Haute école d'ingénierie et d'architecture Fribourg
Hochschule für Technik und Architektur Freiburg

Hes·so

Téléinformatique – Ch. 14

Telnet / SSH

Vincente Magnin
vincent.magnin@hefr.ch

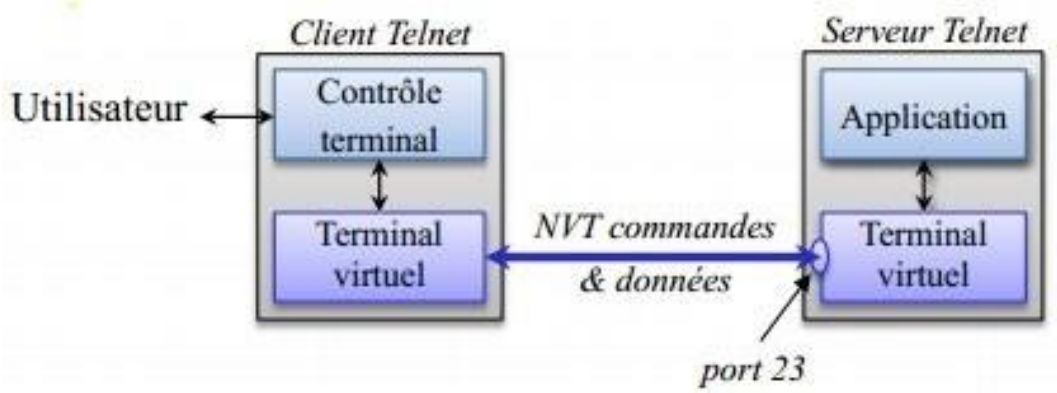
Objectifs

- Comprendre l'utilité ainsi que le fonctionnement général de Telnet.
- Comprendre l'utilité ainsi que le fonctionnement général de SSH.

Protocole Telnet

Le protocole Telnet se situe à la couche 7 du modèle OSI (*applicative layer*) et utilise le port 23/TCP. C'est un protocole qui utilise le modèle C/S et qui envoie ses données au format texte.

L'objectif principal du protocole est d'émuler un terminal à distance (terminal virtuel). Telnet est un protocole relativement ancien qui n'est pas sécurisé : les données sont envoyées en clair sur le réseau.



Protocole Telnet (2)

Le protocole Telnet comporte une commande principale « telnet » qui permet de créer des sessions Telnet.

Cette commande permet de configurer la session, en précisant par exemple le port, le protocole à utiliser... Il est donc possible de l'utiliser pour de nombreux protocoles tels que SMTP, HTTP, SNMP...

On peut par exemple regarder le film Star Wars IV en ASCII, via une session Telnet :

```
telnet towel.blinkenlights.nl
```

Protocole SSH

Le protocole SSH (Secure Shell) est situé sur la couche 7, et utilise le port 22/TCP. Il permet un accès à distance sécurisé d'un hôte à un autre.

Pour sécuriser la connexion, SSH utilise les méthodes suivantes :

- Chiffrement de la session.
- Méthode d'authentification simple.
- Supporte différentes formes de chiffrement et d'authentifications.

Aujourd'hui SSH est l'un des protocoles les plus utilisés pour se connecter à distance à des machines. C'est ce protocole que vous avez utilisé dans le laboratoire Linux.

Protocole SSH (2)

