Programme et Protocole SSH

Secure Shell

2016–2017

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Présentation réalisée dans le cadre du module HLIN408
(TCCP)

UNIVERSITÉ
DE MONTPELLIER

Sommaire

Programme et Protocole SSH

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Présentation réalisée dans le cadre du module HLIN408 (TCCP)

Introduction
Se connecter à une console à distance, pourquoi ?

Rahli Mohammed Ramzi
Nguyen Hoai Nam

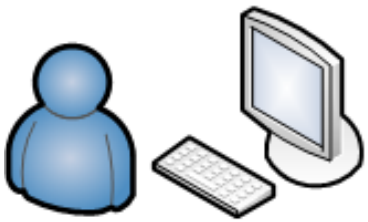
Pourquoi a-t-on besoin de se connecter à une console à distance ?

Introduction

Se connecter à une console à distance, pourquoi ?

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Pourquoi a-t-on besoin de se connecter à une console à distance ?



Machine de la fac

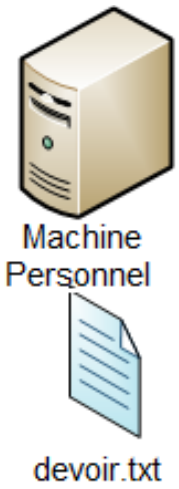
Introduction

Se connecter à une console à distance, pourquoi ?

Rahli Mohammed
Ramzi
Nguyen Hoai Nam

Pourquoi a-t-on besoin de se connecter à une console à distance ?

Machine
de la fac

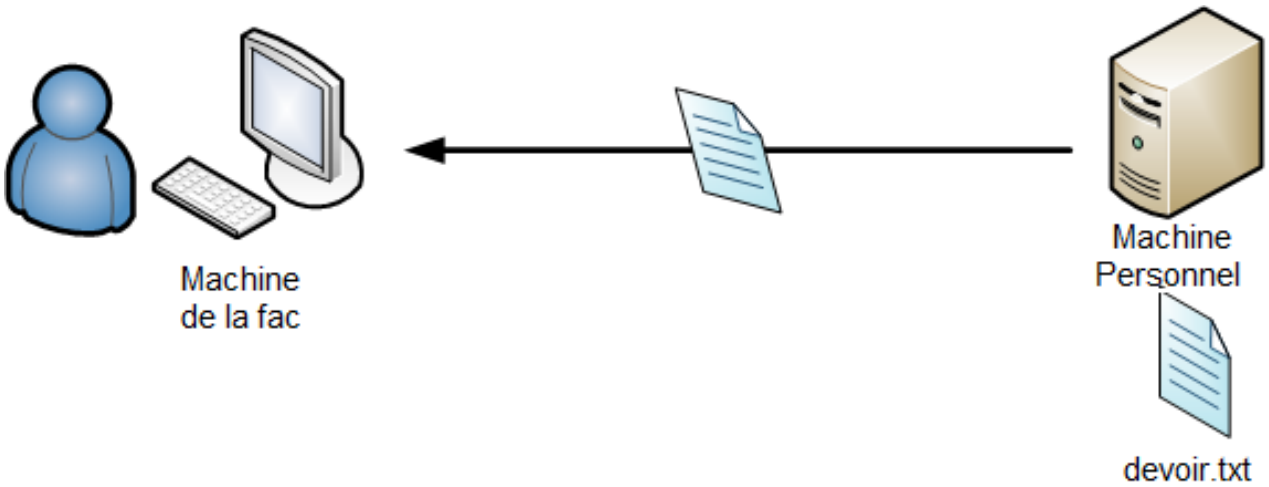


Introduction

Se connecter à une console à distance, pourquoi ?

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Pourquoi a-t-on besoin de se connecter à une console à distance ?



Rahli Mohammed Ramzi
Nguyen Hoai Nam

Qu'est ce qu'un Telnet

- Protocole qui permet d'accéder à distance à une machine.

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Qu'est ce qu'un Telnet

- Protocole qui permet d'accéder à distance à une machine.
- Créé en 1969.

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Qu'est ce qu'un Telnet

- Protocole qui permet d'accéder à distance à une machine.
- Créé en 1969.
- La connexion n'est pas sécurisée : le mot de passe et les données sont transférés en clair (Aucun chiffrement)

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Qu'est ce qu'un Telnet

- Protocole qui permet d'accéder à distance à une machine.
- Créé en 1969.
- La connexion n'est pas sécurisée : le mot de passe et les données sont transférés en clair (Aucun chiffrement)

  $\Rightarrow$ conseillé de ne pas utiliser Telnet (Dangereux).

