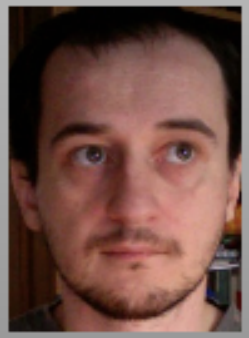
Certificats OpenSSH: gérez vos identités dans l'espace et dans le temps

Kevin DENIS

Le 11 Juillet 2011

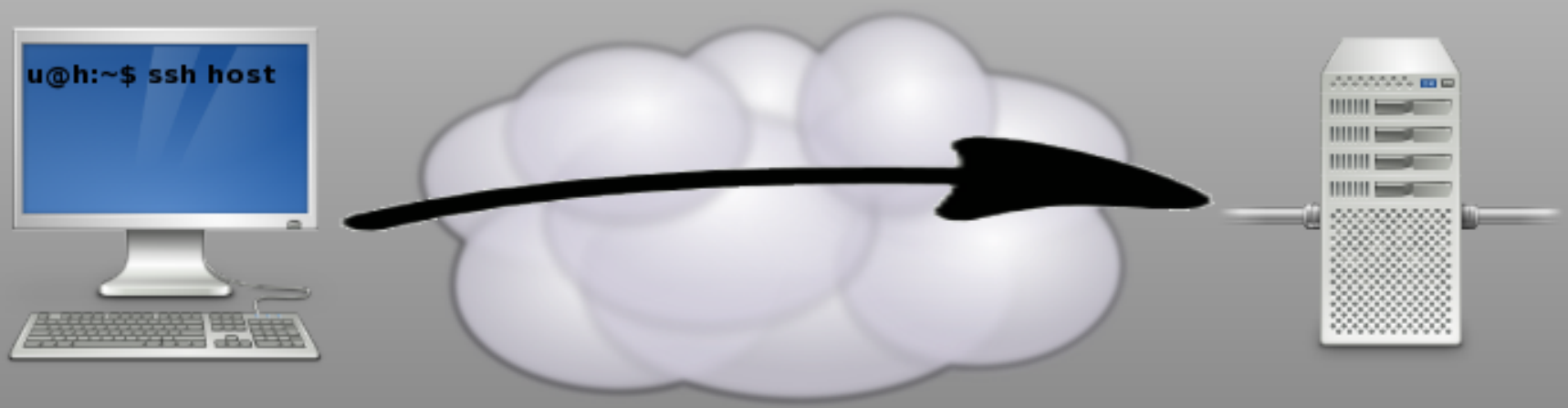


kevin2nis@gmail.com

http://exploitability.blogspot.com

http://www.arkoon.net

http://www.openssh.org/fr/goals.html



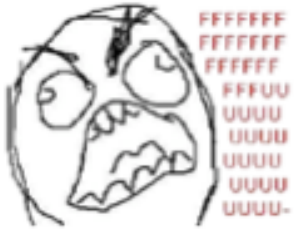
1/ Echange Diffie-Hellman

2/ Authentification du serveur

3/ Authentification du client

Ecoute passive
DNS spoof ou IP spoof
Connection hijacking ou Compensation
Man in the Middle
User lockdown

Security approved!



