Atelier “Sécuriser ses mails”

4 avril 2017

Utilisation de la cryptographie, pourquoi ?

- Utilisation de protocoles sécurisés
  - On évolue parfois en milieu “hostile” (accès wifi, réseau d’un tiers, etc.)
- Chiffrement des contenus
  - L’envoi d’un mail est à peu près équivalent à l’envoi d’une carte postale : tous les serveurs intermédiaires ont accès librement au contenu, ce qui rend possible la surveillance de masse automatisée.
- Contre l’usurpation d’identité

Utilisation du chiffrement pour sécuriser les communications avec le serveur

- Protocoles SSL et TLS
  - Chiffrement
  - Authentification
  - Autorité de certification centralisée
  - STARTTLS pour passer d'un protocole "en clair" à un protocole chiffré
- Chiffrer les connexions avec le serveur de mail
  - Protocoles POP3S et IMAPS pour la consultation
  - Envoi par SMTP authentifié
  - Accès webmail en HTTPS
- Mais aussi
  - Éviter "d'enregistrer le mot de passe", préférer un logiciel de gestion de mots de passe (vol, perte, logiciel espion, etc.)

Rappels sur la cryptographie

- Deux grandes familles
  - Chiffrement symétrique : la même clef sert pour chiffrer et pour déchiffrer
  - Chiffrement asymétrique : clef publique et clef privée
    - Des données chiffrées avec une clef publique ne peuvent être déchiffrées que si on dispose de la clef privée
    - Des données pouvant être déchiffrées par la clef publique ont forcément été chiffrées par la clef privée
- Utilisation dans le cadre de la messagerie électronique
  - Chiffrement : pour assurer la confidentialité d'un envoi
  - Signature électronique : seule protection contre les usurpations d'identité

S/MIME

- Utilise des certificats X509 (similaires à ceux utilisés pour HTTPS)
  - Inconvénient pour utilisation personnelle : nécessite l'acquisition d'un certificat
  - Devrait être utilisé par les institutions, banques, etc.

GPG

- PGP, OpenPGP, GPG (GnuPG) ?
- Chiffrement asymétrique
  - On garde précieusement sa clef privée
  - On publie la clef publique, sous forme de fichier texte (sur un site web par exemple) et/ou sur les serveurs de clefs (principalement *SKS Keyserver Pool* ; par exemple pgp.mit.edu)
- Constitution d'un réseau de confiance
  - On signe avec sa propre clef privée les clefs publiques des autres utilisateurs rencontrés, pour renforcer l'association entre une empreinte de clef et l'identité correspondante.
  - On publie ces informations de signature
  - On rapatrie les informations publiées des autres clefs
  - Par voie indirecte on peut accorder un degré de confiance aux clefs inconnues

Enigmail pour Thunderbird

- Tutoriel en ligne

https://lehollandaisvolant.net/tuto/gpg/

- Sur une distribution Linux penser à installer le paquet de GnuPG

Messagerie instantanée

- Utiliser les connexions chiffrées quand elles sont proposées
- Certains services incluent des fonctionnalités de chiffrement, par exemple Telegram, Signal
- Plugin de chiffrement du contenu des messages
  - OTR (Off The Record) : Chiffrement, Authentification, Déniabilité (authentification limitée à la durée de la conversation), Confidentialité persistante (la compromission d'une clef privée ne permet pas d'accéder aux conversations passées)