What to do When you get a Warning Message Connecting to CSIL/Linux

When you are using remote login or SSH, you will occasionally see warning messages, do not panic. Carefully read the warning message, often times instructions on how to resolve the issue are listed in the warning message.

Step-by-step guide

1. First determine the severity of the message. From least severe to most, messages can be informational, warning, and error.
2. Second determine steps to take to fix the issue, does the error message explain how to fix the error or give a code to look up?

Common Error Types

There are three common error messages that you will likely encounter. They are "spoofing" errors, "connection" errors, and "untrusted/misconfigured" errors

Spoofing Error Example

Example of the error message

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@ WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!      @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
```

Solution: What to do when you get an SSH Error connecting to CSIL/Linux

This message is generated when you try to ssh to a remote host and the remote host settings, identification and/or operating system does not match what is in your computer's records. While this is a good security warning to pay attention to in most circumstances, it can also generate unneeded warnings.

Connection Error Examples

```
ssh: connect to host csil.cs.ucsb.edu port 22: Connection timed out
```

Solution: Check for typos then try another computer

This is essentially either a busy signal or a "computer does not exist" signal. Computers have limited processing power. If more than 6 normal users attempt to sign into a single CSIL computer at any time you will start seeing this message. Until someone signs out, you will not be able to sign in. The same error also shows up if a computer does not exist. If you attempt to sign into csil-49.cs.ucsb.edu you will get this error because there are only 48 CSIL computers. Always check for typos before entering a command in terminal. See: What are the names of the CSIL machines?

```
ssh: connect to host csil.cs.ucsb.edu port 22: Connection refused
```

Solution: When you are trying to connect to...

This message means you are being blocked by the computer's firewall. The most common reason is because you had too many failed logins.

Untrusted Error Examples

```
Warning: untrusted X11 forwarding setup failed: xauth key data not generated
Warning: No xauth data; using fake authentication data for X11 forwarding
```

Solution: check your connection command then check your settings.

This is related to flags you can declare when you try to ssh. Two common flags are -X and -Y

Both options have to do with X11 forwarding which can be enabled on the CSIL computers. This means if you enable X11 on the non-CSIL computer, you can use a graphical client through your SSH session (i.e. use the matlab GUI instead of only the command line).
If you use `ssh -X remotemachine` the remote machine is treated as an untrusted client. So your local client sends a command to the remote machine and receives the graphical output. If your command violates some security settings you’ll receive an error instead. This is the preferred/default setting for most programs due to security concerns.

But if you use `ssh -Y remotemachine` the remote machine is treated as trusted client. This last option can open security problems. ONLY DO THIS IF YOU TRUST THE REMOTE MACHINE Because the other graphical (X11) client can sniff data, take screenshots, do keylogging and other nasty stuff, this setting is not enabled by default on most machines.

If you ssh into CSIL, have X11 enabled and do not use one of the above flags, you might get the above warning message. It is simply the computers way of saying that it failed to set up untrusted X11 forwarding because the settings on both ends do not match.

### Untrusted Error: permissions variant

```
$0000000000000000000000000000000000
  WARNING: UNPROTECTED PRIVATE KEY FILE! 0
$0000000000000000000000000000000000
Permissions 0644 for '/cs/student/yourusername/.ssh/id_rsa' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
```

Solution: check your permissions on your private key and authorized_keys files

Some operating systems create files that by default are world readable, this is generally not a good security practice and should be changed.

**Note**

Please be aware that you want your keys to be as secure as possible. Just as you do not give other people your passwords, you should not let other people read your keys.

First navigate to the file listed in the error message, for the above example that will be '/cs/student/yourusername/.ssh'.

You will then want to use the command `ls -al` to see your current permissions.

Permissions will be in three groups, in order:

- owner: who owns the file
- group: groups the owner belongs to, for example student
- world: everyone else on the entire planet who is not covered by the first two sets of permissions

Permissions will also be in three types:

- `r` for read permission:
- `w` for write permission:
- `x` for execute permission.

It is also possible to have permissions represented by a number 0 to 7 with 0 being no permissions (---) and 7 being all permissions (rwx)

example commands to set world permissions to "0" no read, write, or execute permissions while leaving owner with "6" read and write permissions.

```
$ chmod 650 authorized_keys
$ chmod 600 id_rsa
```

**Related articles**

- What to do When you get a Warning Message Connecting to CSIL/Linux
- Setting up SSH Keys
- How to do X11 Forwarding on a Mac
- My email bounced back with an error...
- How can I access my UNIX account from windows?