*le admin

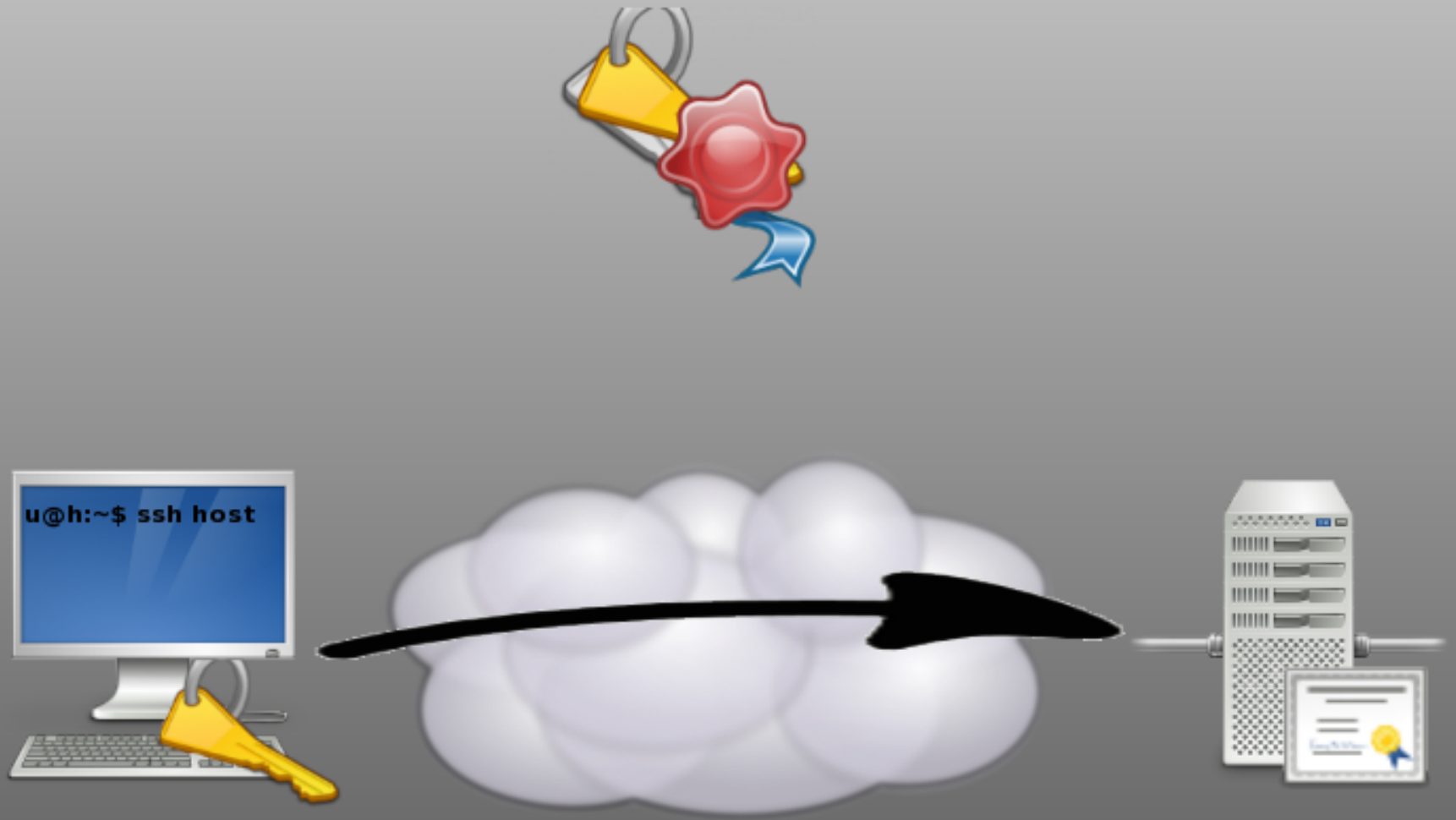
Contraintes de l'administration:

Importance de la clé publique du serveur

Gestion des clés utilisateurs sur chacun des serveurs ssh

Création d'une autorité de certification

```
root@slackware:~# ssh-keygen -f CA-Key
Generating public/private rsa key pair.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in CA-Key.
Your public key has been saved in CA-Key.pub.
```




```
ssh-keygen -s CA-Key -I CA -h host_rsa_key.pub
           [ -n <hostname>|<@IP CIDR>]
```


```
ssh-keygen -s CA-Key -I CA -n user1 user_rsa_key.pub
           [ -V validity ]
           [ -O options ]
```

Le "principal" (-n) n'est pas forcément le nom

Une CA pour certifier les hôtes
-> Valide pour tous les clients

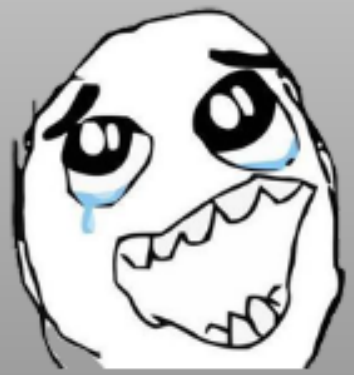
Une CA par groupe d'utilisateurs/serveurs
-> Gestion fine des droits d'accès

WebCA

ClusterCA

Un fichier "principal"
-> Des principals "-n user@host"
-> Fichier authorized_principals: user@host

La révocation:
Manuelle sur chacun des hôtes et clients



En résumé:

Création de la CA

```
ssh-keygen -f CA-Key
```

Ajout de la clé dans les .ssh/known_hosts

```
@cert-authority * AAAAB(...)3A8yfN root@slackware
```

Certification d'un hôte

```
ssh-keygen -s CA-Key -I CA -h host_rsa_key.pub
HostCertificate /etc/ssh/host_rsa_key-cert.pub
```

Certification des utilisateurs

```
ssh-keygen -s CA-Key -I CA -n user1 user_rsa_key.pub
TrustedUserCAKey /etc/ssh/pub.keys
```

Merci

Des questions?