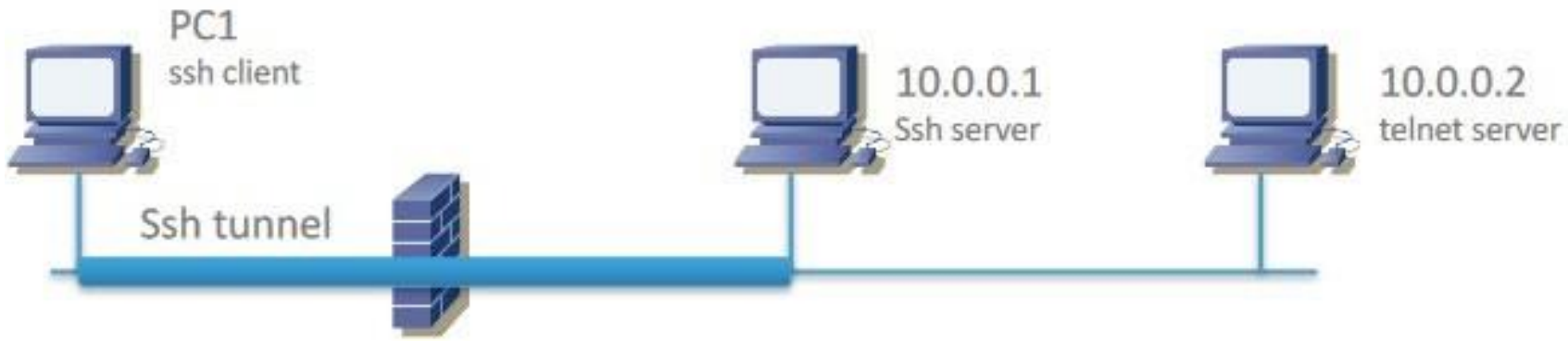
De la même manière que Telnet, SSH permet d'émuler un terminal virtuel sur un hôte distant. C'est une connexion à distance.

Le transfert de fichier est sécurisé, en utilisant la base de 2 protocoles :

- SCP (Secure Copy → scp <file> <user>@<IP>:[path])
- SFTP (Secure File Transfer Protocol)

SSH peut également servir à d'autres protocoles pour augmenter leur sécurité.

Protocole SSH (3)



Dans cette situation, le pare-feu empêche le PC1 d'accéder au serveur Telnet de la machine 10.0.0.2 car c'est une faille de sécurité. En revanche, le PC1 peut accéder en SSH au serveur 10.0.0.1.

Il est donc tout à fait possible que PC1 se connecte en SSH à la machine 10.0.0.1, puis lancer une session Telnet depuis 10.0.0.1 vers 10.0.0.2.

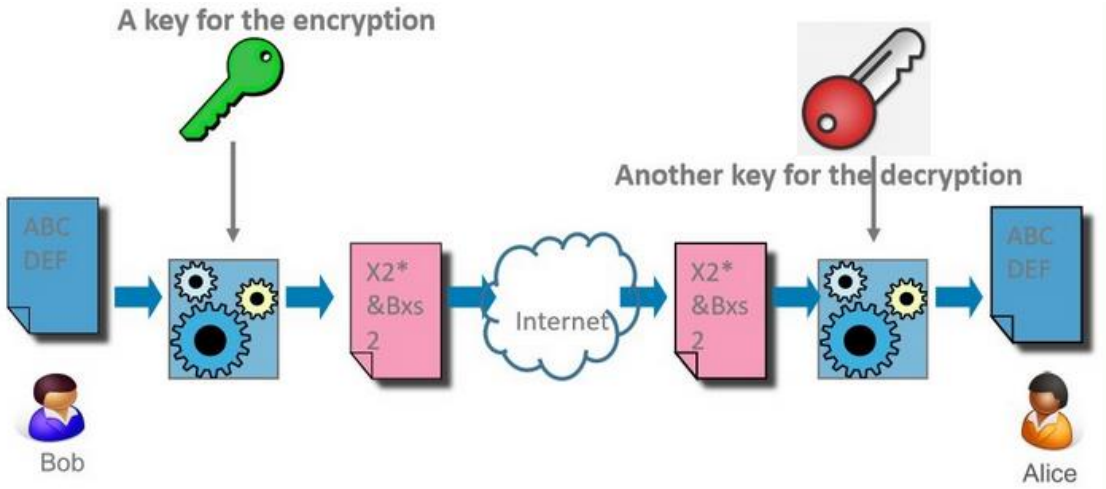
Protocole SSH (4)

Le protocole SSH permet l'authentification par 2 méthodes principales :

- Authentification par mot de passe.
- Authentification par paire de clés asymétriques.

Une paire de clés asymétriques comporte 2 clés :

- Une clé publique, qui est accessible à tous et qui n'est pas secrète.
- Une clé privée, qui doit rester secrète et qui appartient à une personne.



