How to create a SSH keypair (a pair of public/private keys to use for SSH authentication)

Introduction

The most common way to authenticate to a UNIX-like system (*e.g.* Linux, Mac OS, *BSD, etc.) when using the SSH protocol is via standard credentials: the username and password associated to the system user.

This authentication method is not the best from the point of view of security, since an exposed password access can be the target of sophisticated attacks, and a password which is not strong enough can be easily cracked, and the system compromised.

Another (much more secure) authentication method, which makes no use of passwords, is based on a couple of *keys* (*i.e.* a key pair).

How it works

The aforementioned keys are:

- a **private** key, which **must never be shared with anyone, nor put on any storage support accessible via network**
- a **public** key, which can be known by anyone

Such keys work as a lock (the public key) and a key (the private key): whenever an account is secured with the lock (the public key), whoever owns the (private) key can enter.

Concretely, in a UNIX-like system (which we call *e.g.* server.example.com), the public keys are stored in the user's `$HOME/.ssh/authorized_keys` file, one per line. When one tries to connect to the system via SSH

How to create a key pair

A keypair can be created executing the `ssh-keygen` command in a BASH/ZSH (the standard shells in UNIX-like systems and in the Windows Subsystem for Linux (WSL) in Windows) **on the client**, answering to the prompted questions (the default answers, *i.e.* the one obtained by pressing the return button to all questions, are fine). The following is an example:

```
$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key ($HOME/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
```

```
Enter same passphrase again:
Your identification has been saved in $HOME/.ssh/id_rsa.
Your public key has been saved in $HOME/.ssh/id_rsa.pub.
The key fingerprint is:
SHA256:YHUT239POA6FuRGK2rVBixAhKFfwTzZtkLunIRGM3Ps
<USERNAME>@server.example.com
The key's randomart image is:
+---[RSA 2048]----+
| ..Bo =+. =..    |
|. =.+..= = * +   |
| o  .o*.= * = .  |
|    o=.* . o = . |
|     oo.S . o + o|
|    . E .    o +.|
|     . +      . .|
|      .          |
|                 |
+----[SHA256]-----+
```

The above command (with the default answers to the prompted questions) generates two files in the `$HOME/.ssh`:

- `$HOME/.ssh/id_rsa`, containing the **private** key
- `$HOME/.ssh/id_rsa.pub`, containing the **public** key

One must then transfer the copy of the `$HOME/.ssh/id_rsa.pub` (the public key) inside the `$HOME/.ssh/authorized_keys` file (in a single line) **on the server**.

The following is an example of a public key (`id_rsa.pub`) generated with the above procedure (which can be visualized with the command `cat $HOME/.ssh/id_rsa.pub`; please remember that the key must always be contained in a **single** line):

