Using SSH and Security

AFNOG 5 Workshop

Hervey Allen

Topics

- Where to get SSH (Secure SHell)
- How to enable and configure SSH
- Where to get SSH clients for Windows
- Authentication of the server to the client (host keys)
- Issues to do with changing of the host key
- Password authentication of the client to the server
- Cryptographic authentication of the client to the server (rsa/dsa keys)
- ssh-agent and ssh-add

Cryptographic Methods and Apps

Previously we had mentioned the following practical applications apply to the following methods:

- At the link layer — PPP encryption
- At the network layer — IPSEC
- At the transport layer — TLS (SSL)
- At the application layer — SSH, PGP/GPG

SSH Application Layer Security

In this section we will go over SSH at the application layer to do both authentication and data encryption.

In the Apache+SSL section given in track 1 we discussed using SSL at the transport layer for secure web-based connections.

We are going to largely ignore SSH Version 1 issues with RSA 1 Keys, but we will note this a few times during the presentation.

Main Security Concerns

SSH applies directly to dealing with these two areas of security:

- Confidentiality
  - Keeping our data safe from prying eyes
- Authentication and Authorisation
  - Is this person who they claim to be?

Where to Get SSH

First see if SSH is installed on your system and what version. Easiest way is:

ssh -V

If you want or need an updated version of OpenSSH (current version is 3.8) you can go to the following places:

http://www.freebsd.org/ports/security.html
http://www.openssh.org/portability.html
http://www.freebsd.org/ports/
(search on 'openssh')

or, current version on FreeBSD 5.2 CD-ROM:

ftp://noc.ws.afnog.org/pub/FreeBSD/packages/All/openssh-3.6.1_.tbz

Enable and Configure OpenSSH

On our machines this is already done, but if you did somehing like:

```
pkg_add -r openssh
```

- You should make sure that /etc/rc.conf has

```
sshd_enable="YES"
```

- Take a look at /etc/ssh/ssh_config and /etc/sshd_config. In sshd_config you might be interested in:

```
PermitRootLogin yes/no
```

and in /etc/ssh/ssh_config (this can cause problems):

```
Protocol 1,2
```

There are *many* options in ssh_config and sshd_config. You should read through these files to verify they meet your expecations.

Where to Get SSH Clients for Windows

There are multiple free, shareware, and commercial ssh clients for Windows.

See http://www.openssh.org/windows.html for a list.

A few that support protocol version 2 include:

- Putty:
  http://www.chiark.greenend.org.uk/~sgtatham/putty/
- OpenSSH for Windows (using Cygwin):
  http://www.networksimplicity.com/openssh/
- Secure Shell from ssh.com (free for personal use):

  http://www.ssh.com/products/ssh/download.cfm

And F-Secure at http://www.f-secure.com/products/ssh/ is a nice product if you are willing to pay.

Some Useful SSH References

- If you want a great SSH RSA/DSA key overview Daniel Robbins CEO of gentoo.org has written a 3-part series hosted on the IBM Developer Works pages.

- **The three papers and URL's are:**

  OpenSSH Key Management, Part 1
  http://www-106.ibm.com/developerworks/library/l-keyc.html
  OpenSSH Key Management, Part 2
  http://www-106.ibm.com/developerworks/library/l-keyc2/
  OpenSSH Key Management, Part 3
  http://www-106.ibm.com/developerworks/library/l-keyc3/

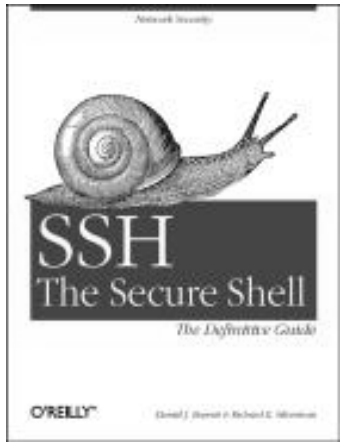
More SSH References

For a comparison of SSH Version 1 and 2 see:

http://www.snailbook.com/faq/ssh-1-vs-2.auto.html

An excellent book on SSH is:

SSH, The Secure Shell
The Definitive Guide
By Daniel J. Barrett &
Richard Silverman
January 2001
ISBN: 0-596-00011-1



SSH Connection Methods

Several things can happen when using SSH to connect from your machine (client) to another machine (server):

- Server's public host key is passed back to the client and verified against known_hosts
- Password prompt is used if public key is accepted, or already on client, or
- RSA/DSA key exchange takes place and you must enter in your private key passphrase to authenticate

SSH Quick Tips

You have a choice of authentication keys - RSA is the default as it's generally better.

