

Verifying Remote Host on First Connect

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2001-12/0338.html>

From: Alvin Sylvain (alvin.sylvain@excite.com)

Date: 12/28/01

From: alvin.sylvain@excite.com (Alvin Sylvain)

Date: 27 Dec 2001 15:14:22 -0800

The first time I connect PuTTY to the remote host, I get:

"

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 key fingerprint is:

<fingerprint>

If you trust this host, hit Yes to add the key to

PuTTY's cache and carry on connecting.

If you do not trust this host, hit No to abandon the connection.

"

OK. This is all fine and well when you trust the host, and 99% of the time, I expect I'm going to trust the host. But this whole message makes me think that obviously there must be a situation where it's possible that you CAN'T trust the host. Otherwise, why bother caching the host fingerprint?

So the question is this: Is there a mechanism where you can be physically on the site where the remote host is, load its fingerprint onto a floppy or a CD or some such, then take it to your PC and install it into the registry cache? The idea being to avoid the above warning, even the first time.

Unless, of course, you've somehow connected to a hacker's trojan host or some such. In which case, instructions to the user would be to notify an administrator immediately.

I'm more-or-less thinking of setting up an InstallShield which would install our company's software, along with a fully-configured Ssh client (such as PuTTY), including the host fingerprint and whatever it needs. The less the end-user needs to be concerned about, the better.

Thanking in advance!

comp.security.ssh: Verifying Remote Host on First Connect

- *Next message:* [ip_warrior@virgilio.it: "Re: cannot login root"](#)
- *Previous message:* [Richard E. Silverman: "Re: cannot login RH6.1 \(PAM\)"](#)
- *Messages sorted by:* [\[date \]](#) [\[thread \]](#) [\[subject \]](#) [\[author \]](#) [\[attachment \]](#)