

OpenSSH Problem –Please Help, Thank you!

Source: <http://www.derkeiler.com/Newsgroups/comp.security.ssh/2003-05/0085.html>

From: Paul (*supersupersupersupersuper_at_hotmail.com*)

Date: 05/08/03

Date: 8 May 2003 02:57:35 -0700

Hello, I was wondering if you could help me with an OpenSSH problem I am having.

I am trying to use a public/private keyset to automate an encrypted session between my client and remote machine, so that my pop3 and smtp passwords are not exposed on the way to the mail server I run. I want my servers and personal client machines on different external IPs for security reasons, which, unfortunately, exposes their passwords to the outside world.

I am having trouble automatically connecting my client Windows XP Pageant machine to my Windows XP OpenSSH remote machine (email server) using my generated keys. I am currently using OpenSSH 3.61 (April 28th, 2003, from <http://lexa.mckenna.edu/sshwindows/>), along with the latest version of Pageant off the developer's homepage (May 7th, 2003), and Puttygen from (May 6th, 2003). I am able to connect to the remote machine using Pageant, but it prompts me for login and password, instead of just letting me in automatically. I also see that it says "server has rejected our key". Now even though the key is refused, I can still login (with my password) to the account I created, and it takes me into the home directory that I am suppose to be in.

Briefly, what I did to install and test was:

On the remote email server

- 1) Create a Windows user account (with Admin privileges) named Paul for remote login.
- 2) Install OpenSSH
- 3) Run the mkgroup and mkpasswd commands (I confirmed they were created in the \etc\ directory, and passwd had Paul listed, with his SID, and BIN as his home directory)
- 4) Ran the ssh-keygen -t rsa command (no name or paraphrase) and created id_rsa and id_rsa.pub keys.
- 5) Renamed id_rsa.pub to authorized_keys and put it in Paul\.ssh\ on the remote machine.
- 6) Copied id_rsa to the client machine

On the client machine for email sending/receiving

comp.security.ssh: OpenSSH Problem –Please Help, Thank you!

- 7) Had the private id_rsa converted to a putty private key called private.pht
 - 8) Used Paagent to login to the remote machine (used default settings, port 22, ssh2 only, and pointed to private.pht
 - 9) Instead of being automatically logged in, I get a Login and Password prompt, and get an error that says "Server rejected our key".
 - 10) I entered the login name and password, which then connected me to the server, and the command prompt showed I was in my home directory on the remote machine, c:\documents and settings\paul.
- *One other note, The first time it tried to connect to the server, it gave me the standard security warning about trusting your host machine, but I knew that was standard and safe, so I said yes to storing the server info in the registry

*Remote Machine Specs: P3 1GHz, 40gigs, 256 ram, Windows XP Pro w/SP1 and patches, 10/100 nic on external IP address (1 of 5 static IPs from ISP)

*Client Machine Specs: P4 2 GHz, 60 gigs, 512 ram, WinXP Pro w/SP1, 10/100 nic on external IP address (IP #2 of 5 static addresses from ISP)

Here are the steps I have done in install, in greater detail:

On the remote machine

- 1) Make a Windows account on the remote machine named Paul, and give it a password, and administrator group membership
- 2) Install the latest version of OpenSSH (this is on a clean XP Pro install with SP1 + latest updates)
- 3) Follow the readme instructions for creating the group file using the command–line utilities in the \open_ssh\bin folder. (`mkgroup -l >> ..\etc\group`) *I typed it exactly like that, and I then checked in the \etc\ folder to see if it actually made the local group file, which it did.*
- 4) Make the user account password file using the command–line utilities. (`mkpasswd -l -u username >> ..\etc\passwd`) I used Paul for the "username". I then went to check the passwd file in the \etc\ folder, which in a text editor said that it created a user "Paul", along with his SID (Windows Security ID), and the home folder "bin".
- 5) From there I generated a public/private key set using the command–line utilities (`ssh-keygen -t rsa`), and did not give it a name or a paraphrase, since I wanted it to login automatically without any prompts.
- 6) It said it stored this in "home/paul/.ssh/id_rsa". What confused me about this was that I thought it would generate the /.ssh/id_rsa and id_rsa.pub in my default OpenSSH install directory (c:/program files/open_ssh/), and in the BIN folder in /open_ssh/ directory. Isn't this, after reading it in the passwd file, my home folder? Bin? So the default area where my account is created/stored is somewhat confusing.
- 7) I did, however, find that in c:\documents and settings\Paul, there

comp.security.ssh: OpenSSH Problem –Please Help, Thank you!

was a `\.ssh\` folder, and in it were the two files, `id_rsa` and `id_rsa.pub`. So, if I understand this correctly, is my default directory that Windows creates when you make an account (`c:\documents and settings\paul`) what OpenSSH considers as the "bin" (home) directory?