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Qu’est ce qu’un SSH

- SSH signifie Secure SHell.

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Qu’est ce qu’un SSH

- SSH signifie Secure SHell.
- Créé en 1995.

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Qu’est ce qu’un SSH

- SSH signifie Secure SHell.
- Créé en 1995.
- Est à la fois un programme informatique et un protocole de communication sécurisé .

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Qu’est ce qu’un SSH

- SSH signifie Secure SHell.
- Créé en 1995.
- Est à la fois un programme informatique et un protocole de communication sécurisé .
- Permet de faire des connexions sécurisées entre un serveur et un client .

Programme et Protocole SSH
Rahli Mohammed Ramzi
Nguyen Hoai Nam

Qu’est ce qu’un SSH

- SSH signifie Secure SHell.
- Créé en 1995.
- Est à la fois un programme informatique et un protocole de communication sécurisé .
- Permet de faire des connexions sécurisées entre un serveur et un client .
- Impose un échange de clés de chiffrement en début de connexion.

Système de chiffrement SSH

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Il y a 3 méthodes de chiffrement

- Chiffrement Symétrique

Système de chiffrement SSH

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Il y a 3 méthodes de chiffrement

- Chiffrement Symétrique
- Chiffrement Asymétrique

Système de chiffrement SSH

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Il y a 3 méthodes de chiffrement

- Chiffrement Symétrique
- Chiffrement Asymétrique
- Combinaison des chiffrements symétrique et asymétrique

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Chiffrement Symétrique

- C’est la méthode de chiffrement la plus simple.

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Chiffrement Symétrique

- C’est la méthode de chiffrement la plus simple.
- Utilise une seule clé pour chiffrer et déchiffrer.

Programme et Protocole SSH
Rahli Mohammed Ramzi
Nguyen Hoai Nam

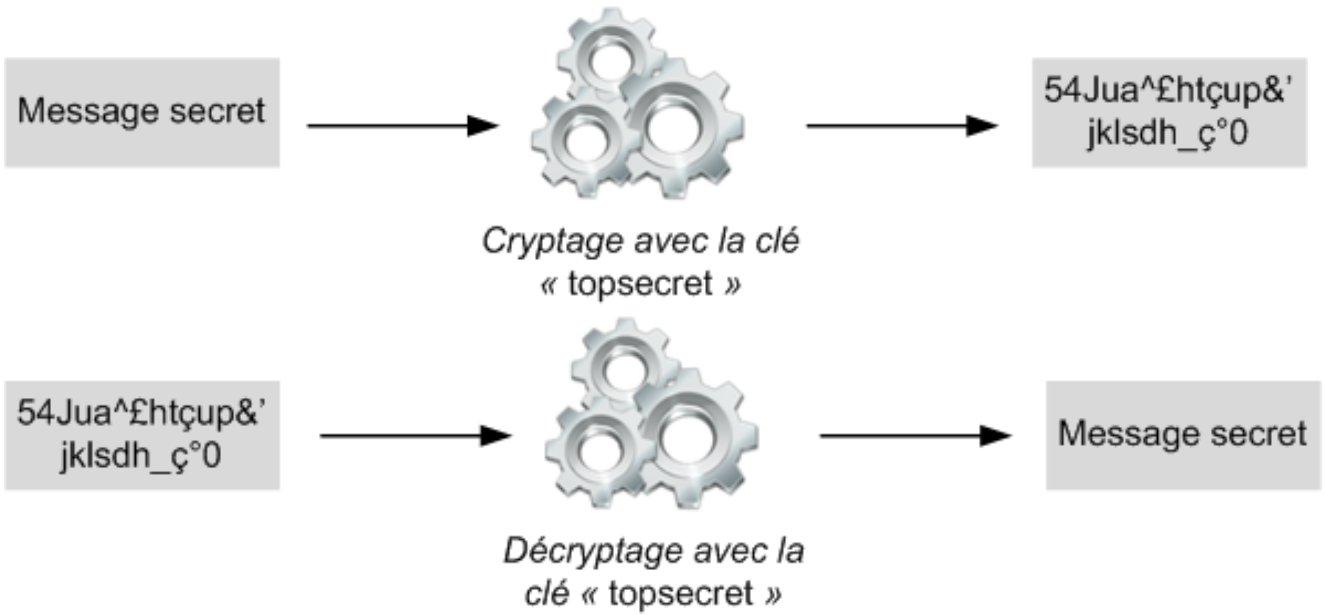
Chiffrement Symétrique

- C'est la méthode de chiffrement la plus simple.
- Utilise une seule clé pour chiffrer et déchiffrer.

