

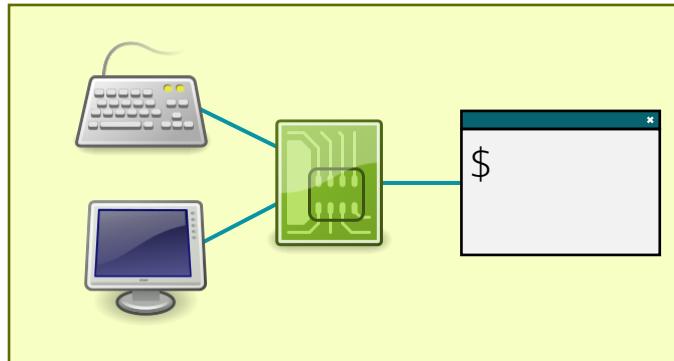
SSH: Secure Shell

COMS10012 / COMSM0085

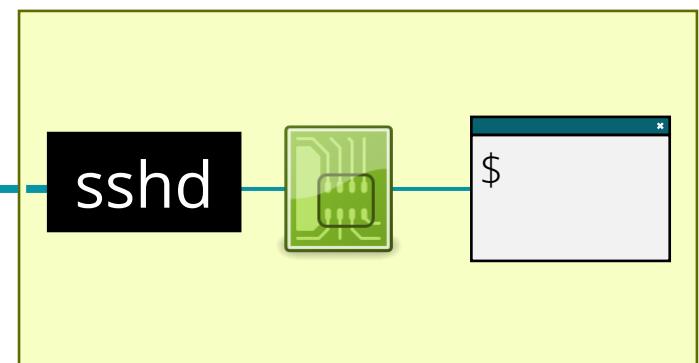
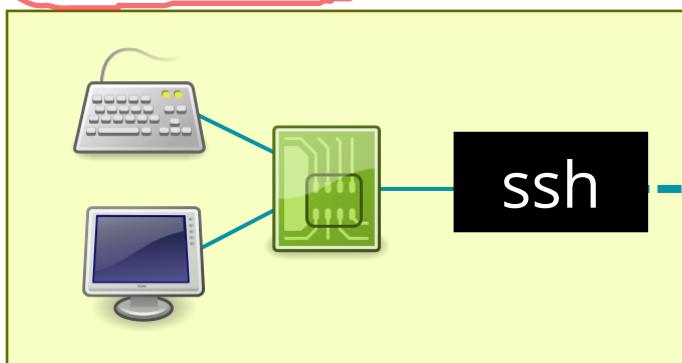
Software Tools

Shell

local



remote with ssh



syntax

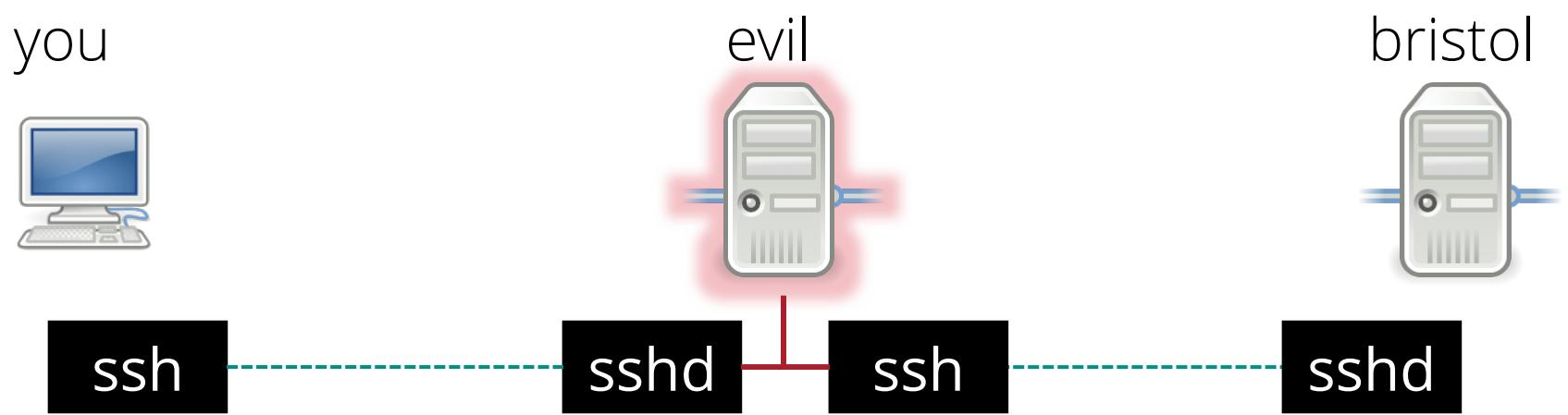
```
$ ssh [USERNAME@]HOSTNAME
```

ssh me23202@seis.bristol.ac.uk

...

Are you sure [y/n]?

man in the middle



cryptography

- SSH servers have a key pair for digital signatures.
- If you connect to a new server, SSH asks you if you're sure.
- If you connect to a server and the key has changed, you get a warning.

keys

You can create your own key too.

- convenient: you don't have to type your password anymore.
- secure: key never leaves your machine, even if you connect to an evil server.

Details in the exercises ...

servers

ssh me23202@seis.bris.ac.uk

me23202是username

seis.bris.ac.uk是hostname

seis.bris.ac.uk

bastion host, accessible from internet, but
doesn't have your files or programs

rd-mvb-linuxlab.bristol.ac.uk

load balancer, connects you to a lab machine

it#####.wks.bris.ac.uk

lab machines, # = 075637 to 075912.