Cours GNU/linux

Accès SSH

alan.simon@free.fr

Présentation

- Protocole de communication
  - Sécurisé :
    - Identification des hosts
    - Chiffrage de la communication
  - Sur le port tcp 22
- Historique
  - ssh V1 : 1995 - Tatu Ylönen (finlandais)
    - Logiciel propriétaire
    - cf http://www.openssh.org/specs.html
  - ssh V2 : 2006 definis comme standard internet par l'IETF
    - RFC : 4251-4254
    - OpenSSH : le plus utilisé sous licence BSD

Fonctionnalités

Connexion shell distante (telnet rlogin)

File transfert : scp sftp (ftp)

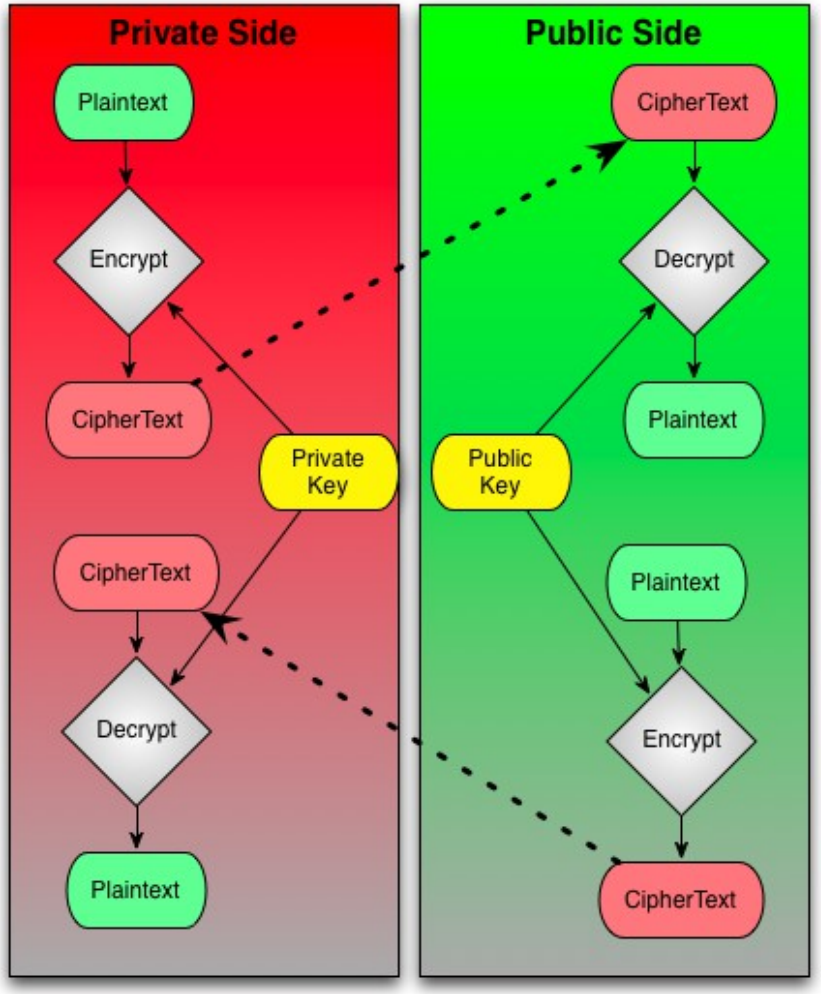
Forward de port / tunneling

Plusieurs mode d'autentification

- Password
- Clef public
- Certificat
- GSSAPI (SSO kerberos5 ou NTLM)

sshfs : parcours d'une arborescance distante comme si elle était locale (FUSE + SSH)

Chiffrement asymétrique, symétrique et hachage



Asymétrique :

- Une paire de clefs de chiffrement
- ce qui est chiffé par l'une est déchiffré par l'autre.

