SSH

Luciano Sampaio
lsampaioweb@gmail.com

What Is ssh-keygen?

- ssh-keygen is a tool for creating new authentication key pairs for SSH. Such key pairs are used for automating logins, single sign-on, and for authenticating hosts.

Algorithm and Key Size

- rsa - an old algorithm based on the difficulty of factoring large numbers. A key size of at least 2048 bits is recommended for RSA; 4096 bits is better.

- dsa - an old US government Digital Signature Algorithm. It is based on the difficulty of computing discrete logarithms. A key size of 1024 would normally be used with it. DSA in its original form is no longer recommended.

- ecdsa - a new Digital Signature Algorithm standarized by the US government, using elliptic curves. This is probably a good algorithm for current applications. Only three key sizes are supported: 256, 384, and 521 (sic!) bits. We would recommend always using it with 521 bits, since the keys are still small and probably more secure than the smaller keys (even though they should be safe as well).

- ed25519 - this is a new algorithm added in OpenSSH. Support for it in clients is not yet universal. Thus its use in general purpose applications may not yet be advisable.

Generate your SSH key

- ssh-keygen -t rsa -b 2048 -f file
- ssh-keygen -t dsa
- ssh-keygen -t ecdsa -b 521 -f file
- ssh-keygen -t ed25519

Sharing your key

- Only copy the public key:
  - ssh-copy-id -i ~/.ssh/key user@host

Connect using SSH

- Specify ssh key if not the default:
  - ssh -i ~/.ssh/key user@host

Specific config for a host

- cat ~/.ssh/config
- Host DUD-Jump-Server
  - HostName DUD-Jump-Server
  - User lsampaio

- Host switch-01.homelab
  - HostName switch-01.homelab
  - HostKeyAlgorithms +ssh-dss
  - KexAlgorithms +diffie-hellman-group1-sha1
  - Ciphers aes128-ctr,aes192-ctr,aes256-ctr,aes128-cbc,3des-cbc
  - IdentityFile ~/.ssh/key

References

- How to Use ssh-keygen to Generate a New SSH Key?
- https://www.ssh.com/academy/ssh/keygen

Questions ?

Thank you!

Luciano Sampaio
lsampaioweb@gmail.com