The files you care about are:

/etc/ssh/ssh_config
/etc/ssh/sshd_config
~/.ssh/identity and identity.pub (deprecated)
~/.ssh/id_dsa and id_dsa.pub
~/.ssh/id_rsa and id_rsa.pub
~/.ssh/known_hosts
~/.ssh/authorized_keys
And, note the rsa/dsa host-wide key files in /etc/ssh

Be *sure* that you do “man ssh” and “man sshd” and read the entire descriptions for both the ssh client and ssh server (sshd).

SSH Authentication

Private key is protected by a passphrase
- So you have to give it each time you log in
- Or use "ssh-agent" which holds a copy of your passphrase in RAM

No need to change passwords across dozens of machines

Disable passwords entirely!
- /etc/ssh/sshd_config

Annoyingly, for historical reasons there are *three* different types of SSH key
- SSH1 RSA, SSH2 DSA, SSH2 RSA

Man in the Middle Attacks

- The first time you connect to a remote host, remember its public key
  - Stored in ~/.ssh/known_hosts
- The next time you connect, if the remote key is different, then maybe an attacker is intercepting the connection!
  - Or maybe the remote host has just got a new key, e.g. after a reinstall. But it's up to you to resolve the problem
- You will be warned if the key changes.

Exchanging Host Keys

First time connecting with ssh:

```
ssh t1@pc1.t1.ws.afnog.org
The authenticity of host 'pc1.t1.ws.afnog.org (84.201.31.11)' can't be
established.
DSA key fingerprint is 91:ba:bf:e4:36:cd:e3:9e:8e:92:26:e4:57:c4:cb:da.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'pc1.t1.ws.afnog.org,84.201.31.11' (DSA) to
the list of known hosts.
t1@pc1.t1.ws.afnog.org's password:
```

At this point the client has in the file ~/.ssh/known_hosts the contents of pc1.t1.ws.afnog.org's /etc/ssh/ssh_host_dsa_key.pub.

Next connection:

```
[hallen@hallen-lt .ssh]$ ssh t1@pc1.t1.ws.afnog.org
t1@pc1.t1.ws.afnog.org's password:
```

Now trusted - Not necessarily a good thing...

Exchanging Host Keys Cont.

Command	Key Type Generated	Public File
ssh-keygen -t rsa	RSA (SSH protocol 2)	id_rsa.pub
ssh-keygen -t dsa	DSA (SSH protocol 2)	id_dsa.pub

- Default key size is 1024 bits
- Public files are text
- Private files are encrypted if you use a passphrase (still text)

Corresponding file on the host for host key exchange is “known_hosts”.

Exchanging Host Keys Cont.

How does SSH decide what files to compare?

Look in /etc/ssh/sshd_config. For OpenSSH version 2 and 3 the server defaults to protocol 2 then 1.

By default OpenSSH version 2 client connects in this order:

RSA version 2 key
DSA version 2 key
Password based authentication (even if RSA version 1 key is present)

Pay attention to the "HostKeyAlgorithms" setting in /etc/ssh/ssh_config to help determine this order - or use ssh command line switches to override these settings.

OpenSSH 3.x Differences

- Note: OpenSSH 3.8 supports SSH protocol versions 1.3, 1.5, and 2.0. There is no SSH protocol version 3.0.
- OpenSSH 3.x vs. 2.x. Some file locations changed.
- OpenSSH 3.8 uses authorized_keys and known_hosts files for *both* protocol 1 and 2 keys.

SSH - “childMagicPhrase”

Basic concept to understand how an SSH connection is made using RSA/DSA key combination:

- Client X contacts server Y via port 22.
- Y generates a random number and encrypts this using X's public key. X's public key must reside on Y. You can use scp to copy this over.
- Encrypted random number is sent back to X.
- X decrypts the random number using it's private key and sends it back to Y.
- *If the decrypted number matches the original encrypted number, then a connection is made.*
- The originally encrypted random number sent from Y to X is the “childMagicPhrase”

We'll try drawing this as well...

