Secure SHell (SSH)

Dr Peadar Grant

February 7, 2024

Contents

1 Shell

The shell is the program we normally interact with in a command-line interface. Examples: PowerShell, Bash, Korn Shell, C Shell. We will return to more details of shell interfaces later on.

1.1 Key concepts

Prompt shows when shell is waiting for input.

Current working directory where commands will read and write files relative to.

Path: list of folders searched for matching command name

1.2 Navigation

In the command-line environment we navigate the exact same set of folders as we see in the File Explorer / Finder. Some hints on navigation (applies to PowerShell and Bash):

```
# print out the folder you're in (i.e. the working directory)
pwd

# list out the contents of the folder you're in
ls
dir   # on windows
ls -l # detail, linux/mac only

# change to a sub-directory of where you are now
cd movies

# directly change to a sub-sub-directory
```

```
cd movies/horror

# change to the parent directory
cd ..

# change to your home directory
cd ~

# change to a known sub-dir of your home directory
cd ~/Desktop

# change to a sub-dir of the parent dir
cd ../music
```

It is essential in command-line environments that you are comfortable navigating around the filesystem.

1.3 Features

History: list of previous commands recalled (usually the up arrow key).

Redirection using *operators*

1. Standard input to a file.
2. Standard input from a file.
3. Piping the standard output of one command to the standard input of another.

Scripting a sequence of commands to be performed.

Variables to capture and recall information.

Control constructs including conditionals, loops, possibly exceptions.

2 Terminal

The shell itself is normally accessed by means of a terminal. This is the program we visually see like the PowerShell Application or XTerm in Linux that encapsulates the terminal program with the GUI environment. Examples of terminals:

GUI terminals like Windows Terminal, XTerm, Terminal.app

Framebuffer console on Windows when the GUI is not running.

Serial console over a serial port (often seen on embedded devices).

Remote network terminals using telnet or more usually SSH.

3 Secure Shell

SSH is a way to for one computer to connect to another's command-line interface in a secure fashion.

SSH clients are included in most common operating systems. Client apps available for mobile.

An SSH client connects to an SSH server. The SSH server normally makes the command-line interface of the OS available (e.g. bash, powershell):

- All modern UNIX/Linux operating systems come with SSH servers as standard.
- Windows 10 onwards and Windows Server now have SSH servers included but need some configuration to get working.

SSH is relatively easy to get started with — the complexity often comes later when features like key-based authentication, multi-factor authentication, port forwarding and other extras are employed.

