How to get, install, configure and use the Windows ssh client

- What is ssh?
- Getting and installing the Win ssh client
- Configuring the Win ssh client
- Generate a public/private keypair on the client
- Generate a public/private keypair on fisher

What is ssh?

- The ssh secure shell (ssh client on either win or linux platforms) is a program that allows secure network services over an insecure network, such as the internet.
- It allows you to
  - ⋆ securely login to remote host computers
  - ⋆ execute commands safely on a remote computer
  - ⋆ provide secure encrypted and authenticated communications between two hosts in an untrusted network
    - ∗ secure ftp (file transfers)
    - ∗ secure tunneling
- It requires ssh server/client and public/private keys to encrypt and decrypt all communications (client gets server's public key at first communication).
- It operates on TCP port 22

  - ftp is on port 21
  - telnet — 22
  - smtp — 25
  - http — 80
  - pop3 — 110
  - imap — 143
  - https — 443
- Our servers fisher.stats.uwo.ca and karl.stats.uwo.ca allow only TCP ports 22, 80, 443 to be accessed from outside our departmental domain.
- Most networks allow only ssh access
  - All SHARCNET access must be through ssh
  - http://www.sharcnet.ca
  - Graduate students can get their accounts through online application

Getting and installing the Win ssh client

- The University of Western Ontario has a site license for the Windows client.
- Get it at http://www.uwo.ca/its/sitelicense/ssh.html
- Or get it at http://www.ssh.com
- Once downloaded, install it by double clicking the exe file.

Configuring the Win ssh client

- Use "Quick Connect" to login a remote site

- Accept remote site public key
- Create a profile to the remote site
- Create a link on desktop
- Edit a profile
- Create tunnels

Generate a public/private keypair on the client

- Go to "Edit > Settings"
- In Global Settings > User Authentication > click on the "Keys" tab.
- Under Key pair management > click on "Generate New...".
  - ⋆ Use defaults (click "Next" or "Yes")
  - ⋆ In "Enter Passphrase", choose a proper file name (userid) and leave "Passphrase" empty.
  - ⋆ Click on the 'Upload public key' button (assuming that you login a remote site).
  - ⋆ Change the Destination folder to ".ssh" and leave both the Public Key file and Authorization file at their default settings.
- Convert your public key to the remote host.
  - ⋆ On the server, the OpenSSH daemon is looking for keys in a file called .ssh/authorized_keys in your home directory. We need to move the public key you just uploaded (/.ssh/userid.pub) into a format readable by OpenSSH.

- From your home directory, run this command:
  ssh-keygen -i -f .ssh/userid.pub >>.ssh/authorized_keys
- When you login next time, you should not need to enter your password.

Generate a public/private keypair on fisher

- ssh to fisher
- On fisher, run
  - mkdir -p $HOME/.ssh
  - chmod 0700 $HOME/.ssh
  - ssh-keygen -t dsa
  - cat id_dsa.pub >> $HOME/.ssh/authorized_keys
  - chmod 0600 $HOME/.ssh/authorized_keys