Secure Shell

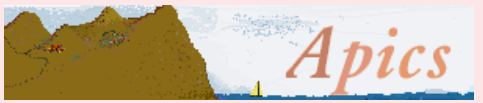
José Grimm

Projet Apics (ex-Miaou)
Institut National de Recherche en Informatique et Automatique
Sophia Antipolis

Mai-octobre 2004

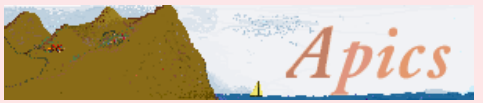
Plan

1 Introduction



Plan

1. Introduction
2. Méthodes d'authentification
   - Pourquoi
   - Comment
   - Secure Key



Plan

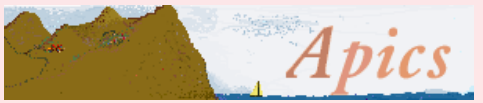
1. Introduction
2. Méthodes d'authentification
   - Pourquoi
   - Comment
   - Secure Key
3. Secure Shell
   - Définition
   - Créer
   - Diffuser la clé
   - Se connecter

Plan

1. Introduction
2. Méthodes d'authentification
   - Pourquoi
   - Comment
   - Secure Key
3. Secure Shell
   - Définition
   - Créer
   - Diffuser la clé
   - Se connecter
4. Utilisation

Plan

1. Introduction
2. Méthodes d'authentification
   - Pourquoi
   - Comment
   - Secure Key
3. Secure Shell
   - Définition
   - Créer
   - Diffuser la clé
   - Se connecter
4. Utilisation

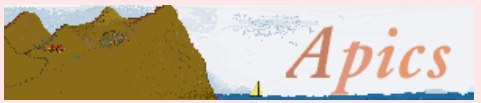


Résumé

A compter du premier juin 2004, on ne peut plus se connecter à l'Inria Sophia que via X/Skey et SSH sur les serveurs de projets.

Résumé

A compter du premier juin 2004, on ne peut plus se connecter à l'Inria Sophia que via X/Skey et SSH sur les serveurs de projets. Cette décision a surpris certaines personnes.



Résumé

A compter du premier juin 2004, on ne peut plus se connecter à l'Inria Sophia que via X/Skey et SSH sur les serveurs de projets. Cette décision a surpris certaines personnes.
Dans cet exposé on expliquera les avantages au niveau sécurité offerts par ces deux mécanismes, l'un par rapport à l'autre, et par rapport aux mots de passe Unix.
On expliquera comment utiliser SSH, en suivant les instructions de la page web du semir :
http://www-sop.inria.fr/semir/securite/ssh/

Plan

1. Introduction
2. Méthodes d'authentification
   - Pourquoi
   - Comment
   - Secure Key
3. Secure Shell
   - Définition
   - Créer
   - Diffuser la clé
   - Se connecter
4. Utilisation

Pourquoi l'authentification

- Protéger mes fichiers (en lecture - écriture)
- Pour les chefs : mails confidentiels, autorisations.
- Pour les administrateurs : (root sur charrette, accès net-sop)
- Éviter les blagues stupides faite par un copain
- Ne pas servir de relais (virus, spam, etc)
- $\Rightarrow$ restrictions mail portable via ppp.

Comment la machine sait qui est quoi

- UID/GID associé à un nom, et des fichiers
- grimm = gaWpl0UUAUsXU:3001:1030

Comment la machine sait qui est quoi

- UID/GID associé à un nom, et des fichiers
- grimm = gaWpl0UUAUsXU:3001:1030
- `groups; ls -lLnd /proj/apics/www`
  apics root cgibin raps nnet
  drwxrwxr-x 15 3000 1030 4096 Sep 28 18:39 /proj/apics/www

Comment la machine sait qui est quoi

- UID/GID associé à un nom, et des fichiers
- grimm = gaWpl0UUAUsXU:3001:1030
- `groups; ls -lLnd /proj/apics/www`
  apics root cgibin raps nnet
  drwxrwxr-x 15 3000 1030 4096 Sep 28 18:39 /proj/apics/www
- Machines reconnues par adresses IP (netgroup m-apics)
- paris = 138.96.114.42, 138.96.242.42

Comment la machine sait qui est quoi

- UID/GID associé à un nom, et des fichiers
- grimm = gaWpl0UUAUsXU:3001:1030
- `groups; ls -lLnd /proj/apics/www`
  apics root cgibin raps nnet
  drwxrwxr-x 15 3000 1030 4096 Sep 28 18:39 /proj/apics/www
- Machines reconnues par adresses IP (netgroup m-apics)
- paris = 138.96.114.42, 138.96.242.42
- Mot de passe Unix associé à un nom de login

Comment la machine sait qui est quoi

- UID/GID associé à un nom, et des fichiers
- grimm = gaWpl0UUAUsXU:3001:1030
- `groups; ls -lLnd /proj/apics/www`
  apics root cgibin raps nnet
  drwxrwxr-x 15 3000 1030 4096 Sep 28 18:39 /proj/apics/www
- Machines reconnues par adresses IP (netgroup m-apics)
- paris = 138.96.114.42, 138.96.242.42
- Mot de passe Unix associé à un nom de login
- Mot de passe nécessaire pour se connecter.
- Idem pour déverouiller l'écran.