Symétrique

- Une seule clef partagée

Hachage

- Un algorithme de chiffrage non réversible

alan.simon@free.fr

Présentation d'un chiffrement simple

Anna dispose d'une paire de clef A_pub et A_priv

Boris dispose d'une paire de clef B_pub et B_priv

Anna et Boris connaisent un algo de hachage commun H(x)

Boris chiffre et emet

- son message chiffré avec la clef publique d'Anna : A_pub(msg)
- un hachage de son message chiffré avec sa clef privée : B_priv(H(msg))

Anna décode

- le message avec sa clef privé : A_priv(A_pub(msg))=msg
- le hachage du message signé par boris avec la clef publique de boris : B_pub(B_priv(H(msg)))

Anna vérifie

- Calcule a son tour le hachage H(msg) et le compare au hachage founis par boris

Processus de connexion

Connexion TCP

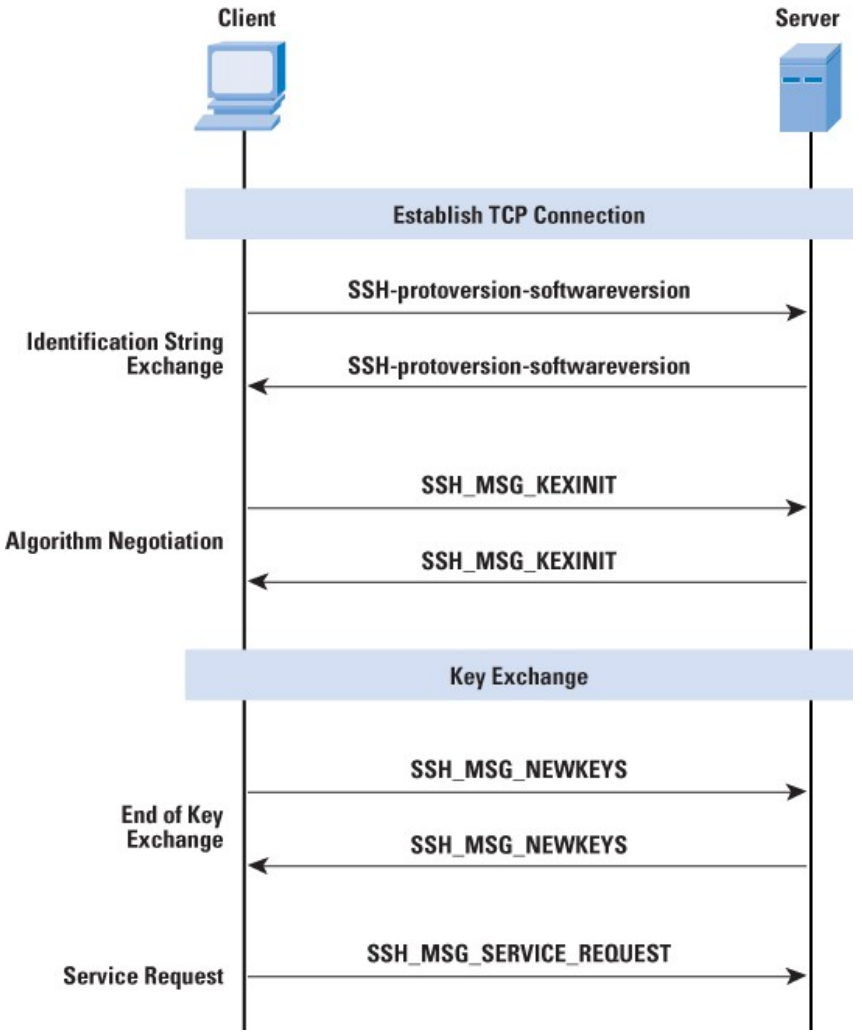
Négociation du protocole ssh

SSH_MSG_KEXINIT

- Négociation du chiffrement et Echange d'une clef partagée : K
- Identification du serveur
- Le client valide
  - Inclue dans la list des host connue de l'utilisateur
  - Demande une validation de l'utilisateur