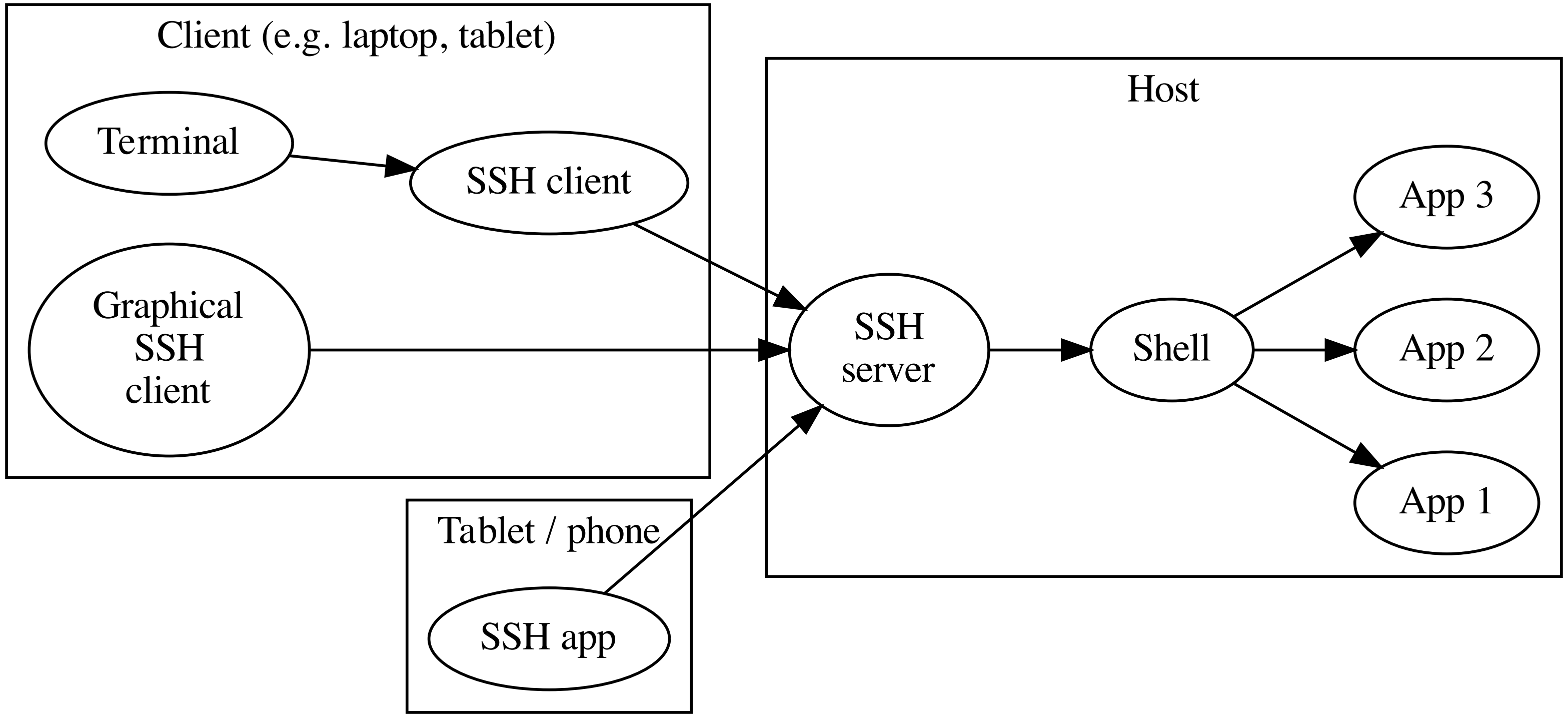
Client (e.g. laptop, tablet)
Terminal
SSH client
Graphical SSH client
Tablet / phone
SSH app
Host
SSH server
Shell
App 3
App 2
App 1

Figure 1: SSH

4 SSH client

Most operating systems use the OpenSSH client, named `ssh`, that is available on the command-lin

4.1 Connecting

To connect to a remote machine, we need to know its name or IP and the username to connect as:

```
# connect via IP
ssh peadar@192.168.0.1

# connect via name
ssh peadar@compute-server.dkit.ie

# connect using same username as on client
# just leave off the username before @ symbol
ssh 192.168.0.1
ssh compute-server.dkit.ie
```

4.2 Host verification

The first time you connect to a host you'll get a warning:

```
The authenticity of host '54.78.220.233 (54.78.220.233)' can't be established.
ECDSA key fingerprint is SHA256:8omkD5RLibZNgJJ/B7MAnL7IbEcrmCmIWFdQXbjJf60.
Are you sure you want to continue connecting (yes/no)?
```

Just type `yes` here:

- Your local SSH client is just confirming it hasn't seen this machine before.
- If a different key fingerprint shows for the same IP you'll get a warning, which means a host has been changed for another.

4.3 Authentication

SSH supports a number of different authentication schemes:

- A server may permit or require multiple authentication methods.
- Simplest is **username** / **password**.
- SSH often used with **Key Pairs** (later on).
- Other authentication methods:

  Authenticator apps like Google Authenticator.

  Kerberos where Windows AD can “pass through” authentication from client.

4.4 Usage

If you see something like the following (on Linux) then you’re connected:

```
       __|  __|_  )
       _|  (     /   Amazon Linux 2 AMI
      ___|\___|___|

https://aws.amazon.com/amazon-linux-2/
2 package(s) needed for security, out of 13 available
Run "sudo yum update" to apply all updates.
[student@ip-10-0-1-80 ~]$
```

What will actually appear will depend on what type of host you are connecting to.

5 Key-based authentication

SSH key pairs are an alternative to a username/password. They consist of:

Private key kept on the client and securely stored.

Public key on the server(s) you want to log in to. (The public key can be freely shared around, even put up in public.)