Rahli Mohammed
Ramzi
Nguyen Hoai Nam

Chiffrement Symétrique

- C'est la méthode de chiffrement la plus simple.
- Utilise une seule clé pour chiffrer et déchiffrer.



Rahli Mohammed Ramzi
Nguyen Hoai Nam

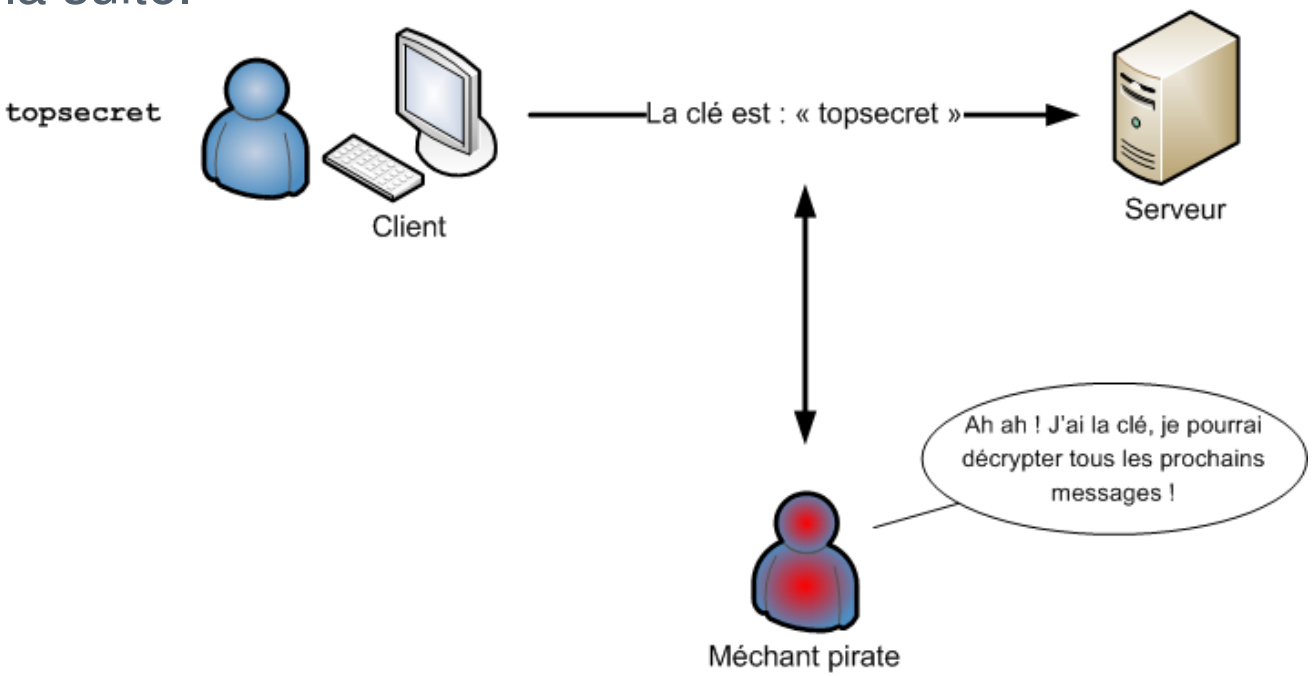
Chiffrement Symétrique

- Désavantage : il faut envoyer la clé secrète de façon publique et donc si quelqu'un connait la clé, cette personne peut déchiffrer tous les messages envoyés par la suite.

Programme et Protocole SSH
Rahli Mohammed Ramzi
Nguyen Hoai Nam

Chiffrement Symétrique

- Désavantage : il faut envoyer la clé secrète de façon publique et donc si quelqu'un connait la clé, cette personne peut déchiffrer tous les messages envoyés par la suite.



Rahli Mohammed Ramzi
Nguyen Hoai Nam

Chiffrement Asymétrique

- Le chiffrement asymétrique utilise une clé pour chiffrer, et une autre pour déchiffrer.

Rahli Mohammed
Ramzi
Nguyen Hoai Nam

Chiffrement Asymétrique

- Le chiffrement asymétrique utilise une clé pour chiffrer, et une autre pour déchiffrer.
- La clé dite « publique » qui ne sert qu'à chiffrer ;

Rahli Mohammed
Ramzi
Nguyen Hoai Nam

Chiffrement Asymétrique

- Le chiffrement asymétrique utilise une clé pour chiffrer, et une autre pour déchiffrer.
- La clé dite « publique » qui ne sert qu'à chiffrer ;

- La clé dite « privée » qui ne sert qu'à déchiffrer.