Connexion vers l'extérieur

- Pas besoin de passwd pour les machines internes Inria dans les bons cas (Réseau de production)

Connexion vers l'extérieur

- Pas besoin de passwd pour les machines internes Inria dans les bons cas (Réseau de production)
- Mot de passe pour les machines Windows

Connexion vers l'extérieur

- Pas besoin de passwd pour les machines internes Inria dans les bons cas (Réseau de production)
- Mot de passe pour les machines Windows
- Connexion sécurisée vers mirsa par le web pour changer son password. Fingerprint : 57:BB:CA:46:EC:C4:B3:88:51:51:36:F2:39:B3:C7:3B

Connexion vers l'extérieur

- Pas besoin de passwd pour les machines internes Inria dans les bons cas (Réseau de production)
- Mot de passe pour les machines Windows
- Connexion sécurisée vers mirsa par le web pour changer son password. Fingerprint : 57:BB:CA:46:EC:C4:B3:88:51:51:36:F2:39:B3:C7:3B
- J'ai 8 mots de passe gérés par Mozilla

Accès aux fichiers/ressources sur machine distante

- Remote shell sans passwd dans le projet [login]
- Cas des fichiers `~/.rhosts` (hors projet)

Accès aux fichiers/ressources sur machine distante

- Remote shell sans passwd dans le projet [login]
- Cas des fichiers `~/.rhosts` (hors projet)
- Xauth et les biscuit magiques [écran]

Accès aux fichiers/ressources sur machine distante

- Remote shell sans passwd dans le projet [login]
- Cas des fichiers `~/.rhosts` (hors projet)
- Xauth et les biscuit magiques [écran]
- Montages NFS pour les disques [fichiers]
- ex1: /0 @m-sophia(ro,all_squash) @m-apics(rw) local25(rw)
- ex2: /0/projserver @m-sophia(insecure,ro,all_squash) @m-apics(insecure,rw) doc-serv(insecure,rw)

Secure key & Mot de passe à usage unique

- Utilise des OTP (one time password)
- Soit $A = f_q^n(P)$, $B = f_q^{n-1}(P)$. Alors $A = f_q(B)$
- Le mot de passe P n'est pas connu par la machine
- La calculatrice calcule B, la machine connait A.
- Si Ok, la machine remplace A par B
- exemple d'OTP: NOLL GLIB YET DIN BEG ELLA
- Ne pas dupliquer les fichiers (q est unique)
- Initialiser (sur place) avant d'utiliser
- Protéger la calculatrice.

Plan

1. Introduction
2. Méthodes d'authentification
   - Pourquoi
   - Comment
   - Secure Key
3. Secure Shell
   - Définition
   - Créer
   - Diffuser la clé
   - Se connecter
4. Utilisation

SSH

- Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another.
- It provides strong authentication and secure communications over unsecure channels.
- It is intended as a replacement for telnet, rlogin, rsh, and rcp.
- For SSH2, there is a replacement for FTP: sftp.

Protocoles

- Algorithme symmétrique rapide (DES). Utilise une clé par session.
- Calcule des paquets de $f_p(x)$, x: 64 bits, p 56 bits.

Protocoles

- Algorithme symmétrique rapide (DES). Utilise une clé par session.
- Calcule des paquets de $f_p(x)$, x: 64 bits, p 56 bits.
- Cryptographie à clé publique (RSA, ou courbes elliptiques). $f(x) = x^e \mod n$; $x = f^d$. Résoudre $ed = 1 \mod \phi(n)$. n de l'ordre de 1024bits

Protocoles

- Algorithme symmétrique rapide (DES). Utilise une clé par session.
- Calcule des paquets de $f_p(x)$, x: 64 bits, p 56 bits.
- Cryptographie à clé publique (RSA, ou courbes elliptiques). $f(x) = x^e \mod n$; $x = f^d$. Résoudre $ed = 1 \mod \phi(n)$. n de l'ordre de 1024bits
- Protéger la clé via un "pass-phrase".
- Échange de clés via Diffie-Hellman.

