

Public key authentication troubles

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-05/0203.html>

From: Nicolas Bertolotti (*nbertolo_at_chez.com*)

Date: 05/22/04

Date: Sat, 22 May 2004 01:01:08 +0200

Hi,

I'm facing troubles while trying to activate connection without a password on a specific linux box.

I've generated the keys using `ssh-keygen -t rsa1`

I've then copied the public key to `authorized_keys` : `cp .ssh/identity.pub .ssh/authorized_keys`

I've also changed the permissions : `chmod go-rwx .ssh`

and when I run (as 'poly' user): `ssh -v -1 `hostname``, I get :

OpenSSH_3.5p1, SSH protocols 1.5/2.0, OpenSSL 0x0090701f

debug1: Reading configuration data /etc/ssh/ssh_config

debug1: Applying options for *

debug1: Rhosts Authentication disabled, originating port will not be trusted.

debug1: ssh_connect: needpriv 0

debug1: Connecting to rhombus.polyspace.us [172.16.1.52] port 22.

debug1: Connection established.

debug1: identity file /home/poly/.ssh/identity type 0

debug1: Remote protocol version 1.99, remote software version OpenSSH_3.5p1

debug1: match: OpenSSH_3.5p1 pat OpenSSH*

debug1: Local version string SSH-1.5-OpenSSH_3.5p1

debug1: Waiting for server public key.

debug1: Received server public key (768 bits) and host key (1024 bits).

debug1: Host 'rhombus.polyspace.us' is known and matches the RSA1 host key.

debug1: Found key in /home/poly/.ssh/known_hosts:2

debug1: Encryption type: 3des

debug1: Sent encrypted session key.

debug1: cipher_init: set keylen (16 -> 32)

debug1: cipher_init: set keylen (16 -> 32)

debug1: Installing crc compensation attack detector.

debug1: Received encrypted confirmation.

debug1: Trying RSA authentication with key '/home/poly/.ssh/identity'

debug1: Server refused our key.

debug1: Doing challenge response authentication.

debug1: No challenge.

debug1: Doing password authentication.

comp.security.ssh: Public key authentication troubles

I've done this in the past very often and it used to work fine. In order to make sure there was no problem with the configuration, I've transferred a number of files (network and ssh configuration and keys) to another computer

:

/etc/ssh/*

/etc/hosts

/etc/sysconfig/network

/etc/sysconfig/network-scripts/*

/etc/rc.d/init.d/sshd

/home/poly/.ssh/*

... and (after I reboot this new computer), when I run `ssh -v -1 `hostname``, everything works fine.

Can anyone help me ?

Best regards

Nicolas