SSH - ssh-agent and ssh-add

You can use ssh-agent to start a process with an ssh wrapper. For example:

```
ssh-agent /usr/local/bin/bash
```

Then you can use ssh-add to add your private keys in to memory under the ssh-agent session. For example to add your private keys:

```
ssh-add ~/.ssh/id_dsa
ssh-add ~/.ssh/id_rsa
```

You will be prompted for your private key password(s) if you have any set. If you just type "`ssh-add`", then all keys are added, with RSA first then DSA.

SSH - Lab

We will now practice the following concepts:

- The use of known_hosts files
- SSH connection with password authentication
- RSA version 2 protocol key generation
- Public key copying
- Connecting with private key passphrase using key-based authentication
- Using scp with RSA key authentication
- Using ssh-agent and ssh-add to connect without a password or passphrase challenge*

*Technically you are still challenged (even if that is a bad pun in English).

SSH - Lab Cont.

The use of known_hosts files

Connect to the machine next to your machine using ssh:

```
ssh t1@pcn.t1.ws.afnog.org
```

If this is your first connection to this machine you should see (example uses host5 connecting to host6):

```
pc1# ssh t1@pc6.t1.ws.afnog.org
The authenticity of host 'pc6.t1.ws.afnog.org (84.201.31.16)' can't be
established.
RSA1 key fingerprint is 60:f7:04:8b:f7:61:c4:41:6e:9a:6f:53:7d:95:cb:29.
Are you sure you want to continue connecting (yes/no)?
```

Go ahead and answer “yes” here, but we'll discuss the implications of this in class. Are there ways around this? Could this be a “man in the middle” attack? What file is created or updated? Why?

SSH - Lab Cont.

ssh connection with password authentication

At the prompt below when you answered yes, you were asked to enter in the root password for pcn.t1.ws.afnog.org:

```
host5# ssh t1@pc6.t1.ws.afnog.org
The authenticity of host 'pc6.t1.ws.afnog.org (84.201.31.16)' can't be
established.
RSA2 key fingerprint is 60:f7:04:8b:f7:61:c4:41:6e:9a:6f:53:7d:95:cb:29.
Are you sure you want to continue connecting (yes/no)? yes
```

And, this is what you should have seen:

```
Warning: Permanently added 'pc6.t1.ws.afnog.org' (RSA2) to the list of known
hosts.                [/etc/ssh/ssh_host_key.pub]

t1@pc6.t1.ws.afnog.org's password:
```

Now you are “securely” connected as t1 to pcn.t1.ws.afnog.org - We will discuss what happened during this connection.

SSH - Lab Cont.

rsa1/rsa2/dsa Key Generation

We will now generate a single RSA SSH protocol 2 key of 2048 bits. To do this, issue the following command. If you are logged in on the other machine, logout first!

Before continuing: you may need to edit /etc/ssh/ssh_config and make sure that the “Protocol” option is set either to “Protocol 2,1” or “Protocol 2”

```
ssh-keygen -t rsa -b 2048
```

You will be prompted for a file location for the key as well as for a passphrase to encrypt the key file. Be sure to enter a passphrase. Private key files without passphrases are a security hole. We'll discuss why as we complete this excercise. You can use a passphrase other than “afnog3” if you wish.

SSH - Lab Cont.

RSA 2 Key Generation

Here is the output from the command "ssh-keygen -t rsa -b 2048":

```
pc55# ssh-keygen -t rsa -b 2048
Generating public/private rsa key pair.
Enter file in which to save the key
(/root/.ssh/id_rsa): [enter]
Enter passphrase (empty for no passphrase): [pw]
Enter same passphrase again: [pw]
Your identification has been saved in /
root/.ssh/id_rsa.
Your public key has been saved in /
root/.ssh/id_rsa.pub.
The key fingerprint is:
0f:f5:b3:bc:f7:5b:c8:ce:79:d0:b1:ab:2c:67:21:62
t1@pc5.t1.ws.afnog.org
pc5#
```

SSH - Lab Cont.

