Sécurité Informatique

Pourquoi crypter ses messages ?

Le courriel demeure un moyen efficace de communiquer avec ses amis, ses collègues, ou encore sa famille, mais:

- il ne permet pas d’authentifier l’identité de l’expéditeur,
- il ne permet pas de s’assurer qu’il n’est déchiffrable que par le destinataire.

Malgré la possibilité de chiffrer et signer les courriels par des méthodes cryptographiques, **gardons à l'espirt que les métadonnées peuvent être modifiées en transit** (expéditeur, objet, date et heure). La date et heure sont les seule métadonnées pouvant être vérifiés dans la signature électronique (voir ci-bas).

> *Le cryptage de messages permet d'encoder un courrier électronique, ce qui le rend lisible uniquement par la personne possédant la clé permettant de le déchiffrer.*

OpenPGP: Le chiffrement asymétrique

Pour pallier au problème d'échange de clés lors de l'établissement de communications sécuritaires, des logiciels utilisant *le chiffrement asymétrique* ont été conçus.

Une des normes basées sur ce concept est la norme **OpenPGP**. Ce type de chiffrement utilise deux clés liées mathématiquement :

- Une clé privée : Elle est utilisée pour déchiffrer un message que vous avez reçu. La vôtre ne devra jamais être révélée, même si elle est elle-même chiffrée par un mot de passe que vous détenez.
- Une clé publique : n’importe qui peut utiliser votre clé publique pour chiffrer un message avant de vous l’envoyer. Elle peut être communiquée à n’importe qui.

Voici un exemple:

Bob et Alice veulent s’échanger des messages chiffrés. Si Bob veut envoyer un message chiffré à Alice, il doit connaître la clé publique de cette dernière. Étant donné qu’elle est autorisée à communiquer sa clé publique à d’autres personnes, Alice l’envoie par courriel à Bob. Ce dernier peut maintenant l’utiliser pour chiffrer son message avant de l’envoyer à Alice.

Maintenant, imaginons qu’une troisième personne, Robert, veuille intercepter et lire les messages de Bob et d’Alice. Bob a donc chiffré son courriel avec la clé publique d’Alice. Robert ouvre le logiciel de messagerie d’Alice alors qu'elle n’est pas à son ordinateur, et découvre que Bob lui a envoyé un message chiffré. En regardant dans le répertoire « Courriels envoyés » d’Alice Robert voit que celle-ci avait transmis à Bob sa clé publique.

Il tentera sans succès d'utiliser la clé publique d’Alice pour déchiffrer le message de Bob. C'est normal car seule la clé privée d’Alice combinée au mot de passe qui y est associé permettent de déchiffrer le message que Bob a envoyé.

La signature numérique

Qu’est-ce que « signer » un message ? C’est le fait d’utiliser la clé privée pour assurer l'authenticité, l'origine et la date de création de contenus. Si vous signez vos courriels, votre destinataire saura que c’est obligatoirement le possesseur de la paire de clés qui a signé ce message. Des fonctionnalités plus avancées de OpenPGP permettent de signer la clé publique de vos interlocuteurs afin de signaler une vérification d'identité à un degré plus ou moins élevé de confiance. Ce processus ressemble au travail des notaires et constitue, dans son ensemble, ce qu'on appelle la « Web of Trust » (toile de confiance). Ainsi, il est suggéré de faire signer sa clé publique par autant de vos interlocuteurs qu'il sera possible, afin que son authenticité soit plus facile à déterminer.

Sur PC / laptop

Sur Mobile / tablette

From:
https://dulib.re/wiki/ - **Le Goût du Libre**

Permanent link:
https://dulib.re/wiki/doku.php/securiteinformatique_courriel?rev=1486127295

Last update: **2017/02/03 05:08**