Réseaux : Sécurité

Sławek Staworko

Univ. Lille3

1er décembre 2017

Sécurité I

Enjeu majeur

- Enjeux militaires (espionnage,...)
- Enjeux financiers (commerce, échanges financiers, secrets industriels,...)
- Enjeux sur l'image de marque (réputation, confiance,...)
- Enjeux sur la vie privée (identité, dissémination d'informations,..)
- En opposition avec la volonté d'ouverture, et de visibilité sur internet, et l'utilisation de ses technologies.

Sécurité II

Plusieurs niveaux de considération : politique de sécurité

- Au niveau des utilisateurs : prise de conscience
- Au niveau des systèmes d'information : RSSI (responsable de sécurité informatique des SI), contrôle d'accès
- Au niveau des données : cryptage
- Au niveau des échanges (réseau) : authentification, identification sécurisée, détection d'intrusion, ...
- Au niveau des applications : utilisations abusives, fraude,...
- Au niveau des systèmes d'exploitation, (mises à jour, sécurité,...)
- Au niveau matériel,...

Sécurité III

3 notions différentes

- Signature : authenticité, authentification
- Chiffrement ou cryptage : confidentialité
- Preuve de non altération : intégrité

Intégrité

Intégrité

- Un test sur les données
- souvent réalisé par une fonction de hachage.
- Hachage : empreinte, représentation courte de la donnée.
- Algorithmes MD5, SHA-256.
- Souvent utilisés pour vérifier qu'un téléchargement s'est bien produit. (`ftp://ftp.free.fr/mirrors/ftp.ubuntu.com/dvd/current/`)

```
tommasi@fitis:~$ sha256sum test.html
ec0d248f191e7225bf4d81b7b4e3974dc6d947491d787a83e98f7be026b94ace  te
tommasi@fitis:~$ md5sum test.html
a9ddfec845affc0344cde06af86278c9  test.html
```

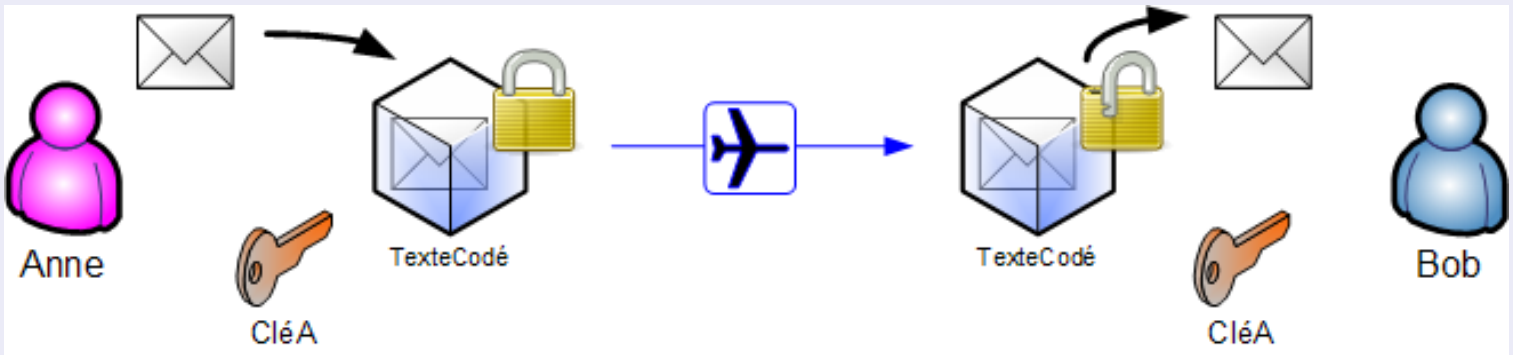
Chiffrement

- Repose généralement sur l'utilisation de clefs de cryptage.
- La clef est comme un paramètre du moyen (algorithme) de cryptage.
- Le mécanisme du chiffrement par clef permet aussi d'assurer la fonction de signature.

Chiffrement symétrique

Chiffrement symétrique

- Chiffrement à clef secrète.
- Une même clef pour chiffrer et déchiffrer.
- Principe : pour être sûr l'algorithme de chiffrement doit pouvoir être donné.
- Le nombre de clef possibles doit être très important pour éviter de les essayer toutes.
- Exemples : DES, AES, ...
- Difficultés : comment échanger les clefs secrètes ?



