

La sécurité des communications

L'objectif de ce cours est de comprendre comment on peut assurer la sécurité d'une communication réseau.

Introduction

Dans un monde où la quantité d'information circulant sur les réseaux explose, le besoin de sécuriser ces communications devient prépondérant.

Trouvez des exemples concrets illustrant ce besoin de sécurité.

Un site Internet de e-commerce, les filiales d'une entreprise qui échangent des données sensibles...

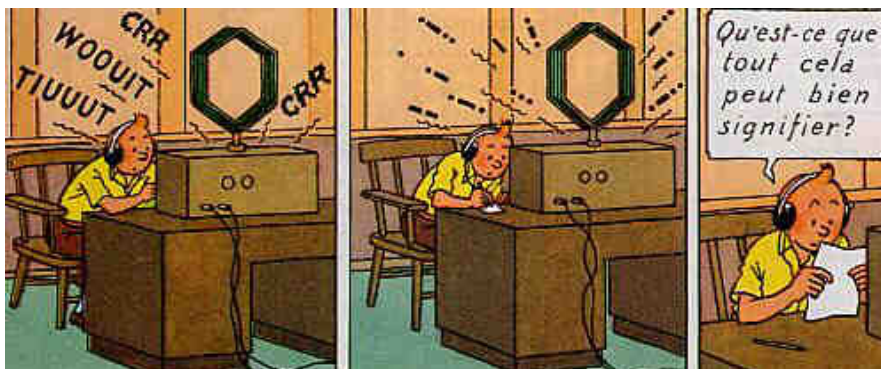
Pour qu'on puisse affirmer qu'une communication est sécurisée, plusieurs conditions doivent être réunies :

- **Confidentialité** : personne d'autre ne peut lire le contenu du message.
- **Authentification** : l'identité des acteurs (envoyeur et receveur) est garantie.
- **Intégrité** : le contenu des message n'est pas modifié pendant l'échange.

Notre objectif est d'étudier comment on peut obtenir ces trois conditions.

La cryptographie

Depuis des siècles, les hommes ont cherché à échanger entre eux des messages sécurisés. Ce besoin s'est exprimé dans de nombreux domaines, depuis les communications militaires jusqu'aux échanges amoureux secrets.



Copyright © Hergé / Moulinsart

La science qui s'intéresse aux moyens de protéger les messages est la **cryptographie**. Ses origines remontent à l'Antiquité, mais elle continue d'évoluer de nos jours. Elle se base sur l'utilisation de différentes techniques de cryptage (ou **chiffrement**) qui transforment le message en clair en un message incompréhensible, sauf bien sûr pour son destinataire.

De son invention jusqu'à aujourd'hui, la cryptographie est une lutte permanente entre deux camps:

- Les inventeurs de méthodes de chiffrement.
- Ceux qui tentent de décrypter les messages échangés en "cassant" ces méthodes.

Quelles sont les motivations des "casseurs" ?

Elles peuvent être criminelles, scientifiques, militaires ou encore ludiques.

La cryptographie constitue la base théorique de tous les mécanismes de sécurisation des échanges de données électroniques: transactions en ligne, protection des DVD...

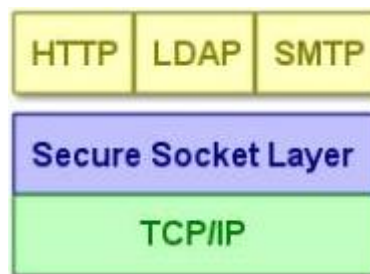
Il existe deux méthodes pour chiffrer un message :

- Le chiffrement **symétrique**, qui repose sur une clé **secrète**.
- Le chiffrement **asymétrique**, qui repose sur une paire de clés, l'une **publique** et l'autre **privée**.

Les applications de la cryptographie

Sécurisation des transactions en ligne

Le protocole de sécurisation des transactions électroniques le plus utilisé se nomme **SSL** (*Secure Socket Layer*). Il a été normalisé sous le nom de **TLS** (*Transport Layer Security*). Il forme une couche intermédiaire entre TCP/IP et les protocoles applicatifs.