Public Key Copying

Now that you have a public and private RSA(2) set of keys you can take advantage of them. We will copy the public key to the same host you connected to previously, save this to the files *known_hosts*, and then reconnect to the host and see the difference:

First you must copy the public key files to the host you used previously (pcn.t1.ws.afnog.org):

```
cd ~/.ssh
scp id_rsa.pub t1@pcn.t1.ws.afnog.org:/tmp/.
```

You will be prompted for the password for the host *and* username you are connecting to. We continue with our example using pc5 connecting to pc6 as t1.

SSH - Lab Cont.

Public Key Copying

The output from the command on the previous page looks like:

```
pc5# scp *.pub t1@pc66.t1.ws.afnog.org:/tmp/.
t1@pc6.t1.ws.afnog.org's password:
id_rsa.pub           100% |*****************************|   408       00:00
pc5#
```

You now have the public key file sitting on the host that will need them to use RSA/DSA public/private key authentication with you. You next step is to place these keys in the appropriate files.

You need the RSA keys in *~/.ssh/authorized_keys*

You can try to figure this out, or go to the next slide for steps to do this:

SSH - Lab Cont.

Public Key Copying

To copy the public keys to the correct places do the following:

```
ssh t1@pcn.t1.ws.afnog.org
cat /tmp/id_rsa.pub >> ~/.ssh/authorized_keys
rm /tmp/id_rsa.pub
exit
```

If you are unsure of what these commands do they will they are explained in class. In addition, you can do this many different ways, and you could issue the commands differently as well. If you understand what these commands do and have a preferred method, then feel free to use it.

Go to the next slide to connect with your public/private keys!

SSH - Lab Cont.

Public/Private Key Connection

To connect using your RSA protocol 2 key simply type:

```
ssh t1@pcn.t1.ws.afnog.org
```

And, here is the output you should see:

```
host5# ssh t1@pc6.t1.ws.afnog.org
Enter passphrase for RSA key 't1@pc5.t1.ws.afnog.org':
```

This is actually pretty neat! You *did not* enter in the root password for the root account on pcn.t1.ws.afnog.org, but rather you used the passphrase that you chose for your private RSA protocol 2 key when you issued the command "ssh-keygen -t rsa -b 2048" - This was used to decode the encoded random number exchanged between the hosts (remember "childMagicPhrase?").

Why was the RSA protocol 2 key used? We'll discuss this in class.

SSH - Lab Cont.

SCP Public/Private Key Connection

First disconnect from the ssh session you previously made:

```
exit
```

Now, try copying a file from your machine to the other machine (pick a small file) using SCP (SeCure coPy):

```
scp filename t1@pcn.t1.ws.afnog.org:/tmp/.
```

What did you notice? You should have noticed that you no longer get a password challenge to this account on this node, but rather you need to provide your RSA protocol 2 private key passphrase.

This is expected. SCP and SSH are from the same package - OpenSSH and both use RSA and DSA keys in the same way.

SSH - Lab Cont.

Example of a No Challenge Connection

We will now use ssh-agent and ssh-add to setup an environment on your machine where you can connect to your other machine, as root, without having to enter a password or passphrase at the time of the connection.

You will, however, have to enter your RSA protocol 2 private key passphrase once during this session. We'll discuss `ssh-add` and `ssh-agent` in class, but read "`man ssh-agent`" and "`man ssh-add`" for more details:

On the next slide you will setup your bash shell environment to contain your RSA protocol version 2 private key passphrase. This will allow you to connect, logout, reconnect, exit, connect again, and so on to root at the host you have chosen issuing your private key passphrase only *once:*

SSH - Lab Cont.

Example of a No Challenge Connection

Follow these steps to setup a "no challenge" connection:

```
ssh-agent /usr/local/bin/bash
ssh-add
ssh t1@pcn.t1.ws.afnog.org
```

What happened? You should have been prompted for your RSA version 2 protocol private key passphrase (remember, that's what is in ~/.ssh/id_rsa) when you typed `ssh-add`. Then, when you connected you did not need a passphrase. (If you have an RSA 1 key, you will be prompted for the passphrase for ~/.ssh/identity).

