installer (en suivant les consignes) : GPGTools.

Avec Thunderbird

Pour chiffrer ses courriels avec Thunderbird, il suffit de :

> télécharger le module Enigmail. Thunderbird lancé, cliquer sur l'icône des préférences, puis sur "Modules complémentaires", dans la barre de recherche chercher Enigmail et l'installer.
>
> Ensuite, après redémarrage de Thunderbird, dans "Préférences", choisir "Enigmail" -> "Gestion de clef"
> puis dans la nouvelle fenêtre ouvrir le menu "Générer" -> "Nouvelle paire de clefs".
>
> Choisir l'adresse concernée, indiquer une phrase de passe, qui protégera la clé, dans l'onglet avancé choisir une clé RSA 4096 (sur le délai d'expiration voir "pour aller plus loin"). Cliquer sur "Générer la clé".

Ainsi est générée la paire "clé publique / clé privée", la clé privée étant protégée par la phrase de passe.

Cette opération est facile, celle de chiffrer un message également. Ces échanges chiffrés nécessitent toutefois que les autres correspondants disposent aussi d'une paire de clé et que l'on récupère leurs clés publiques.

Pour cela soit on reçoit la clé publique et on l'ouvre le fichier *via* Enigmail, soit il faut la chercher dans un annuaire.

> L'accès à ces annuaires se fait dans la fenêtre "Gestion des clefs" d'Enigmail. Cliquer sur "Serveurs de clefs" et indiquer l'adresse du correspondant en espérant qu'il ait publié sa clé.

À chaque rédaction de courriel, muni de la clé publique d'un·e correspondant·e, on peut alors chiffrer le message en appuyant sur le cadenas en haut de la fenêtre.

Le même cadenas permet aussi d'authentifier son message par une signature chiffrée.

En utilisant un Webmail

Il est également possible d'utiliser le module Mailvelope sur Firefox (ou Chrome), qui gère l'utilisation de GPG pour les Webmails à partir du navigateur. Cette solution n'est pas la plus conseillée car le navigateur est un logiciel plus complexe qu'un logiciel dédié à la seule gestion des courriels et a plus de chance de permettre une attaque sur la confidentialité des échanges (par exemple via un autre module).

Cette possibilité fonctionne quel que soit le Webmail, de préférence ceux conseillés par le CECIL, mais même chez les acteurs commerciaux (Gmail, Yahoo, Free, Laposte.net, etc.).

> Il suffit d'ajouter l'extension Mailvelope, alors un petit cadenas avec une clé s'affiche dans la barre de recherche.

Soit l'on dispose d'une paire de clé que l'on peut "importer", soit le module peut en générer comme avec Thunderbird.

Pour chiffrer avec Mailvelope :

> En étant connecté sur son Webmail, l'icône d'un petit bloc-notes avec un crayon apparaît dans le corps du courriel. Si l'on possède la clé publique d'un destinataire, en cliquant sur cette icône il est possible de chiffrer le message.
>
> Pour lire un courriel chiffré, il suffit de saisir sa propre phrase de passe.

Ces indications sont sommaires et ont pour seule vocation d'aider à faire les premiers pas. Il est vivement recommandé de consulter des tutoriels plus complets disponibles en fin de fiche pour comprendre les erreurs à ne pas commettre !

À noter en complément à la fiche 8 sur les hébergeurs de courriels alternatifs, le Webmail suisse ProtonMail.ch propose à la fois un chiffrement par défaut entre titulaires de compte Proton Mail, une gestion de PGP plus large, mais aussi un mécanisme de chiffrement à clé unique (transmise par un autre biais) pour transmettre des courriels chiffrés à des correspondants peu motivés à installer un dispositif ou l'autre. Il peut constituer une solution convenable pour chiffrer des échanges courriels.

Chiffrer ses autres échanges

Les discussions sur Internet ne passent pas que par courriels : forums, discussions directes, qu'elles soient audio, vidéo ou textuelles par *tchat*.

Il existe des solutions (utilisables sur les différents systèmes d'exploitation) qui permettent de discuter en ligne de façon plus sécurisée et que le CECIL recommande :

- **Jitsi.org**, (en remplacement de Skype) qui offre un service protégé pour des échanges audio et/ou de tchat,
- **Tox.chat** et Ring.cx évoqués fiche 7 offrent des services de conversations audio comme textuels chiffrés,
- **Crypto.cat** permet de créer des tchats intégralement chiffrés.

Si l'on souhaite absolument continuer à utiliser sa méthode de tchat habituelle (live, gtalk, Facebook...), il reste possible de chiffrer ses communications. Cela nécessite aussi que les correspondants installent un autre logiciel tel que Jitsi ou Pidgin qui acceptent ces méthodes de tchat et auxquels on peut adjoindre le plug-in Off-The-Record (ou OTR) qui va offrir un chiffrement asymétrique avec ses correspondants (selon le même principe d'échanges de clés).

Ces logiciels sont globalement assez simples à prendre en main et intuitifs dans leurs fonctionnements, le plus difficile reste toujours de convaincre ses correspondant·es de les utiliser !

Pour aller plus loin :

Sur le chiffrement des communications en général :

- Framablog.org, *Le chiffrement maintenant*, une traduction par Framasoft d'un guide anglais sur les bonnes pratiques du chiffrement de ses communications,
- un article très complet de M. Lee sur The Intercept (en anglais), *Chatting in Secret While We're All Being Watched*, expliquant comment protéger autant que possible ses communications en alliant TOR et le chiffrement.

Sur l'HTTPs :

- Wiki.linuxwall.info, *Principes du chiffrement avec le protocole SSL/TLS*,
- sur le site de l'EFF, la FAQ de l'extension HTTPs Everywhere (en anglais) qui permet de comprendre de nombreux aspects du fonctionnement de l'extension et du protocole.

Sur GPG - PGP et chiffrer ses courriels :

Pour compléter les indications de cette fiche et chiffrer correctement ses messages :

- une explication des bonnes pratiques sur GPG sur le site RiseUp.net, *Open PGP Best practices*,
- autodéfense courriel, un tutoriel de la Free Software Fondation (en français) pour chiffrer ses courriels
- PGP sous Windows/Linux/Mac Le b.a-ba celui de l'EFF aussi en français.
- le tutoriel d'OpenPGP, openpgp.vie-privee.org et sur securityinabox.org (en anglais) un guide pour Enigmail sous Thunderbird,
- S. Bortzmeyer, sur son blog, *Ma nouvelle clé PGP*, quelques indications pour créer une clé GPG fiable,
- un tutoriel sur Mailvelope sur le site Openclassrooms.com, **Utilisez GPG depuis votre webmail grâce à Mailvelope**
- depuis les révélations d'E. Snowden, les différents logiciels présentés dans cette fiche ont des communautés actives visant à les améliorer et en démocratiser l'usage. GPG ou

Enigmail sont constamment en train d'être améliorés.

Fiche 12 [publiée le 6 novembre 2015, dernière mise à jour avril 2018]