Protocoles

- Algorithme symmétrique rapide (DES). Utilise une clé par session.
- Calcule des paquets de $f_p(x)$, x: 64 bits, p 56 bits.
- Cryptographie à clé publique (RSA, ou courbes elliptiques). $f(x) = x^e \mod n$; $x = f^d$. Résoudre $ed = 1 \mod \phi(n)$. n de l'ordre de 1024bits
- Protéger la clé via un "pass-phrase".
- Échange de clés via Diffie-Hellman.
- Fonction de hachage (MD5, SHA1). Donne 128 ou 160 bits. Le plus injectif possible.

Créer la clé

```
cligès-% /usr/local/openssh/bin/ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key
(/user/grimm/home/.ssh/id_rsa):
Created directory '/user/grimm/home/.ssh'.
Enter passphrase (empty for no passphrase): méga-secret
Enter same passphrase again: méga-secret
Your identification has been saved in
/user/grimm/home/.ssh/id_rsa.
Your public key has been saved in
/user/grimm/home/.ssh/id_rsa.pub.
The key fingerprint is:
11:22:33:44:55:66:78:90:aa:bb:cd:ef:34:54:23:43 grimm@cligès
```

J'ai une clé

Vous venez de générez une clé publique (fichier `~/.ssh/id_rsa.pub`)

J'ai une clé

Vous venez de générez une clé publique (fichier `~/.ssh/id_rsa.pub`) et une clé privée (`~/.ssh/id_rsa`) sur votre machine.

J'ai une clé

Vous venez de générez une clé publique (fichier `~/.ssh/id_rsa.pub`) et une clé privée (`~/.ssh/id_rsa`) sur votre machine.
La clé publique est en clair et peut être propagée partout où vous en avez besoin.

J'ai une clé

Vous venez de générez une clé publique (fichier `~/.ssh/id_rsa.pub`) et une clé privée (`~/.ssh/id_rsa`) sur votre machine.
La clé publique est en clair et peut être propagée partout où vous en avez besoin.
C'est la présence de cette clé privée sur la machine d'où vous vous connectez qui vous permettra d'accéder au serveur SSH.

A quoi sert ma clé, et la phrase de passe

Corollaire

pas de clé privée, pas de connexion !

A quoi sert ma clé, et la phrase de passe

Corollaire

pas de clé privée, pas de connexion !

Corollaire

La clé privée est une donnée sensible. Elle est stockée de manière chiffrée sur le disque dur ou clé USB.

A quoi sert ma clé, et la phrase de passe

Corollaire

pas de clé privée, pas de connexion !

Corollaire

La clé privée est une donnée sensible. Elle est stockée de manière chiffrée sur le disque dur ou clé USB.

Corollaire

ne laissez pas traîner des clés privées derrière vous.

A quoi sert ma clé, et la phrase de passe

Corollaire

pas de clé privée, pas de connexion !

Corollaire

La clé privée est une donnée sensible. Elle est stockée de manière chiffrée sur le disque dur ou clé USB.

Corollaire

ne laissez pas traîner des clés privées derrière vous.

Le password que la commande ssh-keygen vous demande est celui qui permet de chiffrer/déchiffrer cette clé.

A quoi sert ma clé, et la phrase de passe

Corollaire

pas de clé privée, pas de connexion !

Corollaire

La clé privée est une donnée sensible. Elle est stockée de manière chiffrée sur le disque dur ou clé USB.

Corollaire

ne laissez pas traîner des clés privées derrière vous.

Le password que la commande ssh-keygen vous demande est celui qui permet de chiffrer/déchiffrer cette clé.
Ce password doit être le plus complexe possible et surtout être différent de vos autres password.

Je dépose la clé

Exemple (Dépot local (home dir sur serveur))

```
cligès-% cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys
cligès-% chmod 400 ~/.ssh/authorized_keys
```

Je dépose la clé

Exemple (Dépot local (home dir sur serveur))

```
cligès-% cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys
cligès-% chmod 400 ~/.ssh/authorized_keys
```

Exemple (Dépot rsh)

```
cligès-% rsh charrette mkdir .ssh
cligès-% rcp ~/.ssh/id_rsa.pub charrette:.ssh/authorized_keys
cligès-% rsh charrette chmod 700 .ssh
cligès-% rsh charrette chmod 400 .ssh/authorized_keys
```

Je dépose la clé

Exemple (Dépot local (home dir sur serveur))

```
cligès-% cp ~/.ssh/id_rsa.pub ~/.ssh/authorized_keys
cligès-% chmod 400 ~/.ssh/authorized_keys
```

Exemple (Dépot rsh)

```
cligès-% rsh charrette mkdir .ssh
cligès-% rcp ~/.ssh/id_rsa.pub charrette:.ssh/authorized_keys
cligès-% rsh charrette chmod 700 .ssh
cligès-% rsh charrette chmod 400 .ssh/authorized_keys
```

Exemple (Dépot ftp (via S/Key))

Voir doc en ligne

La première connexion

Exemple (Pas serveur)

cligès-% ssh telegone
ssh: connect to host telegone port 22: Connection refused

La première connexion

Exemple (Pas de clé)

cligès-% ssh charrette
The authenticity of host 'charrette (138.96.114.36)' can't be established.
RSA key fingerprint is a0:f9:b6:ea:5b:72:e2:e6:53:4f:5c:0f:56:06:e8:3c.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'charrette,138.96.114.36' (RSA) to the list of known hosts.
Permission denied (publickey,keyboard-interactive).