Now for the fun part. Logout, and log back in to the same session:

```
logout
ssh t1@pcn.t1.ws.afnog.org
```

Now what happened?

SSH - Lab Cont.

No Challenge Connection Notes

- ssh-add and ssh-agent have some slightly different behavior than just using ssh.
- If you don't specify a passhprase for your private key files when you create them, then you can truly connect with no password challend of any type - This is dangerous!
- Note that ssh-add defaults to ~/.ssh/id_rsa first then id_dsa.

SSH - Lab Cont.

Additional Notes

- You can use ssh-agent to “wrap” other programs that may need to use RSA/DSA authentication, but that cannot deal with multiple passphrase (or password) requests.
- The final Lab slides contain a complete session with notes of using ssh-agent and ssh-add.

SSH - Lab Cont.

ssh-agent/ssh-add session*

```
host5# where bash                              [Find where bash resides]
/usr/local/bin/bash
host5# ssh-agent /usr/local/bin/bash           [Wrap bash in ssh-agent]
bash-2.05a# ssh-add                            [Add rsa1 private key by default]
Need passphrase for /root/.ssh/identity
Enter passphrase for root@host5.t1.ws.afnog.org:
Identity added: /root/.ssh/identity (root@host5.t1.ws.afnog.org)
bash-2.05a# ssh-add ~/.ssh/id_rsa              [Add rsa v2 private key explicitly]
Need passphrase for /root/.ssh/id_rsa
Enter passphrase for /root/.ssh/id_rsa:
Identity added: /root/.ssh/id_rsa (/root/.ssh/id_rsa)
bash-2.05a# ssh root@host6.t1.ws.afnog.org  [Login with no password challenge]
Last login: Tue May  7 02:47:24 2002 from host5.t1.ws.afno
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
         The Regents of the University of California.  All rights reserve
FreeBSD 4.5-RELEASE (GENERIC) #0: Mon Jan 28 14:31:56 GMT 2002

------------------------------------------------------------------------
AFNOG 2002 Workshop -- Lome, Togo
------------------------------------------------------------------------
You have mail.
host6#
```

*Still relevant, but example if from May 2002 using SSH Version 3.1.

SSH - Lab Cont.

ssh-agent/ssh-add session

```
host6# exit                                                [Exit the shell session]
logout
Connection to host6.t1.ws.afnog.org closed.
bash-2.05a# ssh root@host6.t1.ws.afnog.org                 [Log back in - No password!]
Last login: Tue May  7 03:00:53 2002 from host5.t1.ws.afno
Copyright (c) 1980, 1983, 1986, 1988, 1990, 1991, 1993, 1994
        The Regents of the University of California.  All rights reserve
FreeBSD 4.5-RELEASE (GENERIC) #0: Mon Jan 28 14:31:56 GMT 2002

------------------------------------------------------------------------
AFNOG 2002 Workshop -- Lome, Togo
------------------------------------------------------------------------
You have mail.
host6# exit                                                [Exit the session again]
logout
Connection to host6.t1.ws.afnog.org closed.
bash-2.05a#
bash-2.05a# ssh-add -l                                     [Show rsa/dsa key fingerprints]
2048 7d:68:9b:55:0f:ba:6c:75:23:ab:36:fb:4c:a3:66:ea /root/.ssh/id_rsa (RSA)
bash-2.05a#
```

SSH - Lab Cont.

ssh-agent/ssh-add session end

```
bash-2.05a# ssh-add -d ~/.ssh/id_rsa                    [Remove a private key]
Identity removed: /root/.ssh/id_dsa (/root/.ssh/id_dsa.pub)
bash-2.05a# ssh-add -l                                  [List remaining keys]
bash-2.05a#
bash-2.05a# exit
exit                                                    [Exit ssh-agent bash shell]
host5#
```

Don't forget to read up on this with "`man ssh-agent`," and "`man ssh-add`" for many more options and details about how to use these programs.

Tunneling with SSH

The Topic You've Been Waiting For...

- You can use SSH to tunnel insecure services in a secure manner.
- SSH tunneling services includes authentication between known_hosts, password challenge, and public/private key exchanges.
- You can, even, indirectly tunnel via an intermediary machine.

Tunneling with SSH Cont.

