SSH Fingerprinting

Did you receive a message from SSH saying "it is possible that someone is doing something nasty?" Wondering what's going on?

Each time you use SSH to connect to a remote server, your computer verifies that server's identity. The purpose of this check is to ensure that no one is impersonating that server and could potentially intercept sensitive info. (e.g. Criminals could potentially do something like run a free WiFi network that intercepts everyone's connections and attempts to gather their personal data and/or passwords.)

Your computer is telling you that the identity (fingerprint) of the system to which you're connecting has changed since the last time you tried to connect to it.

You can verify that the fingerprint your computer is seeing is correct by logging into the server from a different system (e.g. a lab computer on-campus) and running this command:

```
tdobes@linux2:~$ ssh-keygen -lf /etc/ssh/ssh_host_ecdsa_key.pub
256 SHA256:W8rbGZbIv57nNbbtCKF7FKMoqR0Wblw6lWzrh93HiyQ root@linux2 (ECDSA)
```

(Note that you may need to swap out `ssh_host_ecdsa_key.pub` with the filename for the appropriate key that your computer is has identified. For example, on an older system you might want `ssh_host_rsa_key.pub` instead.)

If the fingerprint you obtain with that command doesn't match what you see on your computer when connecting using ssh, it's likely that your traffic is being intercepted somehow. One common instance in which this can happen is if a free and/or commercial WiFi providers use a "captive portal", which is supposed to send your web browser to an internal web page that asks you to log in or agree to their terms of service. To accomplish this, they instruct your computer to send any attempt to connect to any address to their server that provides that web page. This works for web browsers since you'll end up seeing their page and can proceed by logging into their portal. However, for SSH, it means that you end up trying to connect to their server (which doesn't work, of course). It's also possible that something more problematic is occurring, such as an untrustworthy ISP or WiFi provider attempting to intercept your traffic.

On the other hand, if the fingerprint you see on your computer actually matches what's currently on the server, then the problem is either that the server's key/name/IP has changed or that your computer connected to the wrong server in the past. You might see this if the server was recently moved or rebuilt, which caused the key's fingerprint to change. It's also possible that your computer connected to the wrong server at some point in the past (for example, as a result of the captive portal scenario described above), and your computer is just remembering the wrong key.

If that happens, Basically, you just need to tell SSH to forget about the old server. To do this, you can delete the line(s) with the problematic key in the file `~/.ssh/known_hosts` – Recent versions of ssh provide us with a handy command line tool to do that. You can just run this command:

```
ssh-keygen -R {servername}
```

(substitute {servername} for the name of the server in question, such as linux.cs.uchicago.edu) This command will search the file for any lines pertaining to {servername} and delete them. Then, you can run the normal ssh command to reconnect and your computer will act as though it's seeing the server for the first time (asking you to verify the fingerprint, then connecting you as expected).