Programme et Protocole SSH
Rahli Mohammed
Ramzi
Nguyen Hoai Nam

Chiffrement Asymétrique

- Le chiffrement asymétrique utilise une clé pour chiffrer, et une autre pour déchiffrer.
- La clé dite « publique » qui ne sert qu'à chiffrer ;

- La clé dite « privée » qui ne sert qu'à déchiffrer.
- Pour déchiffrer, la clé publique ne fonctionne pas. Il faut obligatoirement utiliser la clé privée.

Système de chiffrement SSH

Chiffrement Asymétrique II

Programme et
Protocole
SSH

Rahli Mohammed
Ramzi
Nguyen Hoai Nam

Système de chiffrement SSH
Chiffrement Asymétrique III

Rahli Mohammed Ramzi
Nguyen Hoai Nam

- La clé publique peut être transmise en clair sur le réseau (elle est « publique »). Ce n'est pas grave si un pirate l'intercepte. En revanche, la clé privée — qui permet donc de déchiffrer — doit rester secrète.

Système de chiffrement SSH
Chiffrement Asymétrique III

Rahli Mohammed Ramzi
Nguyen Hoai Nam

- La clé publique peut être transmise en clair sur le réseau (elle est « publique »). Ce n'est pas grave si un pirate l'intercepte. En revanche, la clé privée — qui permet donc de déchiffrer — doit rester secrète.
- L'algorithme de chiffrement asymétrique le plus connu s'appelle RSA.

Système de chiffrement SSH
Chiffrement Asymétrique III

Rahli Mohammed Ramzi
Nguyen Hoai Nam

- La clé publique peut être transmise en clair sur le réseau (elle est « publique »). Ce n'est pas grave si un pirate l'intercepte. En revanche, la clé privée — qui permet donc de déchiffrer — doit rester secrète.
- L'algorithme de chiffrement asymétrique le plus connu s'appelle RSA.
- Désavantage : demande beaucoup de ressources au processeur.

Programme et Protocole SSH
Rahli Mohammed Ramzi
Nguyen Hoai Nam

Combinaison des chiffrements symétrique et asymétrique

- On utilise d'abord le chiffrement asymétrique pour s'échanger discrètement une clé secrète de chiffrement symétrique.

Programme et Protocole SSH
Rahli Mohammed Ramzi
Nguyen Hoai Nam

Combinaison des chiffrements symétrique et asymétrique

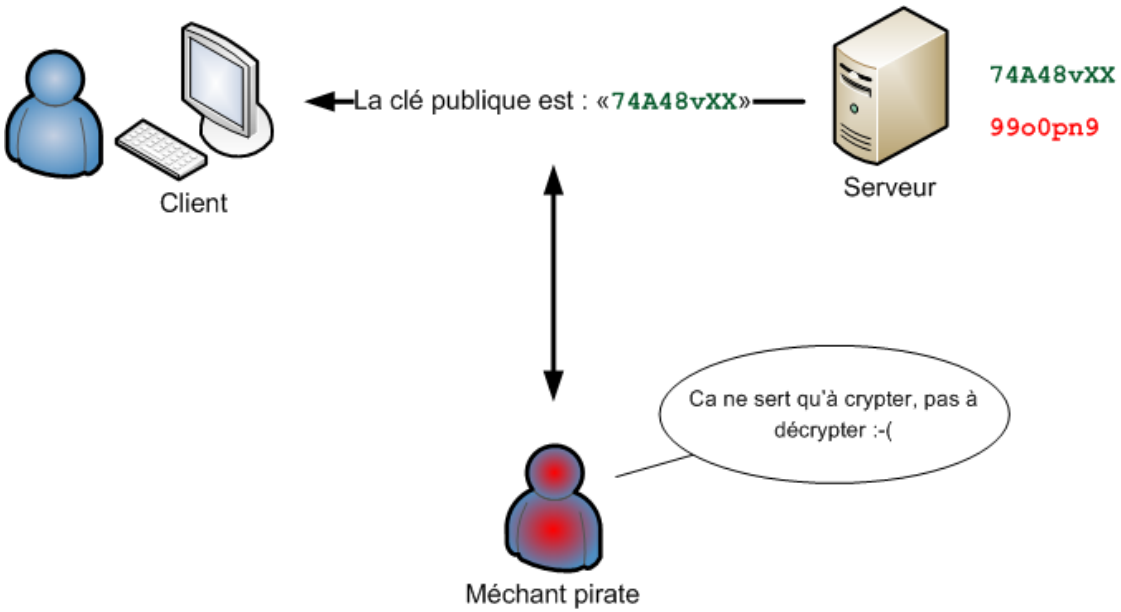
- On utilise d'abord le chiffrement asymétrique pour s'échanger discrètement une clé secrète de chiffrement symétrique.
- Ensuite, on utilise tout le temps la clé de chiffrement symétrique pour chiffrer les échanges.