La première connexion

Exemple (OK)

cligès-% ssh charrette
The authenticity of host ...
RSA key fingerprint is ...
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added ...
Enter passphrase for key '/user/grimm/home/.ssh/id_rsa':
méga-secret
Last login: Fri Oct 1 11:30:21 2004 from medee.inria.fr

charrette-%

La première connexion

Exemple (via ssh-agent)

```
cligès-% ssh charrette
Last login: Fri Oct 1 11:30:21 2004 from medee.inria.fr
charrette-%
```

Plan

1. Introduction
2. Méthodes d'authentification
   - Pourquoi
   - Comment
   - Secure Key
3. Secure Shell
   - Définition
   - Créer
   - Diffuser la clé
   - Se connecter
4. Utilisation

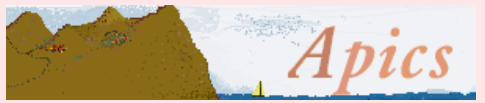
Les tunnels

Un des intérêt de ssh est qu'il permet de tunneller des sessions X11 de manière complètement automatique à l'utilisateur. Ainsi aussitôt après une connexion par ssh, on peut lancer une commande X11 (ex un xterm) qui circulera de manière chiffrée dans le tunnel ssh.
Idem Pop, web, CVS, etc.

Exemple de tunnels

Exemple (Application X)

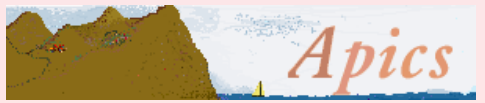
cligès-% ssh charrette
charrette-% xterm



Exemple de tunnels

Exemple (Application distante)

cligès-% ssh charrette
charrette-% rstart saturne xterm



Exemple de tunnels

Exemple (Serveur Pop)

```
cligès-% ssh -L12345:SERVEUR-POP:110 charrette
charrette-% ∅
cligès-% telnet localhost 12345
```

Au lieu de telnet : lire son mail. Configurer son mailer préféré pour lire sur le serveur ‘locahost’, port ‘12345’.

Exemple de tunnels

Exemple (Serveur Web)

cligès-% ssh -L12345:www-sop:80 charrette
charrette-% ∅
cligès-% wget http://localhost:1234/index.html

Exemple de tunnels

Exemple (Proxy Web)

```
cligès-% ssh -L12345:cache-sop:8080 charrette
charrette-% ∅
```

Configurer le proxy de son navigateur comme étant ‘localhost:12345’, puis utiliser les URL classiques.

En cas de problème

```
cligès-% ssh tempete
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-midd
It is also possible that the RSA host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
63:9b:38:ae:55:08:95:82:5e:88:38:54:0f:06:e5:51.
Please contact your system administrator.
Add correct host key in /user/grimm/home/.ssh/known_hosts to ge
Offending key in /user/grimm/home/.ssh/known_hosts:3
RSA host key for tempete has changed and you have
requested strict checking.
Host key verification failed.
```

Agent

ssh-agent est un proxy d'authentification, auquel peut s'adresser le client ssh (dans certaines conditions) pour simplifier la vie de l'utilisateur. En effet, grâce à ce proxy d'authentification, on ne tappe son password qu'une seule fois et ensuite toutes les sessions ssh seront complètement transparentes (sans password).
Attention: l'utilisation de ssh-agent doit être réservée dans les cas où on est complètement sûr de l'environnemenent de travail.
Accès sur le serveur CVS de sophia via SSH.
`:ext:grimm@cvs-sop.inria.fr:/CVS/disc_raweb`

De la lecture

N. Stephenson.
Cryptonomicon.
Payot, 2000.

W. Stallings
Cryptography and network security. Principle and Practice.
Pearson Education, Inc. 2003.

- www.openssh.org
- http://www-sop.inria.fr/semir/securite/ssh/
- http://www-sop.inria.fr/semir/securite/DR:I/gnupg.html
- http://www-sop.inria.fr/semir/serveurs/cvs/

FIN

Cette suite de transparents a été réalisée avec le package beamer.
Version Juan-Les-Pins