

Sécurité et Cryptographie



Principes

La **sécurité** dans les réseaux a trois **objectifs** :

Vérifier l'intégrité

Assurer la confidentialité

Permettre l'authentification

Intégrité

S'assurer qu'un document n'a **pas** été **modifié**.

On utilise une **fonction de hachage** qui calcule un nombre caractéristique (**empreinte** ou **condensé** ou **haché**) du document.

Exemple d'outils :

- Md5, sha-1 (obsolètes trous de sécurité)
- Sha-256, sha-384, sha-512

Intégrité

Pour vérifier l'intégrité on recalcule le condensé du document et on le compare avec une version antérieure.

Si les condensés sont les mêmes alors l'intégrité est vérifiée.

Sinon c'est que soit le condensé soit le document a été modifié

Confidentialité

Elle est obtenu au moyen du chiffrement du message.

Depuis les années 1970 nous disposons de deux types de chiffrement :

- Symétrique
- Asymétrique

Chiffrement **symétrique**

Cette technique est utilisée depuis l'antiquité (code de César).

Elle repose sur un **secret partagé** : la **clé** qui sert **autant** à **chiffrer** qu'à **déchiffrer**.

Il existe de nombreux algorithmes.

À l'heure actuelle le plus **sûr** est **AES**

Chiffrement *symétrique*

De manière *générale* ce type d'algorithme est *rapide* et consomme *peu* de ressources.

Pour *AES* on ne connaît *pas* d'autre méthode *d'attaque* que la *force brute* (essayer toutes les clés)

Chiffrement symétrique

Les algorithmes de chiffrement symétrique sont utilisés pour :

- Wifi WPA-PSK-TKIP (clé partagée)
- Chiffrer vos données
- Ransomware
- ...

Chiffrement *symétrique*

L'utilisation de ces algorithmes
bute sur la *sécurisation* de la
transmission de la clé.

Chiffrement Asymétrique

Ces techniques sont utilisées depuis les années 70 (service secret 1973, grand public 1976). Elle repose sur une **paire** de clés. Ce qui est **chiffré** par **une** des clés ne peut être **déchiffré** que par **l'autre**

Chiffrement Asymétrique

Les deux clés sont liées mathématiquement.

La méthode pour trouver une clé à partir de l'autre est parfaitement connue mais :

Si la taille de la clé est suffisante le temps de calcul nécessaire est prohibitif.

Chiffrement Asymétrique

Le temps de calcul augmente exponentiellement avec la taille de la clé.

Les progrès de la loi de Moore et du calcul parallèle, font que la taille de ces clés doit augmenter régulièrement

Chiffrement Asymétrique

Actuellement taille minimum
recommandée : 2048 bits

Conseillée : 4096 bits

Ces algorithmes sont beaucoup plus
consommateur de ressources que
les algorithmes symétriques.

Chiffrement Asymétrique

Une des deux clés est gardée secrète par son propriétaire, l'autre peut être diffusée librement. On parle alors de :

- Clé privée ou secrète
- clé publique

Chiffrement Asymétrique

Les deux principaux algorithmes utilisés sont :

- **RSA** (Rivest, Shamir, Adleman) (1978)
- **Diffie-Hellman** (1976)

Chiffrement Asymétrique

Diffie-Hellman

C'est le premier algorithme asymétrique Publié.

Il sert à construire un secret partagé entre deux machines.

Il permet d'utiliser des clés éphémères (différentes à chaque fois), ce qui augmente la sécurité.

Bilan intermédiaire

Fonction de **hachage** : **intégrité**

- Et si le condensé est aussi modifié ?

Chiffrement : **confidentialité**

- Êtes vous sûr de votre interlocuteur ?

Authentification ?

Bilan intermédiaire

Et si le condensé est aussi
modifié ?

Il faut protéger le condensé de
toute modification

Êtes vous sûr de votre
interlocuteur ->

Authentification forte

Solution

Les **outils** pour **résoudre** ces deux problèmes nous sont donnés par le chiffrement **asymétrique** :

Prouver qu' on **possède** la **clé privée** permet de prouver son **identité**.

Clé privée == identité

Signature

On utilise la clé privée pour chiffrer le condensé :

- Une seule personne peut le faire
- Tout le monde peut le vérifier avec la clé publique

il est impossible à une tierce personne de recréer un condensé chiffré

C'est la signature électronique

Signature

Pour **vérifier** l'intégrité d'un document **signé** il faut :

- 1) Utiliser la **clé publique** pour **déchiffrer** la **signature** et obtenir le **condensé originel**
- 2) **Calculer** le **condensé** du document **reçu**
- 3) **Comparer** les deux **condensés**

Si les deux **condensés** ne **concordent pas** c'est que **soit** le document à été **modifié**, **soit** la **signature** est **contrefaite**.

Man in the Middle

Ces techniques ne protègent pas d'une usurpation d'identité nommée attaque de « l'homme au milieu ».

Contre elle il faut avoir la garantir que la clé publique utilisée est bien celle de la personne qu'on pense → authentication Forte

Authentication forte

Elle **nécessite** l'intervention d'un tiers de confiance : une **autorité**, l'équivalent électronique d'un **notaire**.

L'**autorité** va **emmettre** un **document** qui **garantie l'identité** du **propriétaire** de la clé **publique** :

Le **certificat électronique**

Certificat

Un **certificat** fait appelle à toute les notions vu précédemment :

Il contient La **clé publique**

+ **informations** sur :

- **l'identité** du propriétaire de la clé
- Les **algorithmes** utilisés
- **Durée** de validité

Il est **signé** par l'autorité

Certificat

Pour vérifier un certificat il faut avoir la clé publique de l'autorité qui l'a émis et signé.

Elle est disponible dans le certificat racine de cette autorité.

→ Qui signe le certificat racine ?

Il est signé par l'autorité elle même :

C'est un certificat auto-signé

Certificat

Le **point faible** de ce système se trouve dans les **certificats racines** qui sont installés dans vos ordinateurs (système et navigateurs).

Il faut faire très attention à la **source** de ces **certificats Racines** pour ne pas avoir d'autorité **frauduleuse installée** sur votre machine.

Fonctionnement de SSL/TLS

La plupart des échanges sur le net sont chiffrés avec le protocole TLS.

Celui ci repose sur trois piliers :

- **Certificat** pour l'authentification
- **Diffie-Helman / RSA** pour l'échange de la clé de session
- **AES** pour le chiffrement de la session

Fonctionnement de SSL/TLS

Étape 1 : Négociation

Connexion et négociation des algorithmes de hachage et chiffrement qui seront utilisés entre client et serveur

Étape 2 : échange des certificats

Vérification de l'identité des interlocuteurs (au moins le serveur)

Étape 3 Clé de session

mise en place d'une clé de chiffrement symétrique pour chiffrer les échanges

Documentation et approfondissement

Consultez les pages de [Wikipédia](#) dans
le [portail de la cryptographie](#) pour
avoir des informations plus détaillées