Système de chiffrement SSH

Combinaison des chiffrement symétrique et asymétrique II

Programme et Protocole SSH

Rahli Mohammed
Ramzi
Nguyen Hoai Nam



- Envoi de la clé publique au client

Système de chiffrement SSH

Combinaison des chiffrement symétrique et asymétrique III

Programme et Protocole SSH

Rahli Mohammed
Ramzi
Nguyen Hoai Nam

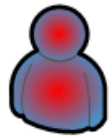
*Crypte une clé symétrique de son choix (**topsecret**) avec la clé publique « **74A48vXX** »*

Client

Serveur

74A48vXX

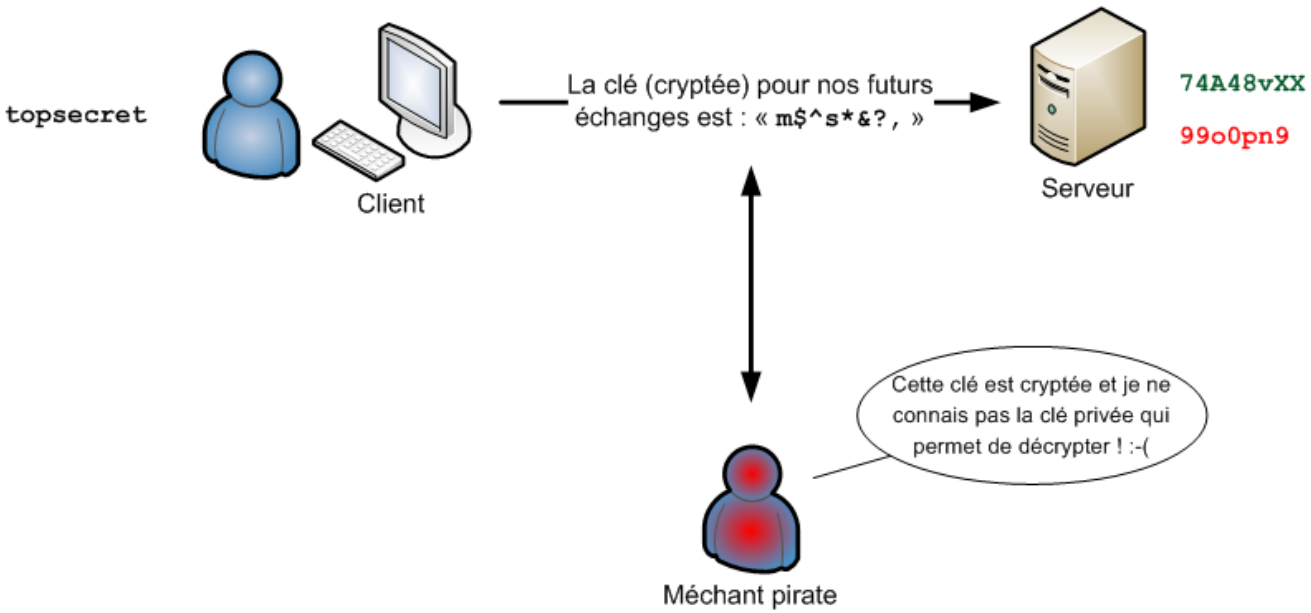
99o0pn9



Méchant pirate

-
- Création de clé symétrique et chiffrement par le client

Système de chiffrement SSH
Combinaison des chiffrement symétrique et asymétrique IV



