SSH

報告學生:何冠儒

指導教授:梁明章

SSH 之認證方法

- 1. 密碼認證
- 2. 金鑰認證

SSH 欺騙

- 1. 觀察同學在學校的使用方式
- 2. 四處利用公用電腦
- 3. 使用 Putty or Pietty
- 4. 不經確認的便接受金鑰

金鑰確認錯誤的處理(Linux)

```
decaylala@ubuntu:~$ ssh 140.127.220.59
The authenticity of host '140.127.220.59 (140.127.220.59)' can't be establishe
RSA key fingerprint is ac:6a:3e:6b:41:6e:76:3d:37:27:00:4f:34:39:c6:a5.
Are you sure you want to continue connecting (yes/no)?
```

金鑰確認錯誤的處理(XP)

PieTTY Security Alert

ΧI



The server's host key is not cached in the registry. You have no guarantee that the server is the computer you think it is.

The server's rsa2 key fingerprint is:

ssh-rsa 2048 ac:6a:3e:6b:41:6e:76:3d:37:27:00:4f:34:39:c6:a5

If you trust this host, hit Yes to add the key to PieTTY's cache and carry on connecting.

If you want to carry on connecting just once, without adding the key to the cache, hit No.

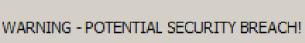
If you do not trust this host, hit Cancel to abandon the connection.

是(Y)

否(№)



PieTTY Security Alert



The server's host key does not match the one PieTTY has cached in the registry. This means that either the server administrator has changed the host key, or you have actually connected to another computer pretending to be the server.

The new rsa2 key fingerprint is:

ssh-rsa 2048 ef:93:eb:83:74:7c:91:d5:7e:1e:76:9e:ca:82:88:72
If you were expecting this change and trust the new key,
hit Yes to update PieTTY's cache and continue connecting.
If you want to carry on connecting but without updating
the cache, hit No.

If you want to abandon the connection completely, hit Cancel. Hitting Cancel is the ONLY guaranteed safe choice.

是(Y)

否(N)

取消

X

SSH 欺騙之方式

- 1. 監聽網路
- 2. 使用 IP 欺騙
- 3. 拐騙 Client 連線至『假』登入環境
- 4. 騙取 account 和 password

SSH 欺騙之問題

若再重新連到正確 Server '

會跳出接受金鑰的確認視窗。

SSH 金鑰認證之優點

- 1. 增加安全性,確保機器正確性
- 2. 減少主機被 try 密碼的機會
- 2. 不用密碼,連線很方便

SSH 金鑰認證之缺點

- 1. 較麻煩,若多台機器,需一一設定
- 2. 使用公用電腦的不便
- 3. Private Key == Password

SSH 金鑰認證之設定

設定檔 /etc/ssh/sshd_config

SSH 金鑰認證之作法(Linux)

\$ ssh-keygen -t rsa 產生 id_rsa (Private Key) 和 id rsa.pub (Public Key)

```
decaylala@ubuntu:~$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/decaylala/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/decaylala/.ssh/id_rsa.
Your public key has been saved in /home/decaylala/.ssh/id_rsa.pub.
The key fingerprint is:
cc:17:c7:25:75:32:79:45:48:79:b6:52:c8:fb:ea:07 decaylala@ubuntu
```

SSH 金鑰認證之作法(Linux)

◆ Client 端

將 id_rsa 放置 ~/.ssh/ 裡

◆ Server 端

\$ cat id_rsa.pub >> ~/.ssh/authorized_keys

SSH 金鑰認證之作法(Linux)

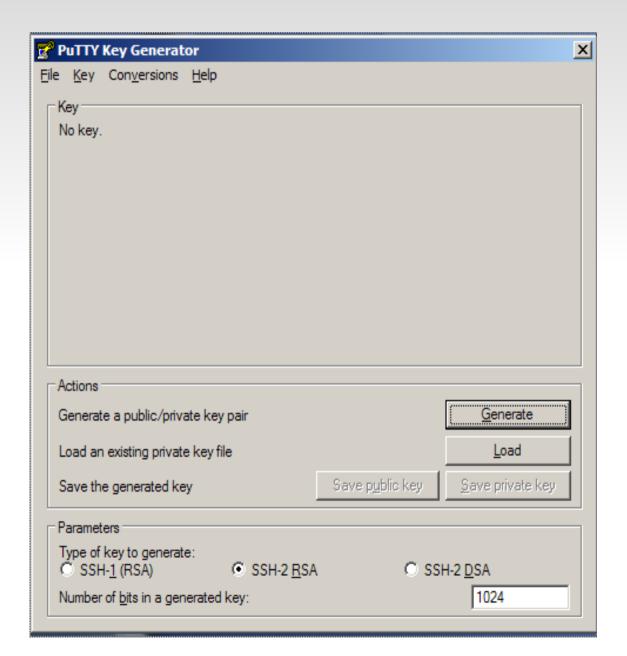
```
decaylala@ubuntu:~$ ssh 140.127.220.59
Linux ubuntu 2.6.20-16-generic #2 SMP Sun Sep 23 19:50:39 UTC 2007 i686
```