Protocole SSH (5)

Les paires de clés asymétriques peuvent être utilisées dans 2 cas :

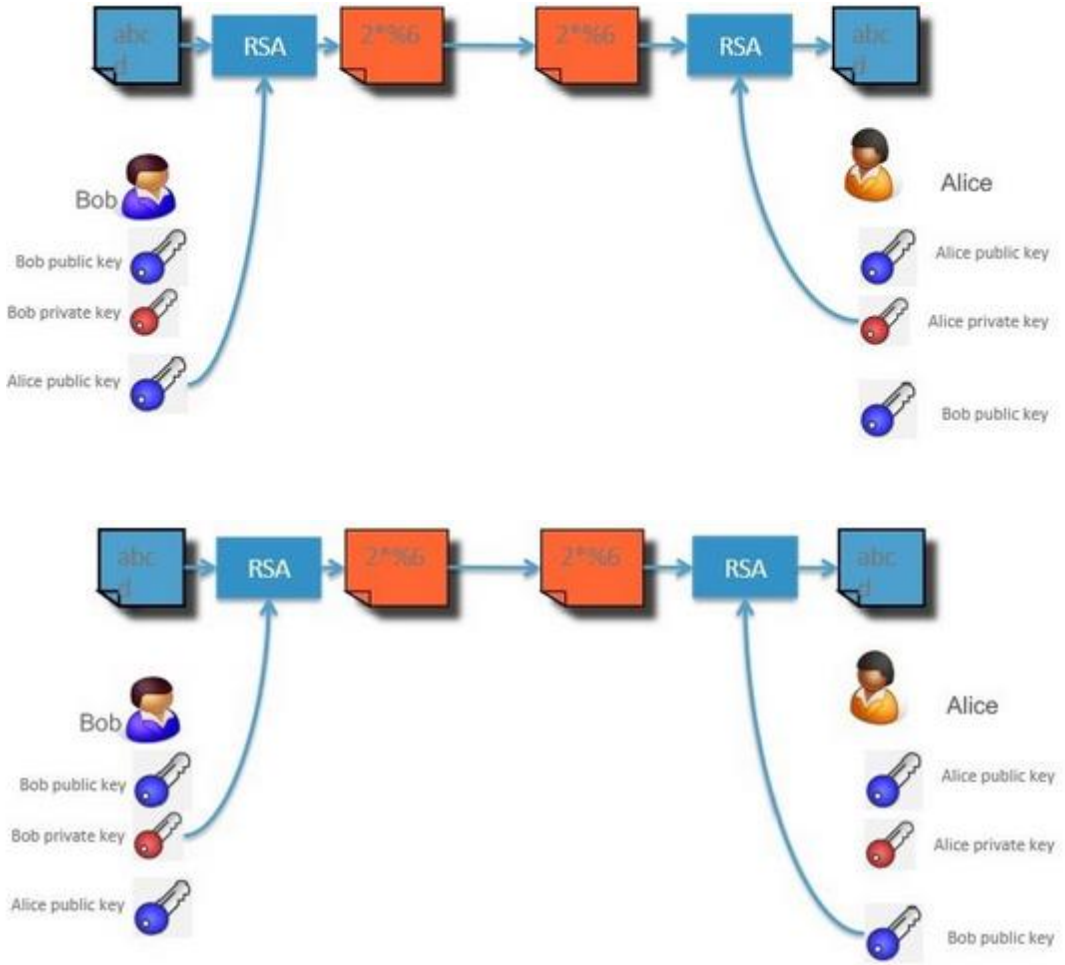
1. Pour assurer la confidentialité et l'intégrité d'un fichier.
2. Pour assurer l'authenticité et l'intégrité d'un fichier.

Dans le 1er cas, on chiffre le fichier avec la clé publique. Seule la personne avec la clé privée pourra le déchiffrer.