-
- Envoi de la clé chiffrée au serveur

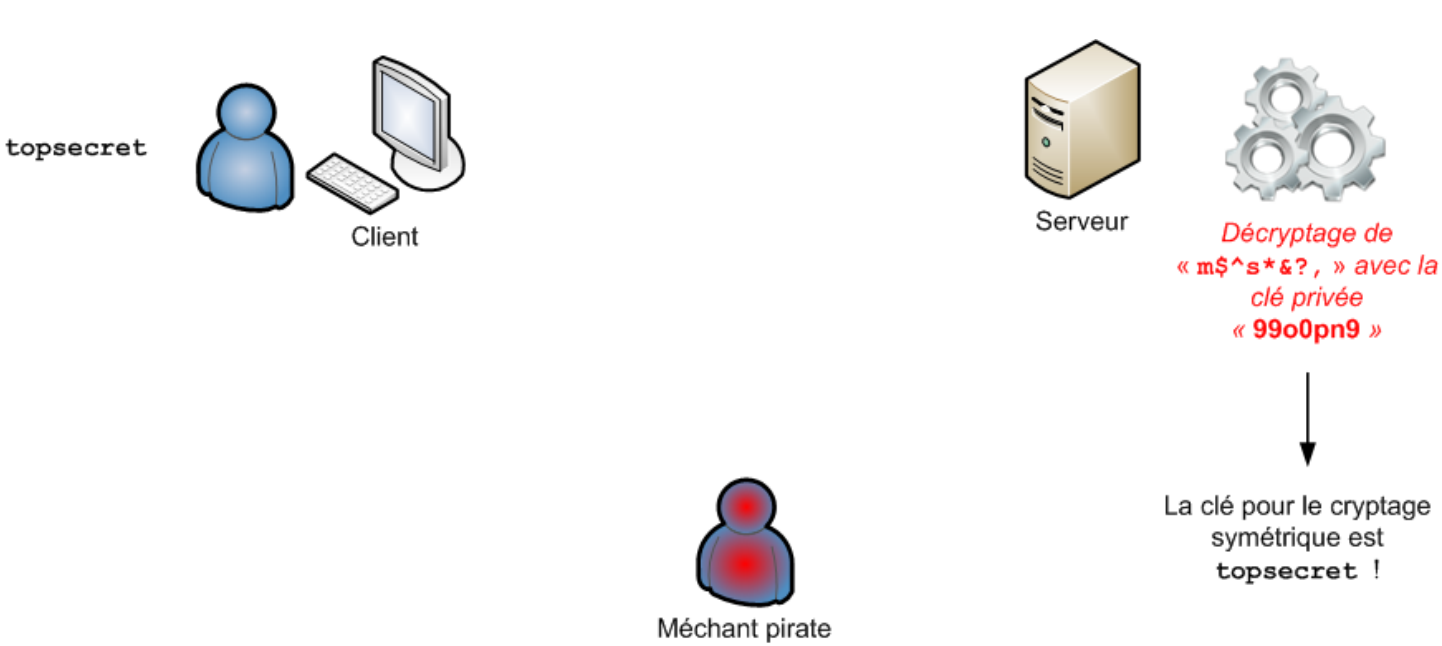
Programme et Protocole SSH

Rahli Mohammed
Ramzi
Nguyen Hoai Nam

Système de chiffrement SSH
Combinaison des chiffrement symétrique et asymétrique V

