CyberEdu A13 : Cryptographie

De nos jours les données circulent tous les jours et doivent rester privées. Les échanges ont donc été sécurisés au fil du temps et répondent à 3 critères :

- Confidentialité : Les trames ne doivent pas être accessibles par un tiers.
- Authenticité : L'expéditeur doit savoir qui est le destinataire et inversement.
- Intégrité : L'information ne doit pas être modifiée entre l'envoi et la réception.

Pour répondre à ce besoin de sureté, les chiffrements ont été inventés. Un chiffrement est un procédé par lequel un message est changé à l'aide d'un algorithme qui se nomme la clé. Il existe 2 types de chiffrement : le chiffrement symétrique et celui asymétrique. Le premier impose un échange de clé (impossible en clair sur internet) pour décrypter le message, les personnes qui échangent doivent donc avoir la même clé. Quant au chiffrement asymétrique, pour être efficace on doit être sûr de l'authenticité des pairs c'est-à-dire que leurs clés doivent êtres différentes et que l'expéditeur doit posséder une image de la clé privé du destinataire pour pouvoir grâce à sa clé publique créer un codage uniquement décryptable par le destinataire. Chaque message est donc crypté différemment selon le destinataire.

Les clés publiques et privées ont donc une utilité différente dans le procédé de cryptage/décryptage :

- La clé publique sert uniquement à chiffrer le message.
- La clé privée est une clé personnelle, propre à chacun, et sert à décrypter un message avec l'aide de la clé publique de notre clé publique.

Des protocoles ont été élaborés pour différents types d'activité d'échange comme le protocole HTTPS. Celui-ci est un protocole d'échange web sur un réseau (internet ou intranet). Il existe aussi le protocole TLS (Transparent Layer Security) qui repose sur un "Handshake", c'est-à-dire qu'il y a un accord pour transmettre les clés. Ce protocole définit donc les règles de sécurité à suivre lors de l'envoi d'un message par le biais d'un réseau. Ce protocole possédait de nombreuses failles permettant aux pirates d'être un "man in the middle", c'est-à-dire de se mettre au milieu de la communication soit en se faisant passer pour l'expéditeur soit pour le destinataire. Ce protocole a donc été remplacé par son successeur le protocole SSL (Secure Sockets Layer) lequel créé un canal sécurisé entre les 2 machines réalisant l'échange, c'est aujourd'hui le protocole de sécurité le plus répandu. Pour se prémunir des risques que constitue le TLS (non-patché) et encore présent sur de nombreuses machines, il faut le désactiver des serveurs afin que les pirates ne puissent repasser les serveurs en protocole TLS et exploiter les failles et porter atteinte aux données.

Enfin, pour se prémunir des risques de piratages, il existe les certificats de domaines SSL correspondant à une carte d'identité numérique. Il en existe 3 : Organisation, Validation et étendu. Ces trois certificats sont gérés par l'organisme OCSP (Online Certificat Status Protocol), celui-ci s'assure de la validité des certificats et gère l'attribution et le contrôle de ceux-ci.