Pratique du courriel et autodéfense informatique

Le courriel (ou email) est un courrier électronique. Comme un courrier papier, il a un expéditeur, un destinataire ou plusieurs, ainsi qu'un contenu. Dans le cas du papier, le fonctionnement est clair, on comprend intuitivement comme cela fonctionne. C'est moins vrai dans le cas du courriel. De manière très simplifiée, un courriel s'apparente à une version électronique de la carte postale : toutes les intermédiaires entre l'expéditeur et le destinataire peuvent le contenu du courriel. De plus, le secret des correspondances papiers n'est pas remis en cause, tandis qu'au nom de certains motifs (comme le « terrorisme » ou la « radicalisation ») la violation du secret des correspondances électroniques gagne en légitimité publique, tout en étant déjà pratiquée par nombre d'États (comme mis en évidence par Snowden en 2013) et par des entreprises (comme Google). Il peut donc être prudent de s'en tenir aux échanges papiers (qui ont de plus l'avantage de ne pas forcer à indiquer d'expéditeur), mais il existe aussi des moyens informatiques plus ou moins efficaces.

Tout d'abord, il faut commencer par qui héberge la boite email. Non seulement, l'hébergeur reçoit et stocke tous les courriels, mais il sait aussi quand et à partir d'où les courriels sont récupérés. Ainsi, même dans le cas où le contenu des échanges est chiffré (nous reviendrons plus loin sur cette notion), détenir accès à la boite email permet de quand même connaître les méta-données des communications (avec qui elles se font, à quelle fréquence, etc.). Ne pas utiliser une boite email fourni par n'importe qui est donc important. GMail, Microsoft Outlook et Yahoo sont typiquement à proscrire. Idéalement il faut s'auto-héberger (par exemple aidé de YunoHost). Sinon, on peut se tourner vers une association respectueuse de la vie privée (de préférence locale et à but non lucratif) qui propose l'hébergement de boîtes email (comme certains de `chatons.org` ou `riseup.net`) ou une entreprise commerciale [1, 2] (comme ProtonMail, Tutanota ou Posteo). Prévenons qu'il n'y a pas de miracle : s'il n'y a pas d'exploitation des données, le service ne se finance pas par magie, et il faut donc être prêt à donner de l'argent.

Ensuite, le choix du logicel pour intéragir avec sa boîte email est important également. Ce logiciel peut être soit une interface web (webmail), soit un logiciel à installer sur sa machine. L'interface web, qui varie selon le hébergeur, est généralement limitée au niveau sécurité. Il faut donc mieux privilégier un logiciel installé sur notre machine. Pour les ordinateurs de bureau, il y a notamment Thunderbird, et Claws Mail si on veut quelque chose de plus léger, fonctionnant tous deux sur GNU/Linux et *BSD, ainsi que sur Windows et macOS. Pour ce qui est d'Android, on peut se tourner vers K-9 Mail (disponible via F-Droid).

Enfin, on va présenter d'autres mesures de sécurité significatives. On peut chiffrer le contenu des courriels, pièces jointes comprises, mais pas les méta-données (expéditeur, destinataires, etc.). Pour cela, il y a le standard OpenPGP et sa réalisation libre GPG. La FSF a fait un très bon guide à ce sujet [3]. Le module complémentaire (plug-in) pour Thunderbird est Enigmail, c'est OpenKeychain pour K-9 Mail et GPG pour Claws Mail. Pour protéger son adresse IP et donc depuis où on communique, on peut faire passer l'email via Tor (par exemple pour Thunderbird avec TorBirdy ou le système d'exploitation Tails).

Étant donné les efforts nécessaires pour sécuriser correctement ses emails, on peut également opter pour une solution informatique qui soit plus facile pour le chiffrement des communications. Pour cela, on peut se tourner vers certaines messageries instantannées [4]. Signal est un exemple, mais il se base sur un serveur centralisé. Pour une même sécurité cryptographique, mais avec la décentralisation et la fédération en plus (comme « l'email classique »), il y a le protocole XMPP couplé à OMEMO. Pour l'utiliser, on peut conseiller les logiciels suivants : Gajim avec le plug-in OMEMO, Dino (GNU/Linux et FreeBSD), Conversations pour Android, ainsi que Monal et Siskim IM pour Apple iOS.

1. `https://privacytools.dreads-unlock.fr/#email`
2. `https://www.fsf.org/resources/webmail-systems`
3. `https://emailselfdefense.fsf.org/fr/`
4. Chiffrement de messagerie quasi instantanée : à quel protocole se vouer ?, ANSSI (`ssi.gouv.fr`) et MISC n° 90, mars 2017