Programme et Protocole SSH

Rahli Mohammed
Ramzi
Nguyen Hoai Nam

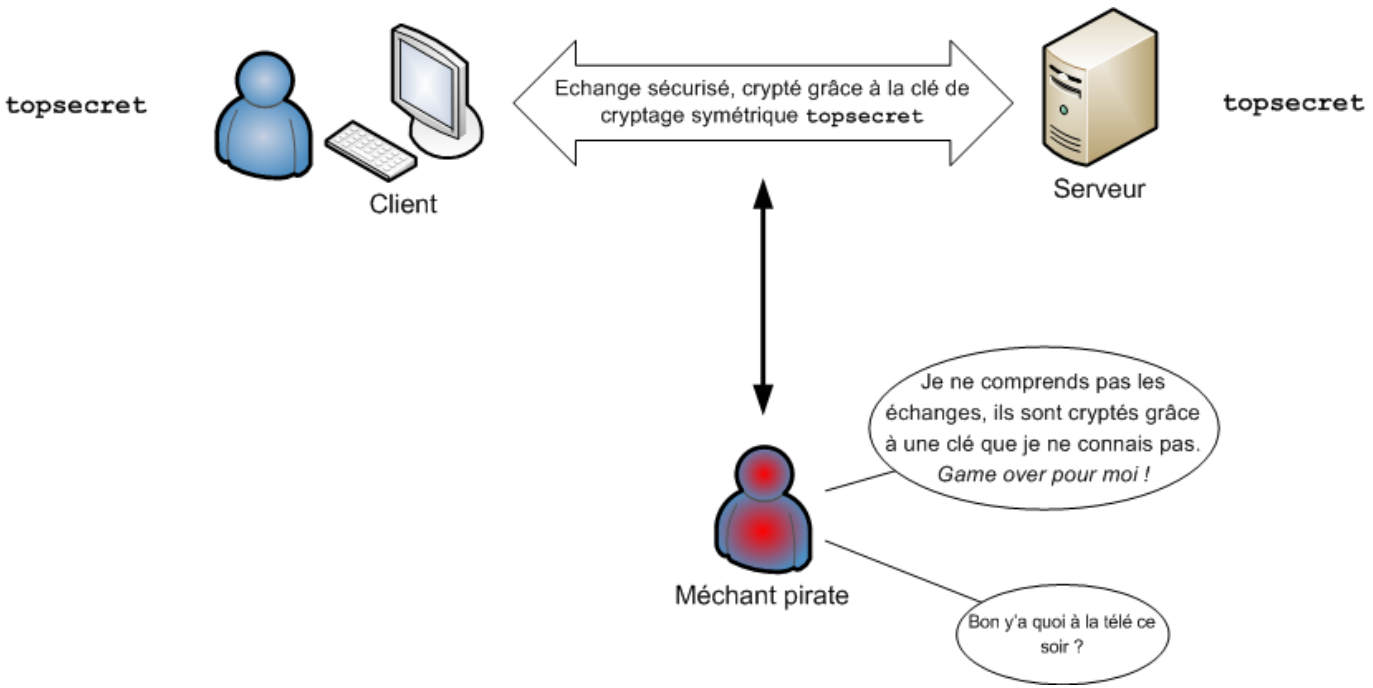
- 

- Déchiffrement de la clé par le serveur grâce à sa clé privée

Système de chiffrement SSH
Combinaison des chiffrement symétrique et asymétrique VI

Programme et Protocole SSH

Rahli Mohammed
Ramzi
Nguyen Hoai Nam



-
- Échange sécurisé établi !

Transformer sa machine en serveur

Rahli Mohammed
Ramzi
Nguyen Hoai Nam

Comment transformer sa machine en serveur ?

- Installer le paquet openssh-server :

```
mrahli@m11:$ sudo apt-get install openssh-server
~
```

```
mrahli@m11:$ Creating SSH2 RSA key; this may take some time ...
Creating SSH2 DSA key; this may take some time ...
* Restarting OpenBSD Secure Shell server sshd
~
```

- Lancer le serveur avec la commande suivante :

```
mrahli@m11:$ sudo /etc/init.d/ssh start
~
```

- Arrêter le serveur avec la commande suivante :

```
mrahli@m11:$ sudo /etc/init.d/ssh stop
~
```

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Comment se connecter via SSH à partir d'une machine Linux

- Se connecter avec la commande suivante :

```
mrahli@m11:$ ssh login@ip
~
```

- (Où login est votre login et ip est votre adresse IP (ex nnguyen@87.112.13.165).

```
mrahli@m11:$ ssh nnguyen@87.112.13.165
~
```

- Saisie du mot de passe

```
mrahli@m11:$ nnguyen@87.112.13.165 password:
~
```

Rahli Mohammed Ramzi
Nguyen Hoai Nam

L’identification automatique par clé

- L’authentification par mot de passe (ce que nous avons vu précédemment) .

L'identification automatique par clé

Rahli Mohammed Ramzi
Nguyen Hoai Nam

L'identification automatique par clé

- L'authentification par mot de passe (ce que nous avons vu précédemment) .
- L'authentification par clés publique et privée du client.

L'identification automatique par clé
L'authentification par clés publique et privée du client

Rahli Mohammed Ramzi
Nguyen Hoai Nam

L'authentification par clés publique et privée du client

- Au lieu de s'authentifier par mot de passe, les utilisateurs peuvent s'authentifier grâce à la cryptographie asymétrique et son couple de clefs privée/publique, comme le fait le serveur SSH auprès du client SSH.

Générer ses clefs

- Pour générer un couple de clefs publique/privée, tapez (sur la machine du client) :

```
mrahli@m11:$ ssh-keygen -t rsa
~
```

- Vous pouvez remplacer rsa par dsa si vous voulez utiliser l'autre algorithme de chiffrement.

L'identification automatique par clé

Générer ses clefs

Rahli Mohammed Ramzi
Nguyen Hoai Nam

```
$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/mateo21/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/mateo21/.ssh/id_rsa.
Your public key has been saved in /home/mateo21/.ssh/id_rsa.pub.
The key fingerprint is:
b7:22:94:aa:8c:fb:d3:ef:53:86:df:b9:37:40:bd:4d mateo21@mateo21-laptop
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|                 |
|          .      |
|       .  . . E  |
|      o.S..  +   |
|     o. o.... .  |
|   .. .+...o     |
| o... ....o o    |
|oo+. oo.  .o .   |
+-----------------+
```