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCxESaVn6tW5yjSjWSsfkX21WiprCOG4czCH82tScqvqG
mxzOHB6wY/phknZ8U7MM8PzahX4SmnR2x3wAqJ2GqMa1ygJRChuYmn9aQW/It21I0qeI9DcTWS
hBkMRY2u+p+6iud8qegDdpdMMDNzGbfrW7qtIPpPWQ669JYmhkY6EvEIr9UzCTvH8ky7PmVtNL
JXljrNgdjVg2GMpHxdHV/oaxYNEqYaccCGX7xSxN8sivemrbOTe3PStrEAP2GYPfE6ymA6vUKy
87NE0tFfZWRucygOEnZ36X2oES6PnSF9ONWit58/8963GEK7nAR1He+WgUHxOoRVdG1M/oedow
Kv <USERNAME>@<CLIENT>
```

Where the corresponding private key (`id_rsa`) is (which can be visualized with the command `cat $HOME/.ssh/id_rsa`; please note that it is **not** contained in a single line):

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAsREmlZ+rVuco0o1krH5F9tVoqawjhuHMwh/NrUnKr6hpsczh
wesGP6YZJ2fFOzDPD82oV+Epp0dsd8AKidhqjGtcoCUQobmJp/WkFvyLdtSNKniP
Q3E1koQZDEWNrvqfuornfKnoA3aXTDAzcxm361u6rSD6T1kOuvSWJoZGOhLxCK/V
Mwk7x/JMuz5lbTSyV5Y6zYHY1YNhjKR8XR1f6GsWDRKmGnHAhl+8UsTfLIr3pq2z
k3tz0raxAD9hmD3xOspgOr1CsvOzRNLRX2VkbnMoDhJ2d+l9qBEuj50hfTjVoref
```

```
P/PetxhCu5wEdR3vloFB8TqEVXRtTP6HnaMCrwIDAQABAoIBAD4eljrH2YSTdG7p
y/f4FPOTyzQ7f/tCHGO+ZJn22XTm0K3gAxPVMEwEKa75aOhrJzmUHQs3ozVciWE5
rnjNxBOfVs+YMU2Lmg+izf6CeyslRqEvypMOlIziaycy/5HzuzXmpW/G6+7LHClO
f75Rt4SKmeNDPo234MMWK9c4JEsa5DH12pbJLnevaQ2gqzPSA599+rxtFAJhC0zB
u1zbJZpoce/OV4Zu/YH8/IR1GYhBX/6F3eRig0IXiE52G2p8WKhoqF5JyQeNE/qq
M8AxUAyev9xfU8Ail6clh6a06/o1fSxsGUEPsETKtkriPW0HmIxJdzor9dE7FvMS
ZBq2r4ECgYEA5weuazCXu6N1TZ4G8s0gxNvAsOupRBbJa8brpUNrgxFvQC9ZcMbB
NTj4nq0zZKRJMifbNOFVDGz67ewTgU5XmwCt/Dudluf2GksYi450/+F7igTI51Vf
BMpd9mWYwMmx6v6vM9jy61sTUgQSXrUjGD26bEb9YA0spurabn6YQJ0CgYEAxDRg
8LpAReDQt+M1vwBPKxtCc60G5RiipfxyYYmtj0h8f+gNkbun8vlguBX2VVQdsYs6
N62xGMhOzBj/w2wElk7C84HcbW0Jwu6z4IMIFXm9lHh2GFDJ/A2nS/sGIRyeWZsz
SkxcJedjPF4wqJvCe+nEesS/XmPiI5NiXs9KELsCgYEAqv4acCeFBlITLiF6TxbX
3Bwx4EBsBYNADU8rdiQSXO34g28IKdpRggzqprbWxPR7YG3zZo4onovCpXoHbbsI
SCcWnwuYtep1UjymrBQCMKk5AIxODjo3m5oUNZw4lOgzkRRzpFI8aUn9YMS2u/Yh
RX3aju1z9zWJCPnmNcXo9lkCgYB/rG3gd/JXBmILJwjUT0k1DboCN/eioJNGW626
lrKf6FVLjh82U9yIGYq8f14aTHA+FhE+JgJ10/KikSntap7ZiEsH1dswQaH2fQoD
8IAUKXIZ6QE/9WJaaDATGzfz2AGa4YlQsbvM1nMW11vme+TkaUv3b4vvyiNfbwq2
E0Fo/QKBgQC8Coqkb8ukvdW1gSmoUm6g+CEnmbTSxD6A7+2SRuBc/+3rWg1dVXkJ
ONoRKsi137v6u/+vThHIiDOXVisxiD7IFwaV4jVzzfYRQqsJOJYP5P/6u2ltycuB
kzfLjSKGVZkk1Q1B6EZg7ZTXxyvHR9CRPAZ03HNCVa67VV7DXEaoIQ==
-----END RSA PRIVATE KEY-----
```

How to connect to a server via SSH using a key pair

One can connect to the server via SSH executin the following command **on the client**:

```
ssh -i <PATH_TO_PRIVATE_KEY> <USERNAME>@<SERVER>
```

replacing

- `<PATH_TO_PRIVATE_KEY>` with the (absolute or relative) path to the file containing the **private** key on the file system of the client
- `<USERNAME>` with the username of the user on the **target** system (*i.e.* **on the server**)
- `<SERVER>` with the *fully qualified domain name* (FQDN, *e.g.* server.example.org) or the IP address **of the server**

The system will then ask for the passphrase, if one has been set up when creating the key pair, otherwise access to the server will be granted directly.

Please notice that many UNIX-like systems automatically try to use the private keys stored in the user's `$HOME/.ssh` directory when connecting to a remote server via SSH.

Troubleshooting

It can happen that the server answers with a `Permission denied (publickey)` message when one tries to connect. This can happen for different reasons:

Wrong private key

If one tries to connect to the server using a private key not corresponding to the one copied inside the `$HOME/.ssh/authorized_keys` file, the system will deny access. If this happens, **one must make sure to use the correct key, specifying it with the `-i` flag of the `ssh` command**:

```
ssh -i <PATH_TO_PRIVATE_KEY> <USERNAME>@<SERVER>
```

replacing

- `<PATH_TO_PRIVATE_KEY>` with the (absolute or relative) path to the file containing the **private** key on the file system of the client
- `<USERNAME>` with the username of the user on the **target** system (*i.e.* **on the server**)
- `<SERVER>` with the *fully qualified domain name* (FQDN, *e.g.* server.example.org) or the IP address **of the server**

File and directory permission

Please notice that (on the **server**) the `$HOME/.ssh` (hidden, as it starts with a `.`) directory must have `drwx------` (or `700`) permissions, while the `$HOME/.ssh/authorized_keys` must have `-rw-------` (or `600`) permissions. These permissions can be set executing the following commands on the server (server.example.com in the previous example):

```
$ chmod 700 $HOME/.ssh
$ chmod 600 $HOME/.ssh/authorized_keys
```

Moreover, the `$HOME/.ssh/id_rsa` private key (on the **client**) must have the `-rw-------` (or `600`) permissions, which can be set executing the following command:

```
$ chmod 600 $HOME/.ssh/id_rsa
```