8) I renamed the `id_rsa.pub` to `authorized_keys` in the `\Paul\.ssh\` folder, and copied the `id_rsa` (private key) to my client machine,

* On the client machine*

9) From there, I used the `puttygen` utility to import `id_rsa` (it didn't ask for a passphrase, which was correct, as I didn't designate one), and then exported it to a private `putty` key, which I called `private.pht`.

10) I also noticed that it was indeed an RSA `ssh2` key, which was correct.

11) I then added the key to `Paagent`, and went into `New Session` to configure (I used the default settings)

12) I set the `ssh` tab to point to the private `putty` key I took from the remote server and converted. I set it to `ssh2` only (I also tried just `SSH2` in troubleshooting). I also tried using the forwarding ports, since I want to route my emails, but for troubleshooting, I took out those settings.

13) I also set the port to 22, and entered the external IP address of the remote machine (mail server). Then I saved my settings, checked them over again one more time, and then hit `Open`.

13) From there, like I mentioned above, it asks me for my login name and password (it took about 3 seconds to tell me this from when I hit `OPEN`). Unless I misunderstood the readme, I shouldn't have been prompted for a `Login/Password` at this point. So that's my problem.

14) I decided to enter my login name anyways, and then am greeted with the standard warning about privacy, and asked for a password. And just above the password prompt, it says "Server has rejected our key".

So I did enter `Paul's Windows's` account password on the remote machine, and it logged me in, to the path `c:\documents and settings\paul`.

One other note, the first time I tried to connect by hitting `Open`, it mentioned the standard security warning about trusting your host, but I knew it was safe, so I said `Yes` to save the registry information.

So I have read through the `Readme` files from the `OpenSSH` documentation, and the `Putty` documents, and I am just stumped. I also tried this newsgroup `comp.security.ssh`, other websites, and groups on google, but no luck in solving this issue.

I guess I have a few questions that might make help solve this problem....

1) I assume, as long as I have the private key on the client machine, and the public on the remote, that my client-side Windows login name –Mike– doesn't have to be the same as on the remote side, which is Paul?

comp.security.ssh: OpenSSH Problem –Please Help, Thank you!

- 2) I tried using `authorized_keys2` afterwards, just to troubleshoot, even though the newest version of OpenSSH doesn't need the 2, but that didn't help. Am I suppose to put this `authorized_keys` file somewhere else as well, like where the `passwd` and `group` files are, in the `\etc\` directory?
- 3) I assume, since I just renamed `id_rsa.pub` to `authorized_keys` and put it on the remote machine in `Paul\.ssh\`, I don't need that `id_rsa.pub` file on the remote machine as well in the same `\.ssh\` folder, or anywhere else?
- 4) I remember reading something about a command – `chmod 600`– or something like that, which I believe locked the file from being overwritten by the group. I tried typing that in the command prompt, but it said that wasn't recognized. (For information purposes, I always ran my command prompt in `c:\program files\openssh\bin`, which is where all the utilities are, such as `ssh-keygen.exe`). I didn't see any `chmod.exe` in that folder or anywhere, thus, I could not run that command. Is it required?
- 5) Do I need to edit anything in the `ssh_config` file or `rsa_host` files in the `\etc\` directory? I didn't mess with any of that, as I didn't see anything about it in the readme about configuring them.
- 6) I noticed that when I ran the `ssh-keygen` command and created the `Paul\.ssh\` folder with the `id_rsa` files, it didn't create anything else in the `\.ssh\` folder. Should there be a `ssh_config` file in there?
- 7) Does `openssh` need to be installed on the client machine as well? I don't think so, but just wanted to bring it up... I assume Paagent does all the work.
- 8) Since all I am trying to do is forward ports to make my email connections encrypted, all I am using is Paagent, and not putty, since I just want to authenticate keys automatically, and not do command prompt work. Should I have still installed putty?
- 9) I also tried generating another SSH2 RSA keyset using `puttygen` first, instead of the `ssh_keygen` utility with OpenSSH. I then gave pageant the private key, and copied the public key text that `puttygen` listed into the remote server's `authorized_key` file, and saved it. But that still didn't work.

Thank you for your time, and I apologize for such a long description, but I just wanted to get in every detail incase you had any questions.

Thanks again!

Paul