<http://www.cnblogs.com/ggjucheng/archive/2012/08/19/2646029.html>

当你登入远程服务器时，本机会主动的用接收到的服务器的 public key 去比对 ~/.ssh/known\_hosts 有无相关的公钥， 然后进行底下的动作：

* 若接收的公钥尚未记录，则询问用户是否记录。若要记录 (范例中回答 yes 的那个步骤) 则写入 ~/.ssh/known\_hosts 且继续登入的后续工作；若不记录 (回答 no) 则不写入该档案，并且离开登入工作；
* 若接收到的公钥已有记录，则比对记录是否相同，若相同则继续登入动作；若不相同，则出现警告信息， 且离开登入的动作。这是客户端的自我保护功能，避免你的服务器是被别人伪装的。

虽然说服务器的 ssh 通常可能会改变，问题是，如果是测试用的主机，因此常常在重新安装，那么服务器的公钥肯定经常不同， 果真如此的话，你就无法继续登入了！

那怎办？让我们来模拟一下这个行为吧！让你比较有印象啦！

例题：

仿真伺服器重新安装后，假设服务器使用相同的 IP ，造成相同 IP 的服务器公钥不同，产生的问题与解决之道为何？

答：

利用前一小节讲过的方式，删除原有的系统公钥，重新启动 ssh 让你的公钥更新：

rm /etc/ssh/ssh\_host\*

/etc/init.d/sshd restart

然后重新使用底下的方式来进行联机的动作：

[复制代码](javascript:void(0);)

[root@www ~]# ssh root@localhost

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED! @ <==就告诉你可能有问题

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@

IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!

Someone could be eavesdropping on you right now (man-in-the-middle attack)!

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

a7:2e:58:51:9f:1b:02:64:56:ea:cb:9c:92:5e:79:f9.

Please contact your system administrator.

Add correct host key in /root/.ssh/known\_hosts to get rid of this message.

Offending key in /root/.ssh/known\_hosts:1 <==冒号后面接的数字就是有问题数据行号

RSA host key for localhost has changed and you have requested strict checking.

Host key verification failed.

[复制代码](javascript:void(0);)

上述的表格出现的错误讯息中，特殊字体的地方在告诉你：/root/.ssh/known\_hosts 的第 1 行，里面的公钥与这次接收到的结果不同， 很可能被攻击了！那怎办？没关系啦！请你使用 vim 到 /root/.ssh/known\_hosts ，并将第 1 行(冒号 : 后面接的数字就是了) 删除，之后再重新 ssh 过，那系统又会重新问你要不要加上公钥啰！就这么简单！ ^\_^

 转自 <http://vbird.dic.ksu.edu.tw/linux_server/0310telnetssh_2.php#ssh_start>