Secure SHell (SSH) basics

Dr Peadar Grant

September 22, 2021

1 Secure Shell (SSH)

SSH is a way to for one computer to connect to another's command-line interface in a secure fashion. It is widely used both in cloud-based and non-cloud environments for remote access.

SSH clients are included in most common operating systems. You can also get SSH client apps for iOS and Android.

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 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 authenticatio multi-factor authentication, port forwarding and other extras are employed.

1.1 SSH client

Most operating systems use the OpenSSH client, named ssh, that is available on the command-line. To connect to a remote machine, we simply supply 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 username on client
ssh 192.168.0.1
ssh compute-server.dkit.ie
```

2 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.)

2.1 Creating key pair (windows 10, mac, linux)

Key pairs are 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 ???.

To create a 4096-bit RSA key pair, in Powershell/Bash type:

```
ssh-keygen -t rsa -b 4096
```

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

```
    Directory: C:\Users\peadar\.ssh


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----       16/10/2020     15:19           3243 id_rsa
-a----       16/10/2020     15:19            749 id_rsa.pub
-a----       16/10/2020     15:32            176 known_hosts
```

The public key is stored in id_rsa.pub. The private key is stored in id_rsa.

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.