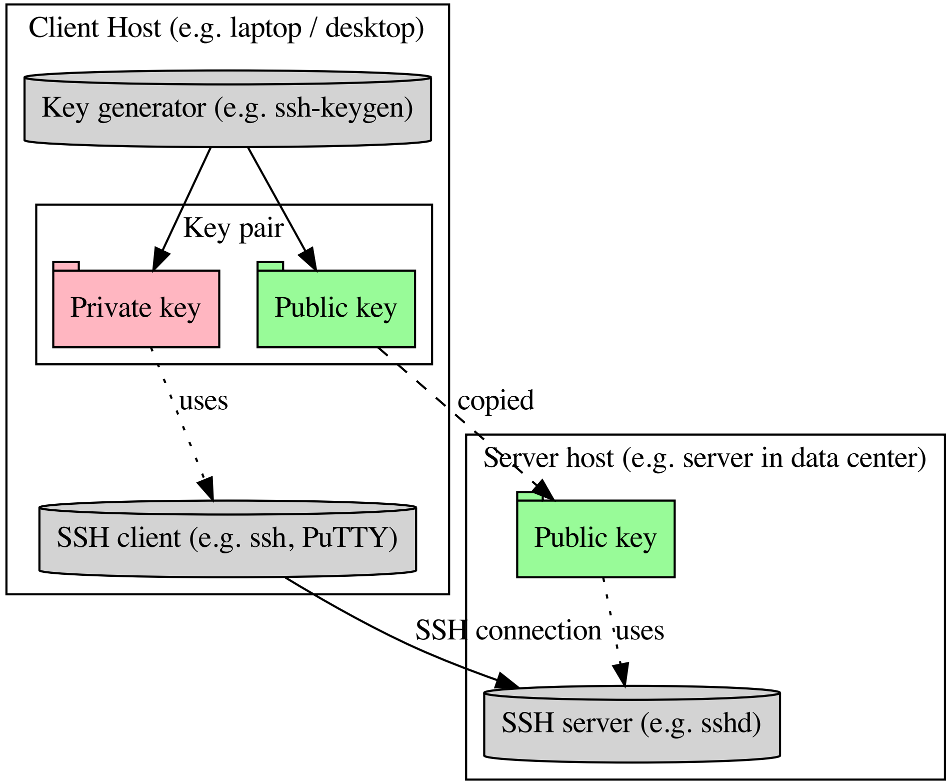
Client Host (e.g. laptop / desktop)
Key generator (e.g. ssh-keygen)
Key pair
Private key
Public key
uses
copied
Server host (e.g. server in data center)
Public key
SSH client (e.g. ssh, PuTTY)
SSH connection
uses
SSH server (e.g. sshd)

Figure 2: Key-based authentication

5.1 Creating key pair (mac, linux, windows 10 onwards)

Key pairs are normally and ideally created on your own local client computer. Key pairs only need to be generated once. (If you already have a key pair created, you can skip on ahead...)

To create an ED25519 key pair, in Powershell/Bash type:

```
ssh-keygen -t ed25519
```

You can optionally use a passphrase to encrypt the key pair or leave it blank for easier usage.

5.2 Default key locations

The key pair is then stored in two files in your home directory (same for Mac, Linux, Windows). You can find them by changing into the `.ssh` directory and listing the contents of it:

```
cd .ssh
dir
```

From the directory listing:

```
Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-a----       16/10/2020     15:19           3243 id_ed25519
-a----       16/10/2020     15:19            749 id_ed25519.pub
```

The public key is stored in `id_ed25519.pub`. The private key is stored in `id_ed25519`.

You can of course copy these files to/from a memory stick or online storage. Remember though that if your private key is compromised, anybody can use it. Best to protect it with a passphrase!

5.3 Connecting over SSH with keys

In PowerShell/Bash we can use the SSH command to connect to the SSH server on a remote host:

- This will then present us with a new shell on the remote computer (Bash for Linux/UNIX, PowerShell for Windows).
- By default, SSH will try all private keys in `.ssh` so we don't need to specify which.

```
ssh student@$publicIp
```

5.4 Using specific key

We can force the use of a specific key using the `-i` option:

```
ssh -i private_key_file_name_here username@host
```