Le port **443** est réservé pour le trafic HTTP sur SSL (HTTPS).

Sécurisation des connexions à une machine distante

Les protocoles de connexion sur une machine distante comme **telnet** ou **rlogin** ont été à l'origine de nombreuses failles de sécurité. De plus, ils transmettent les informations échangées (en particulier les mots de passe) en "clair".

Le protocole **SSH** a été développé pour les remplacer. Il permet de se connecter à une machine distante en mode console de manière similaire aux protocoles précédents. Cependant, un échange de clés de chiffrement a lieu au début de l'échange, puis les données sont cryptées en utilisant ces clés.

SSH utilise le port **22** par défaut. Il existe des versions du protocole pour tous les principaux systèmes d'exploitation.



Sécurisation des échanges inter-réseaux

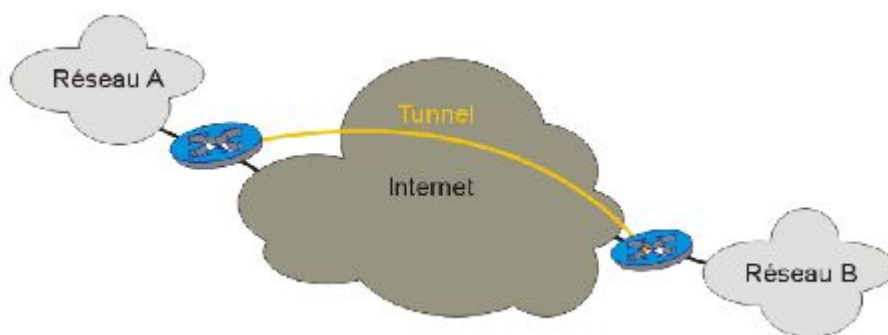
De nombreux organismes souhaitent interconnecter leurs sites distants de manière sécurisée. Pour cela, deux solutions existent:

- Louer des lignes spécialisées entre chaque site.
- Utiliser les infrastructures publiques de l'Internet.

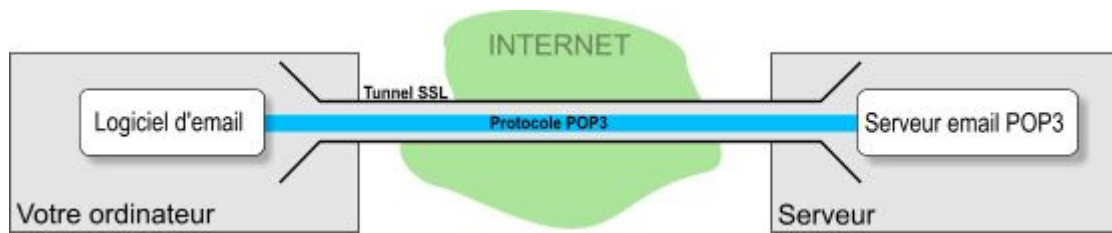
	Avantages	Inconvénients
Ligne spécialisée	- Fiabilité - Sécurité des données garantie	- Coût élevé - Complexité
Internet	- Coût faible - Infrastructures existantes	- Sécurité des données non garantie

Les réseaux privés virtuels (**RPV** ou **VPN**, **Virtual Private Network**) ont été conçus pour sécuriser les échanges de données. Il est dit virtuel parce qu'il n'a pas d'existence physique réelle (il se superpose à un réseau existant). Un VPN peut être assimilé à une ligne spécialisée virtuelle.

Un VPN fonctionne selon le principe du *tunnel*: les données des utilisateurs transitent sous forme chiffrée sur le réseau public, ce qui les rend illisibles entre les deux extrémités du VPN. On trouve sur le marché un grand nombre de solutions VPN, matérielles (routeurs) ou logicielles.



Il existe plusieurs protocoles VPN : **PPTP, L2TP, IPSec, MPLS** ... Tous utilisent des algorithmes cryptographiques pour chiffrer les données échangées.