The basic concept looks like this:

- Connect from one machine to another as `username`.
- Use ssh options to specify the port number on the remote machine that you wish to forward to the port on your local machine.
- Your ssh connection will *"tunnel"* data securely across ssh from the remote machine to your local machine.
- There are several options to be aware of.

Tunneling with SSH Cont.

Tunneling by Example

Here is a sample tunnel command using SSH under FreeBSD:

```
ssh -C -f username@host.domain -L 1100:localhost:110 sleep 10000
```

What is happening here?

- The '-C' option specifies compress the data. Good on modems, bad on fast networks.

- '-f' means ssh goes to the background just before executing the specified command listed (in this case, “sleep 10000”).

- '-L' forwards the port on the left, or client (1100) to the one on the right (110) or remote side.

Tunneling with SSH Cont.

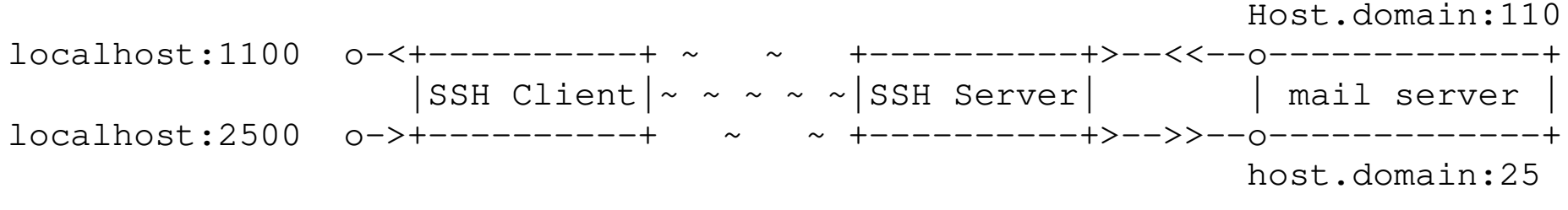
Tunneling by Example Cont.

So, what does this command do?

```
ssh -C -f username@host.domain -L 1100:localhost:110 sleep 10000
```

- This “tunnels” your POP email from port 110 on the remote side through port 1100 on your local side.
- The process backgrounds for 10000 seconds (detaches and runs).
- This is done under the authority between yourself (client) and user@host.domain.

Diagram* of Tunneling *both* smtp and POP Services



*Thanks to http://www.ccs.neu.edu/groups/systems/howto/howto-sshtunnel.html

Tunneling with SSH Cont.

Tunneling by Example Cont.

Why use something like ports “1100” and “2500”?

- Ports up to 1024 can only be reset by the root user.
- If you are root you can forward 110 to 110, 25 to 25, and so on.
- Other popular tunneling tricks include tunnels for XWindows, IMAP, etc.
- On the client side you must set programs to use “localhost” - For example, for POP and smtp, your mail client must use “localhost” instead of host.domain (i.e. no more “mail.host.com”).
- If you are not root, and your ports are changed, then your mail client must be able to set the smtp and POP ports as well.
- **We'll show this using Sylpheed under Linux right now...**

Tunneling with SSH Cont.

One More Tunneling Example

You can use SSH to do "Indirect Port Forwarding"

- What to do if your organization's email sits behind a firewall?
- Connect via an intermediary box (gateway).
  Here's a real world example:

```
Ssh -C -f hallen@gateway.turbolinux.com -L 2500:mail.us.tlan:25
-L 1100:mail.us.tlan:110 /bin/sleep 10000
```

Tunneling with SSH Conclusion

- Tunneling lets you securely access basic services such as POP and IMAP.
- You can securely tunnel ports using SSH.
- You can use /etc/services to verify you are not using a port that is already defined.
- Only root can redfine ports below 1024.
- You can tunnel ports directly between two machines, and indirectly with a machine in the middle.

SSH Conclusion

SSH and SCP are two great tools for connecting between machines and copying data while helping to maintain a secure environment.

If you can, we recommend you remove telnet and FTP from your system. Or, at most, only allow anonymous FTP access.

You can use SSH to tunnel ports securely that would otherwise pass your information (username, password, and session data) in the clear.

Remember - Use the references for more detailed information. This includes "`man ssh`" and "`man sshd`" for much more information.