- Le client génère une paire de clés public/privé
- La clef privée est stockée dans le fichier ∼/.ssh/id_rsa avec les permissions 600.
- La clef publique est stockée dans le fichier ∼/.ssh/id_rsa.pub avec les permissions 644.
- On vous demande une passphrase. C'est une phrase de passe qui va servir à chiffrer la clé privée pour une meilleure sécurité

Autoriser votre clef publique

- Pour cela, il suffit de copier votre clef publique dans le fichier ∼/.ssh/authorized_keys de la machine sur laquelle vous voulez vous connecter à distance. La commande suivante permet de réaliser cette opération via SSH :

```
ssh-copy-id -i id_rsa.pub login@ipServeur
```

L'identification automatique par clé
Se connecter !

Rahli Mohammed Ramzi
Nguyen Hoai Nam

Se connecter !

- La commande est la même que pour une authentification par mot de passe

```
ssh ramzi@88.92.107.7
Enter passphrase for key '/home/ramzi/.ssh/id_rsa':
```

- On vous demande la phrase de passe pour déchiffrer votre clé privée. Entrez-la.

OK, auparavant, on me demandait mon mot de passe. Maintenant, on me demande une phrase de passe pour déchiffrer la clé privée. Où est le progrès ???

- Solution : l'agent SSH.

L'identification automatique par clé
L'agent SSH

Rahli Mohammed Ramzi
Nguyen Hoai Nam

L'agent SSH

- L'agent SSH est un programme qui tourne en arrière-plan en mémoire. Il retient les clés privées pendant toute la durée de votre session.

L'identification automatique par clé
L'agent SSH

Rahli Mohammed Ramzi
Nguyen Hoai Nam

L'agent SSH

- L'agent SSH est un programme qui tourne en arrière-plan en mémoire. Il retient les clés privées pendant toute la durée de votre session.

L'intérêt :

- Il ne vous demande la passphrase qu'une seule fois au début.
- Vous pouvez vous connecter plusieurs fois sur le même serveur,sans avoir besoin de retaper votre passphrase !
- Vous pouvez vous connecter sur plusieurs serveurs différents, sans avoir besoin de retaper votre passphrase !

L'identification automatique par clé
L'agent SSH

Rahli Mohammed Ramzi
Nguyen Hoai Nam

- Tout ce que vous avez à faire est de lancer le programme ssh-add sur le PC du client :

```
ssh-add
Enter passphrase for /home/ramzi/.ssh/id_rsa :
Identity added:  /home/ramzi/.ssh/id_rsa(/home/ramzi/.ssh/id_rsa)
```

- Il va automatiquement chercher votre clé privée. Pour la déchiffrer, il vous demande la passphrase. Entrez-la.
- Maintenant que c'est fait, chaque fois que vous vous connecterez à un serveur, vous n'aurez plus besoin d'entrer la passphrase.

Transférer des fichiers
Transférer des fichiers en utilisant SCP

Rahli Mohammed
Ramzi
Nguyen Hoai Nam

Utiliser SCP

- Pour transférer le fichier test1.txt situé dans le répertoire courant vers le home du compte toto de la machine ordi1.exemple.org sur laquelle tourne un serveur SSH :

```
scp test1.txt toto@ordi1.exemple.org:
```

- Pour récupérer le fichier test2.txt situé dans le répertoire personnel de l'utilisateur toto de la machine ordi2.exemple.org et l'écrire dans le répertoire courant :

```
scp toto@ordi2.exemple.org:test2.txt .
```

- Pour récupérer tous les fichiers ayant l'extension .txt situés dans le répertoire /usr/local de la machine ordi2.exemple.org et l'écrire dans le sous-répertoire test-scp du répertoire courant :

```
scp toto@ordi2.exemple.org:'/usr/local/*.txt' test-scp
```

Transférer des fichiers

Transférer des fichiers en utilisant SCP II

Rahli Mohammed Ramzi
Nguyen Hoai Nam

- Pour transférer l'intégralité du sous-répertoire test-scp du répertoire courant vers le sous répertoire incoming du home de l'utilisateur toto de la machine ordi1.exemple.org :

```
scp -r test-scp toto@ordi1.exemple.org:incoming
```

Bibliographie

Rahli Mohammed Ramzi
Nguyen Hoai Nam

wikipedia

- https://fr.wikipedia.org/wiki/Secure_Shell

ecp

- http://formation-debian.via.ecp.fr/ssh.html

openclassrooms

- https://openclassrooms.com/courses/reprenez-le-controle-a-l-aide-de-linux

Merci pour votre attention !

UNIVERSITÉ
DE MONTPELLIER