

Sharing the SSH server keys & other questions

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2004-06/0204.html>

From: Carlos N (*cgnjunkregDELETE_at_hotmail.com*)

Date: 06/25/04

Date: Fri, 25 Jun 2004 17:05:44 -0400

Basic SSH question:

If I want to use RSA authentication by clients the process is simple. I generate a key pair, leave the private key (encrypted or not) on the client, give the public key to the server, make sure the server knows about it and presto.

This makes sense. The server administrator has to actively accept the clients key, insuring that not just anyone can login.

However, it seems that the reverse is not true. The server also has a private/public key pair (whether using key or password authentication).

It seems, however, that the server automatically will feed its public key to the client. The client checks to make sure the key is OK – sure that protects the client. But it seems like ANY client can connect and automatically gets the key. Is there a way to limit the exchange so that the admin has to hand out the server's key through a different channel? Am I missing the point?

In case you are wondering... I'm trying to set up a very simple SSH server on my home machine, so my wife can access it remotely. It seems like handing out the server key manually would be a way to restrict passerbys from trying to log in. Of course, the password and/or client key does the same thing. I'm just wondering....

On a very related note. Since she will be traveling, sometimes using her laptop, sometimes using internet cafes or hotel computers, it seems like the best option is to use password rather than key authentication.

Is this correct? This way she doesn't have to install a new key in each place. It also seems to preclude my doing any host-level access privileges in SSD.

Thanks!
Carlos