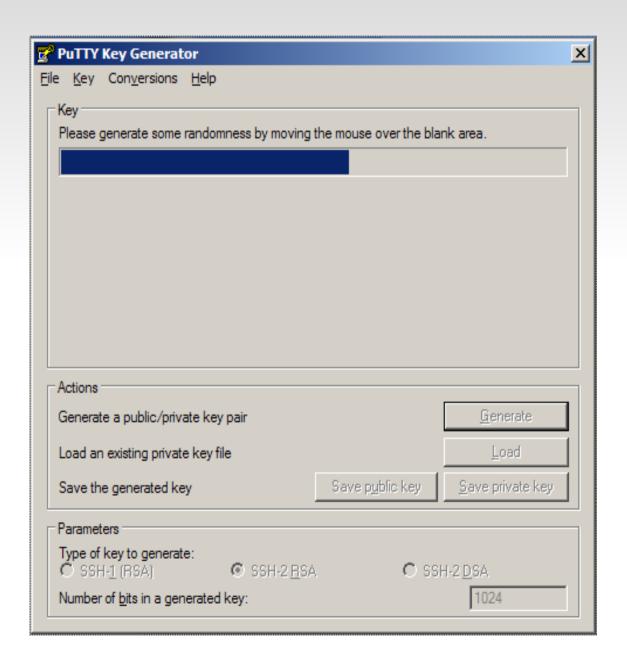
The programs included with the Ubuntu system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law.

Last login: Fri Jan 18 00:39:59 2008 from 122-122-103-131.dynamic.hinet.net decaylala@ubuntu:~\$

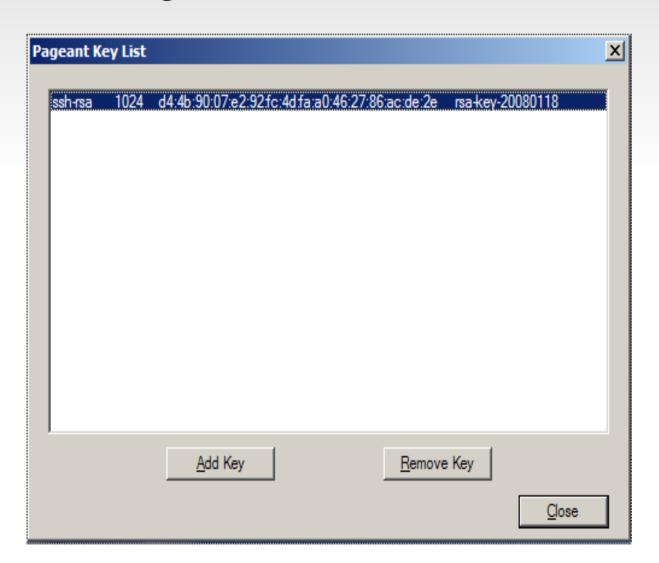
使用 PuTTYgen 產生公、私鑰





| 📝 PuTTY Key Generator | | | | X |
|---|--|--------------------------|--------------------------|---|
| <u>File Key Conversions</u> | <u>H</u> elp | | | |
| - Key | | | | |
| Public key for pasting into OpenSSH authorized_keys file: | | | | |
| ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAIEAqU8S/BZam4PStTUJ8bjRzeGt6zxzRHJZ2YArP E1p8xqqksylJ7t0Ev91o8yfoBgwARlrR1BlnzEF0bZNMK+1gpAS+NiYffEl10vTrdogqH QS+CLcM86z99FVkZJF8CRe7PlFguvDD6ycmufA+QZjM+t8zqrYlLlTur6lwPEq2o0= rsa key-20080118 | | | | |
| Key fingerprint: | ssh-rsa 1024 0a:61:56:87:85:04:60:63:72:bd:74:93:a7:5e:89:36 | | | |
| Key comment: rsa-key-20080118 | | | | |
| Key passphrase: | J | | | |
| Confirm passphrase: | | | | |
| Actions | | | | |
| Generate a public/private key pair | | | <u>G</u> enerate | |
| Load an existing private key file | | | <u>L</u> oad | |
| Save the generated key | | Save p <u>u</u> blic key | <u>S</u> ave private key | |
| Parameters | | | | |
| Type of key to generate: © SSH-1 (RSA) © SSH-2 RSA © SSH-2 DSA | | | | |
| Number of bits in a generated key: 1024 | | | | |

使用 Pageant 處理 Private Key



The End