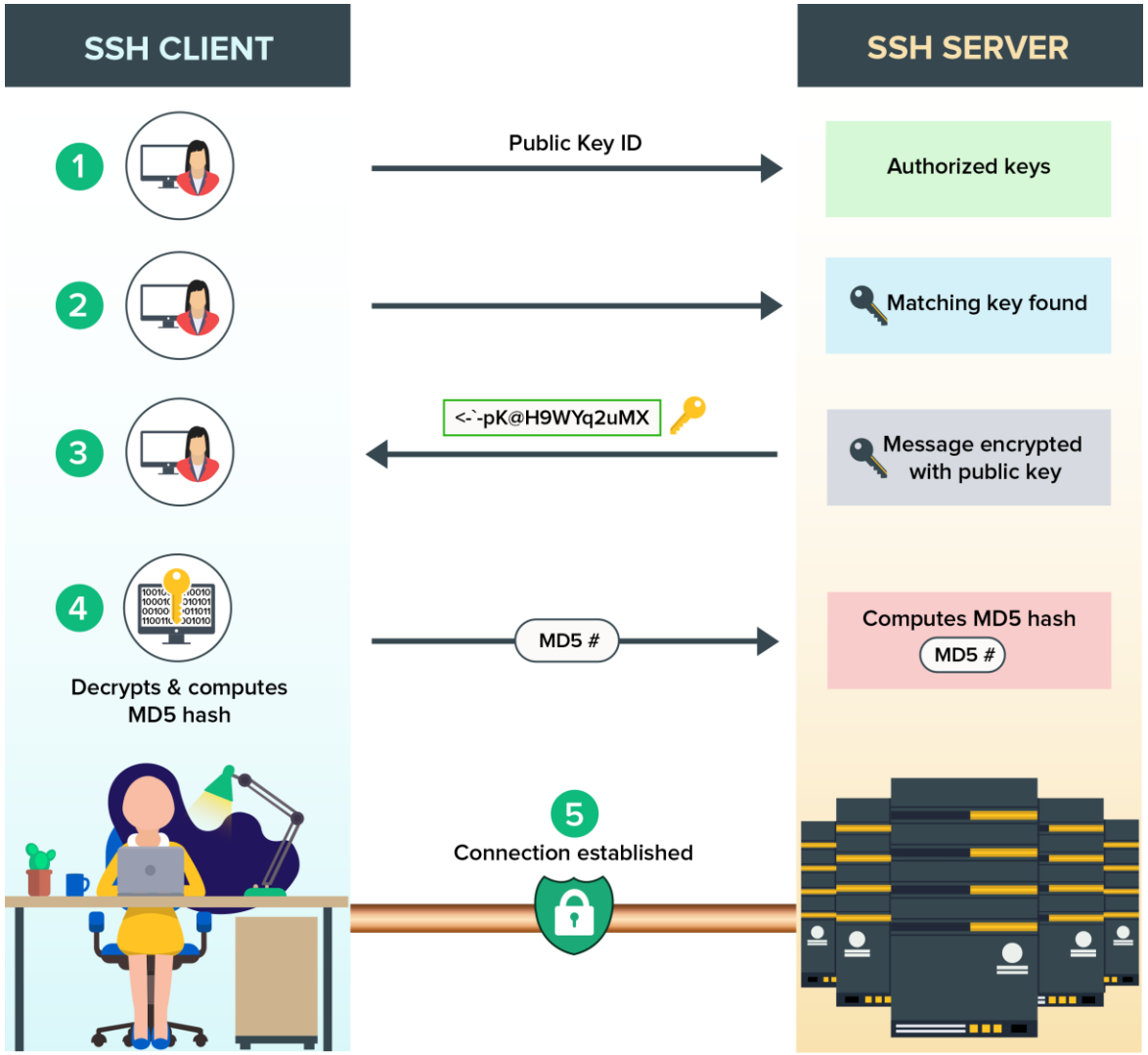
Dans le 2ème cas, on chiffre avec la clé privée, et toutes les personnes avec la clé publique pourront le déchiffrer. On aura la certitude que le fichier a bien été chiffré par la personne possédant la clé privée.

Dans les 2 cas, il est fondamental que la clé privée ne soit pas divulguée.

Protocole SSH (6)



Protocole SSH (7)



Références

- Ancien cours « Téléinformatique » (G. Waeber, S. Paccard, Q. Vaucher, N. Wirth).
- Ancien cours « Téléinformatique » (M. Roch-Neirey).