

SSH Tutorial: UNIX Quick Guide

Last Updated Monday, 08 January 2007

What is SSH?

SSH is a protocol used to communicate with remote systems from a local host. It is different from other protocols(such as telnet) in that it uses keys generated by the local and remote hosts to encrypt the messages to prevent certain security risks such as a "man in the middle" attacks, spoofing and many other hacking techniques. Basically, SSH is a protocol that protects your computer as well as the remote host from possible security risks.

For a more detailed explanation of what SSH is, how it works and why you should use it, read Scott D. Brown's [SSH HowToSsh](#)

Connecting to a Remote Host

Usage for ssh is as follows (per UNIX man page):

```
$ ssh [-l login_name] [ hostname | user@hostname ] [ command]
```

I'll show a couple ways to use ssh, both work just as well. In these examples I am logged into one of the center's UNIX machines and am trying to ssh into my account on the Computer Science machines. The following is what is entered and returned from the command prompt.

```
$ ssh -l djh6585 hilly.cs.rit.edu
```

```
The authenticity of host 'hilly.cs.rit.edu (129.21.30.36)' can't be established.  
RSA key fingerprint is 65:50:c5:60:14:df:56:83:3c:7a:02:72:37:21:aa:f9.  
Are you sure you want to continue connecting (yes/no)?
```

```
djh6585@hilly.cs.rit.edu's password:
```

It's as simple as that. You will be asked to save a key to a local database if it is the first time using ssh to access a particular remote host. It will not force you to save it, but it is recommended to assure the authentication of the remote host. After answering yes or no to this question, it will prompt you for the password and then log you

in.

Another way to do the same thing is to enter the following in the command prompt:

```
$ ssh djh6585@hilly.cs.rit.edu
```

To log off after using ssh to login simply exit:

```
$ exit
```

Using scp(secure ftp)

Scp is similar to the UNIX command cp except that it can be used between remote hosts to transfer files securely. It works alot like the ssh program. The general format for transferring a file is as follows:

```
$ scp username@hostname:file destination
```

Where file can be a directory path. The follwing is an example of me copying a picture from my Computer Science account to the current directory on my CIS account (which I am currently logged into).

```
$ scp djh6585@hilly.cs.rit.edu:Courses/CV/HW2/TextImage.tif .
```

djh6585@hilly.cs.rit.edu's password:

```
TextImage.tif                100% 304KB 304.0KB/s  00:01
```

It will prompt me to save the key if I don't have it saved, just like the ssh in the previous section. In this case I already have the key saved so it does not ask me. It then asks me for a password. It then opens a connection to the remote host, transfers the file as asked and closes the connection telling you how much was displayed and how

long it took.