Architectures matérielles, systèmes d'exploitation et réseaux

SÉCURISATION DES COMMUNICATIONS

Yannick CHISTEL

Lycée Dumont d'Urville - CAEN

5 mai 2021

Introduction

Communication

Les communications internet utilisent plusieurs protocoles organisés en couches.

1. La couche matérielle avec le protocole **ethernet** ou **802.11.N** ;
2. La couche internet avec le protocole **IP** qui définit les routes à suivre c'est à dire les machines du réseau qui seront utilisées ;
3. La couche transport avec le protocole **TCP** ou **UDP** qui s'occupe de garantir l'intégrité des données transmises ;
4. La couche application avec les protocoles dédiés comme **HTTP** pour le web ou **IMAP / SMTP** pour la messagerie ... qui initient la communication.

Transmission des données

Les données transmises par le protocole de la couche application sont découpées en paquets. Ces paquets sont encapsulés à chaque couche traversée ce qui signifie que chaque protocole enveloppe le paquet reçu par des données qui lui permet d'acheminer correctement les données initiales de la couche application.

Ces paquets sont envoyés au routeur se trouvant sur le réseau, puis de routeurs en routeurs jusqu'à la destination souhaitée. Chaque routeur peut inspecter les paquets et donc en connaître le contenu.

Cela est donc un vrai problème si les données sont personnelles et sensibles et nécessitent le secret comme des données bancaires, d'authentification ou de santé.

Sécuriser les communications

Principe

Comme on vient de le voir, il est nécessaire de sécuriser les communications entre la source et la destination. La sécurité des communications repose sur les 3 points suivants :

1. Comment chiffrer le contenu des communications pour qu'il ne soit lisible que par la source et la destination.
   - La cryptographie est la science qui permet de rendre incompréhensible des contenus pour tous et de les rendre compréhensibles pour certains.
   - Le chiffrement et le déchiffrement sont les procédés qui permettent de crypter des contenus.
   - La cryptanalyse est la science qui décrypte un contenu sans connaître le processus de chiffrement.
2. Comment garantir que la destination est bien celle avec laquelle on veut communiquer.
   - La destination avec laquelle on communique peut être une destination piratée ;
   - La destination doit donner des éléments qui confirment que c'est bien celle souhaitée.
3. Comment garantir les 2 points précédents avec une infrastructure **internet** reposant sur les protocoles **TCP / IP** accessible à tout le monde.
   - Le réseau internet est accessible à toute machine possédant un point d'accès (carte réseau, wifi, etc)
   - On ne va pas construire un réseau isolé pour chaque communication !

Cryptographie symétrique

Principe

Le chiffrement d'un message (contenu) utilise une **clef de chiffrement** qui doit rester secrète.
La cryptographie symétrique utilise deux fonctions :

- une fonction pour chiffrer qui prend en arguments un message et une clef de chiffrement et renvoie une chaine de caractères chiffrée.
- une fonction de déchiffrement qui prend en argument un message chiffré et la clef de chiffrement et renvoie le message déchiffré.

Le chiffrement est dit symétrique car les deux fonctions utilisent la même clef de chiffrement.
Cela implique que la source et la destination ont connaissance de la clef de chiffrement commune.
Cela soulève plusieurs problèmes :

- trouver un moyen pour la source de communiquer secrètement la clef au destinataire
- utiliser différentes clefs pour éviter le piratage en cas d'interception de la clef par un tiers

À travers l'histoire, l'évolution de l'informatique et la vulnérabilité des chiffrements, différents systèmes de chiffrement ont été utilisés :

1. le chiffrement de César dont la clef est un décalage constant des lettres de l'alphabet ;
2. le chiffrement affine qui étend le chiffrement de César en utilisant une fonction affine pour le décalage des lettres ;
3. le chiffrement de Vigenère qui repose aussi sur le chiffrement de César mais avec une clef constituée de plusieurs lettres ;

Cryptographie asymétrique

Principe

Le principal défaut du chiffrement symétrique réside dans la transmission ou la mise en commun de la clef de chiffrement, ce qui le rend vulnérable.
Pour résoudre ce problème, différentes techniques ont été développées. Ces techniques proposent un chiffrement **asymétrique** utilisant une paire de clefs, l'une publique et l'autre privée.

Deux méthodes

Deux méthodes sont très utilisées aujourd'hui :

1. La première est la méthode de Diffie-Hellmann développée en 1976 par les cryptologues américains Bailey W. Diffie et Martin Hellman.
2. La seconde méthode est le système RSA. Son nom est formé des initiales de ses inventeurs : Ron Rivest, Adi Shamir et Len Adleman

Méthode de Diffie-Hellman

Principe

La méthode consiste a créé une clef commune pour un chiffrement symétrique avec 2 clefs privées, celle de la source et l'autre de la destination. Cette clef est créée avec une fonction mathématique qui vérifie les propriétés suivantes :

Soit M cette fonction, x la clef publique, y la clef privée de la source et z la clef privée de la destination :

1. Si on connaît la valeur $M(x, y)$ et la valeur de la clef publique x, alors il est très difficile de trouver la valeur y autrement qu'en testant toutes les valeurs possibles de y ;
2. Pour toutes valeurs de clefs x, y et z possibles, on a $M(M(x, y), z) = M(M(x, z), y)$ qui sera la clef commune pour un chiffrement symétrique.

Le protocole d'échange de clef se fait en 4 étapes :

- **Étape 1 :** La source calcule la valeur $M(x, y)$ avec sa clef privée y et la clef publique x et l'envoie à la destination ;
- **Étape 2 :** la destination calcule la valeur $M(x, z)$ avec sa clef privée z et la clef publique x et l'envoie à la source ;
- **Étape 3 :** la source calcule la valeur $M(M(x, z), y)$ avec sa clef privée et la valeur envoyée par la destination ;
  la destination calcule la valeur $M(M(x, y), z)$ avec sa clef privée et la valeur reçue par la source.
- **Étape 4 :** la source et la destination disposent de la même valeur de clef puisque $M(M(x, y), z) = M(M(x, z), y)$ donc les échanges peuvent être chiffrés et déchiffrés avec

Méthode de Diffie-Hellman

Principe

Cette méthode peut se transposer au mélange de couleur. La source et la destination choisissent une couleur commune : un violet La source choisit sa couleur secrète : un bleu ; La destination choisit se couleur secrète : un vert ; La source mélange sa couleur bleue avec la couleur violette et obtient une couleur orange ; La destination mélange son vert et le violet et obtient un jaune moutarde La source mélange le jaune moutarde et son bleu et obtient un violet proche du prune La destination mélage son vert avec le orange de la source et obtient la même couleur prune

1. Dans une représentation de la matrice d'adjacence, les valeurs de la matrice peuvent être réunies dans une liste Python ;
2. Dans un dictionnaire d'adjacence, les clefs seront les sommets du graphe et les sommets adjacents seront rassemblés dans un ensemble de type **set** en Python.