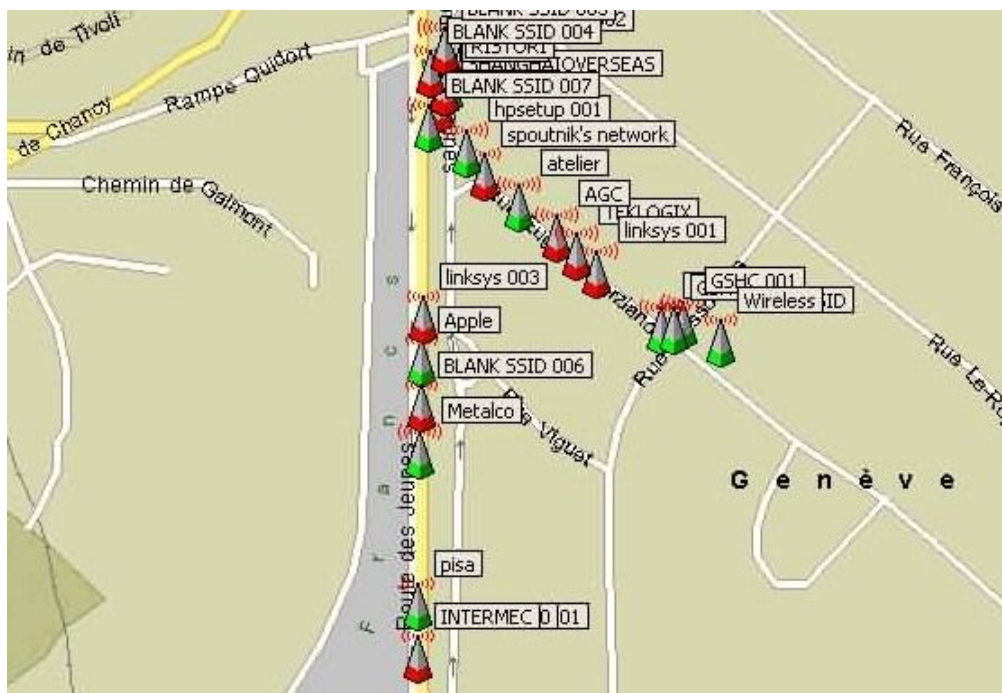
Sécurisation des réseaux sans fil

Le nombre de réseaux sans fil déployés a explosé au cours des dernières années. Leur nature même rend leur sécurisation problématique.

Pourquoi un réseau sans fil est-il plus difficile à sécuriser qu'un réseau filaire ?

**Les ondes se propagent dans toutes les directions.
Si la communication n'est pas chiffrée, le simple
fait d'être à portée de réception permet de l'écouter.**

La norme Wifi (**802.11**) est devenue le standard en matière de réseaux locaux sans fil (ou WLAN, *Wireless LAN*). Sans mécanisme de sécurité, un réseau Wifi est facile à détecter et à écouter. La pratique qui consiste à parcourir les voies publiques à la recherche de réseaux sans fil vulnérables s'appelle le *wardriving*.



Même pour une utilisation personnelle de son réseau, il est donc indispensable de mettre en place des mécanismes de sécurisation.

Citez les mesures possibles pour sécuriser un WLAN.

- Placer judicieusement les points d'accès.
- Modifier les paramètres par défaut (SSID, mot de passe administrateur...).
- Masquer le SSID.
- Filtrer les adresses MAC.
- Utiliser un protocole de cryptage.

Le protocole de cryptage **WEP** (*Wired Equivalent Privacy*) a été conçu à l'origine pour donner à un réseau Wifi le même niveau de sécurité que celui d'un réseau sans fil. Il utilise des clés secrètes de 40 ou 128 bits pour chiffrer les communications. Même s'il constitue un premier niveau de protection, son niveau de sécurité est maintenant **insuffisant** face à l'apuiissance de calcul des machines actuelles. Aussi, il convient d'utiliser si possible son successeur, **WPA** (*Wifi Protected Access*).