Chiffrement asymétrique I

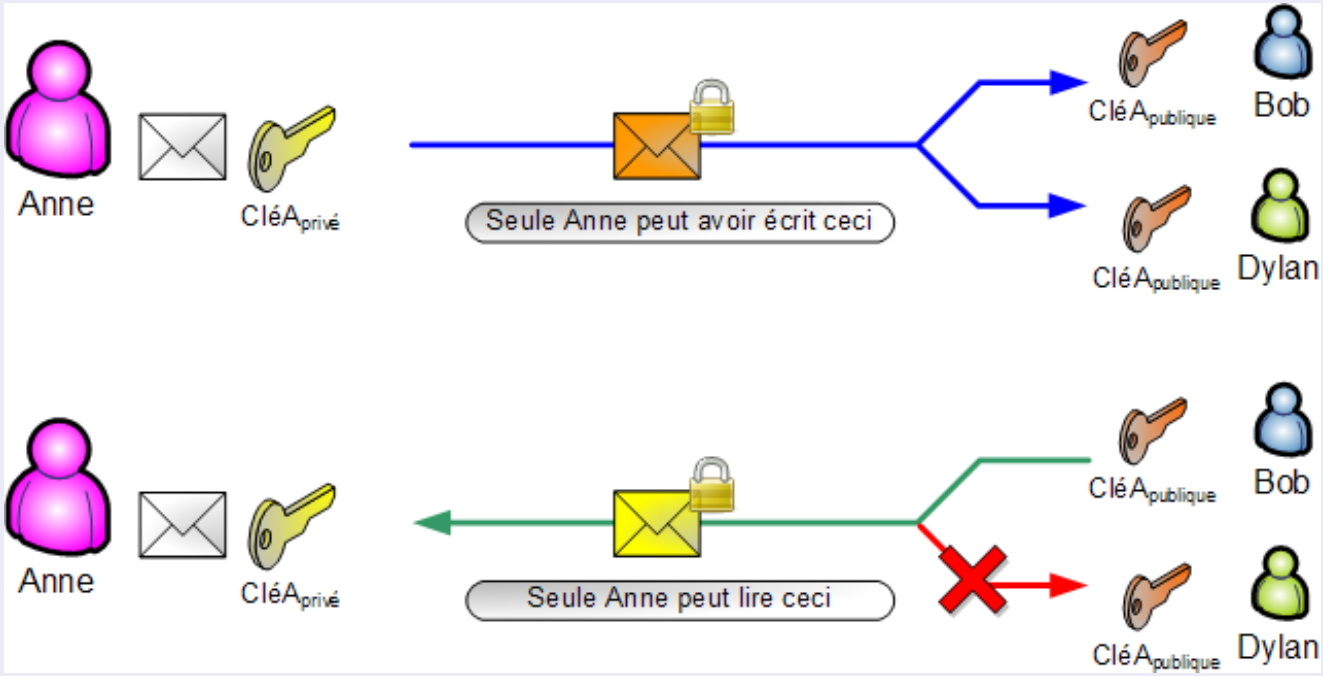
Chiffrement asymétrique

- Résout (partiellement) le problème de l'échange de clefs.
- Paire de clefs : une clef privée, une clef publique.
- Exemples : RSA (chiffrement, signature), DSA (signature)
- Difficultés : lent.

En pratique

- Clef asymétrique utilisé pour un échange de clef symétriques.
- Transmissions suivantes utilisant les clefs symétriques pour lesquelles le chiffrement est plus rapide.

Chiffrement asymétrique II



Certificats

Objectifs

- Comment transmettre les clefs publiques ?
- Comment être sûr que la clef publique est bien celle de la personne ou le service avec qui on peut communiquer ? (Attaques man in the middle)
- Le certificat = pièce d'identité numérique.

Principes

- Une clef publique
- Des méta-données incluant l'identité, la fin de validité, etc.
- Une ou des signatures certifiant que cette clef est correcte.
- Les certificats sont parfois stockés sur des serveurs de clefs.
- Deux formats : OpenPGP et X509

OpenPGP

- D'abord pour le courrier,
- Mise en place d'un réseau de confiance
- Approche décentralisée à l'image du peer to peer.
- Signature de clefs par les membres de ce réseau.
- Échange physique d'empreintes de clefs publiques si possible.

Applications

- Signature de courrier électronique : GnuPG, avec l'extension enigMail pour thunderbird, ou les autres clients de mail. Peu disponible pour les webmails.
- Ssh : connexion sécurisée à un ordinateur distant.

Exemple

ssh, sftp

- Se connecter sur une machine distante : `ssh masterid.pedago.local`.
- Générer une clef : `ssh-keygen -t rsa`
- La passphrase permet d'avoir accès à la clef privée (dans `/.ssh/id_rsa`)
- La clef publique (dans `/.ssh/id_rsa.pub`) peut être déposée sur des serveurs distants.
- Exemple : Déposer sa clef sur une machine distante dans le fichier `/.ssh/authorized_keys`
- La connexion peut se faire maintenant sans mot de passe.
- Les commandes `scp,sftp` permettent d'échanger des fichiers entre deux machines de façon cryptée.

X509

Infrastructures à clef publiques : PKI

- Des autorités de certifications existent.
- Les clefs de ces autorités reposent sur d'autres clef, etc... jusqu'à des certificats racine.
- Les certificats racine sont stockés et distribués dans les applications.
- S/MIME permet d'ajouter les méta-données pour l'échange à travers internet, par mail,...

PKI

- Ensemble de moyens organisationnels, techniques et humains mis en place pour gérer les certificats.
- Création, renouvellement, révocation, publication, séquestre,...

Applications

- TLS (ex SSL) utilise OpenPGP ou X509 au niveau transport
- HTTPS utilise TLS.
- ssh, sftp
- OpenSSL
- Les porte clefs numériques (kwallet, seahorse et autres logiciels intégrés)

Acteurs

- Thawte, Verisign, Certinomis (La poste), de nombreuses banques... pour les autorités de certification
- Soi-même (certificats auto-signés)
- Les agences gouvernementales : ANSSI, le CERTA,...

Exemple

- Allez dans les préférences de firefox, onglet, avancé, puis chiffrement.
- Observez les certificats, les autorités de certifications. Repérez les certificats racine.
- Rendez-vous sur le site `cas.univ-lille3.fr`. Affichez les informations de signature en cliquant sur l'icône devant l'URL.

Autres constructions

- VPN : réseau privé virtuel, largement utilisé par les institutions, organisations.
- Tor : réseau mondial décentralisé.