Numérique et Sciences Informatiques
Chapitre XI - Sécurisation des communications

Classe de terminale

I. Généralités

Définition

Afin de sécuriser une communication, il faut avoir :

- l'**authentification** de la source et des destinataires : on utilise des clefs de sécurité.
- La **confidentialité** : un algorithme de chiffrement transforme le contenu du message afin qu'il ne soit plus lisible par personne ne possédant pas les clefs.
- l'**intégrité** des données : les données ne sont pas modifiées pendant la communication.

Principe de base

Les différentes étapes de la communication sécurisée sont :

- création du message.
- modification du message par chiffrement.
- envoi du message chiffré.
- déchiffrement par le destinataire.
- lecture du message.

II. Le chiffrement

Les méthodes de chiffrement utilisent des clefs, qui ne sont autres que des chaînes de caractères, et qui vont permettre, grâce à des algorithmes, de chiffrer ou déchiffrer des messages.
Une fois le message chiffré, il sera illisible par quelqu'un qui ne possède pas la clef de déchiffrement.

Il existe deux techniques de chiffrement : le **chiffrement symétrique** et le **chiffrement asymétrique**.

II.1. Le chiffrement symétrique

Définition

Le chiffrement symétrique consiste à :

- définir un clef de chiffrement, appelée **clef partagée**.
- la communiquer à l'ensemble des interlocuteurs.

Cette clef partagée servira à chiffrer et déchiffrer le message.

Remarque

Ainsi chaque ordinateur qui connaît cette clef partagée peut être émetteur ou récepteur.

Le cheminement d'un message est donc le suivant :

- création du message
- chiffrement du message avec la clef partagée
- envoi du message
- réception du message
- déchiffrement du message avec clef partagée
- lecture du message

Remarque

Si on fait une analogie avec la vie courante, on peut avoir la situation suivante :

- l'expéditeur et l'émetteur ont la même clef
- l'expéditeur envoie un message dans un coffre qui a été cadenassé avec la clef.
- Le destinataire reçoit le coffre cadenassé et l'ouvre grâce à la clef. Il peut alors lire le message.

L'inconvénient majeur est de donner la clef au destinataire avant d'envoyer le message. En effet, si j'envoie la clef à mon destinataire, elle ne doit pas être chiffrée, sinon je ne peux pas la lire car je n'ai pas encore la clef pour la déchiffrer. Et si elle n'est pas chiffrée, toute personne qui intercepte le message peut récupérer la clef partagée et donc intercepter mes futurs messages pour les déchiffrer.

II.2. Le chiffrement asymétrique

Définition

Le chiffrement asymétrique permet au poste destinataire de messages de générer une unique paire de clefs :

- une **clef privée** gardée secrète sur le poste destinataire des messages et stockée de manière sécurisée.
- un **clef publique** diffusée par le destinataire à tous les postes distants.

La clef publique ne peut que chiffrer le message.
La clef privée ne peut que déchiffrer le message.

Le cheminement d'un message est donc le suivant :

- création du message
- chiffrement du message par la clef publique
- envoi du message
- réception du message
- déchiffrement du message par clef privée
- lecture du message

Remarque

Un ordinateur doit connaître toutes les clefs publiques de tous les postes à qui il envoie un message.

Remarque

Si on fait une analogie avec la vie courante, on peut avoir la situation suivante :

- Le destinataire envoie à la terre entière des cadenas identiques dont lui seul à la clef.
- L'expéditeur envoie un message dans un coffre cadenassé avec le cadenas envoyé par le destinataire.
- Le destinataire reçoit le coffre cadenassé dont lui seul a la clef.

Avantages

Même si quelqu'un intercepte le message, il n'a pas la clef privée donc ne peut déchiffrer le message.

Inconvénients

On doit générer autant couple de clefs que d'expéditeur potentiels. De même, l'expéditeur doit avoir autant de clef publique que de destinataire à qui il envoie des messages.

Remarque

On peut envoyer des clefs partagée du chiffrement symétrique grâce au chiffrement asymétriques. Cela enlève l'inconvénient du chiffrement symétrique.

III. HTTPS

On rappelle que le protocole HTTP (HyperText Transfer Protocol) permet au client de faire une requête au serveur et le serveur répond à la requête.

Le problème du HTTP est la sécurité : par exemple, quelqu'un pourrait intercepter les données envoyées par un client au serveur et les lire sans problème.

C'est pourquoi la version sécurisé de HTTP a été créée. Elle s'appelle **HTTPS**(HyperText Transfer Protocol Secure). Ce protocole s'appuie sur le protocole TSL(Transport Layer Security), anciennement SSL (Secure Socket Layer).

Fonctionnement des échanges entre le client et le serveur

Les échanges vont se faire grâce à une clef symétrique.
Et pour échanger cette clef sans risque, un chiffrement asymétrique va être nécessaire.

Pour chaque nouveau client effectuant une requête, on a :

- Le client fait une requête auprès du serveur.
- Le serveur génère une clef publique ($clef\_publique\_serveur$) et une clef privée($clef\_prive\_serveur$) pour un chiffrement asymétrique. Il envoie la $clef\_publique\_serveur$ au client.
- Le client génère une clef partagée ($clef\_partage$) pour un chiffrement symétrique.
- Le client chiffre la $clef\_partage$ avec la $clef\_publique\_serveur$ et l'envoie au serveur.
- Le serveur reçoit la version chiffrée de la $clef\_partage$ du client, la déchiffre avec la $clef\_prive\_serveur$.
- Le client et le serveur sont donc en possession de la $clef\_partage$ déchiffrée. Ils peuvent dorénavant échanger des données en les chiffrant et les déchiffrant avec la $clef\_partage$.