Echange des clefs de chiffrement à partir de K

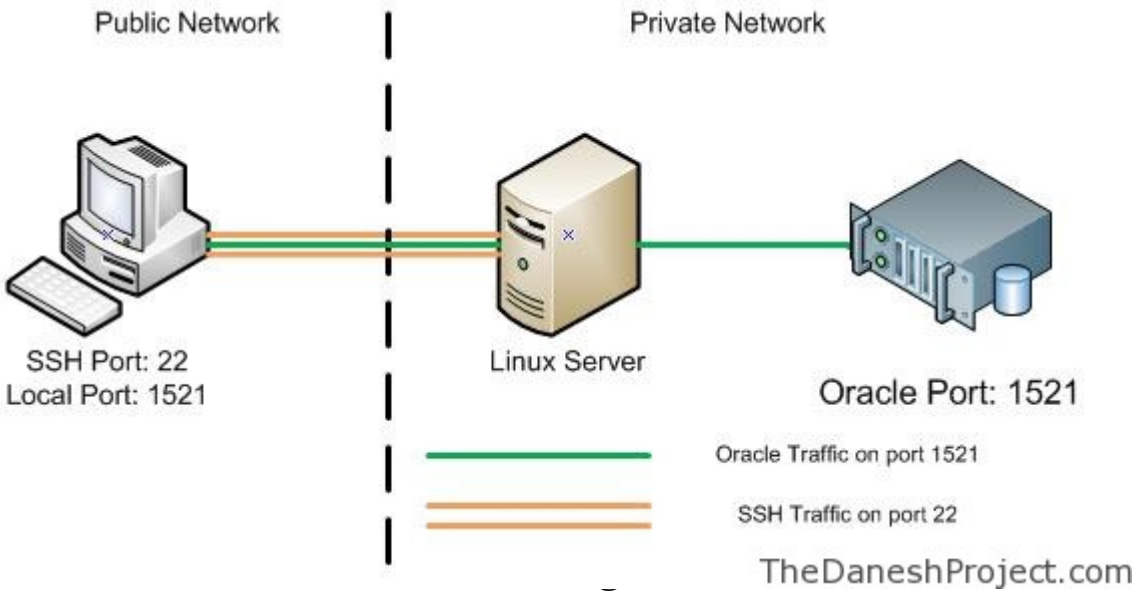
Le client demande à accèder à un service en proposant une authentification.



Port forwarding

Fontionnalité permettant de transmettre dans le flux de communication ssh d'autre flux réseaux

- Un port sur le loopbak local du host client ssh
- Un port et une ip à partir du host Serveur ssh



Fichiers importants

Configuration Serveur : /etc/ssh/sshd_config

Configuration Client : /etc/ssh/ssh_config

User known host : ~/.ssh/known_hosts

Authorized keys : ~/.ssh/authorized_keys

Configuration Serveur

Fichier de configuration : /etc/ssh/ssh**d**_config

Configuration réseau et protocole:

```
Port 22
AddressFamily any
ListenAddress 0.0.0.0
ListenAddress ::
Protocol 2
```

Configuration du service

```
PermitRootLogin yes
PubkeyAuthentication yes
AuthorizedKeysFile     .ssh/authorized_keys
AllowTcpForwarding yes
X11Forwarding yes
X11DisplayOffset 10
```

Configuration client

Fichier de configuration : /etc/ssh/ssh_config

Forwarding :

```
ForwardAgent no
ForwardX11 no
ForwardX11Trusted yes
```

Identité :

```
IdentityFile ~/.ssh/identity
IdentityFile ~/.ssh/id_rsa
IdentityFile ~/.ssh/id_dsa
```

Réseau / protocole :

```
Port 22
Protocol 2,1
```

Commandes utiles

sshkeygen : gestion de pair de clef publique/privée

ssh user@host : connection distante

ssh -L localport:distant-host:distant-port user@host

TD

Mise en place d'une relation d'approbation.

Depuis votre poste vers votre VM

- Génération d'une pair de clé publique / privée
- Déposez votre clé publique sur le compte distant dans ~/.ssh/authorized_keys
- Validation test de connexion

Présentation X11 (Xorg)

- Moteur d'interface graphique
  - Gestion des interfaces d'entrées sorties utilisateur
    - Clavier souris écran
  - Serveur X : Serveur d'interface
  - Le display manager : authantification et choix de l'interface
  - Les Clients X : applications fenètrées clientes de l'interface graphique
    - notamment le window manager
      - Gnome
      - Kde
      - XFCE

TD X11 forwarding

Installation de Xming sur votre host ou utilisation d'un host linux graphique

Installation de xauth et xclock sur votre guest

```
# apt-get install xauth xclock
```

Utilisez putty pour vous connecter avec la configuration modifiée :

- Config / SSH / X11 :
  - enable X11 forwarding
  - X display location “:0.0”

Lancez “xclock”

Tappez : “echo $DISPLAY”

Magic cookie

C'est une methode permettant de sécuriser l'accès au serveur X.

Création / mise à jour du fichier ~/.Xauthority afin d'y inserer le magic cookie via l'utilisation de xauth.

Il est possible de transfèrer l'authorisation par simple copie du fichier ~/.Xauthority dans le home de l'utilisateur à authoriser.

TP

Faire un scripte qui va déposer votre clef public sur un serveur distant pour un user distant

- Tester les arguments
- Tester l'existance de la clef local
- Si non existante la générer (vérifier la génération)
- Ajouter la clef publique sur le serveur distant