SSH: Keys, Agents, & more

Jaxon Haws

About Me

- 4th Year Computer Science
- CPSEC:
  - Sys-Admin: 2022-23
  - President: 2021-22
- CPLUG:
  - Treasurer/Sys-Admin: 2022-23
  - President: 2021-23
- Experience: AMD, Jump Trading, Honeywell
- Fun Fact: I just built my first gaming PC

Agenda

Did someone say bonus?

- SSH Overview
- What is an SSH key?
- Key Types & Recommendations
- How to generate keys
- What is an SSH Agent?
- How to set up an SSH Agent
- Bonus SSH content

SSH Overview

The UNIX servers run OpenSSH 7.4p1 :(

- ssh (secure shell):
  - A program for logging into a remote machine and for executing commands on a remote machine.
  - It is intended to provide secure encrypted communications between two untrusted hosts over an insecure network.
  - ssh connects and logs into the specified destination, which may be specified as either:
    - [user@]hostname
    - ssh://[user@]hostname[:port]
  - The user must prove their identity to the remote machine using one of several methods.

What is an SSH key?

- Cryptographic key using a public key cryptosystem (RSA, DSA, ECC, etc)
- Authentication credentials presented to a remote server, similar to a password

Key Types

- RSA & DSA
  - RSA-4096
  - RSA-3072
  - DSA (1024 bits)

- Elliptic Curve
  - ecdsa
  - ecdsa-sk
  - ed25519
  - ed25519_sk
  - ecdsa (256, 384, 521 bits)
  - ecdsa_sk

Key Recommendations

Real ones use ed25519_sk

- Personal Recommendations
  1. ed25519
  2. ed25519_sk
  3. RSA-4096
  4. RSA-3072
- Everything else
  - dsa
  - ecdsa
  - ecdsa-sk
  - RSA < 3072

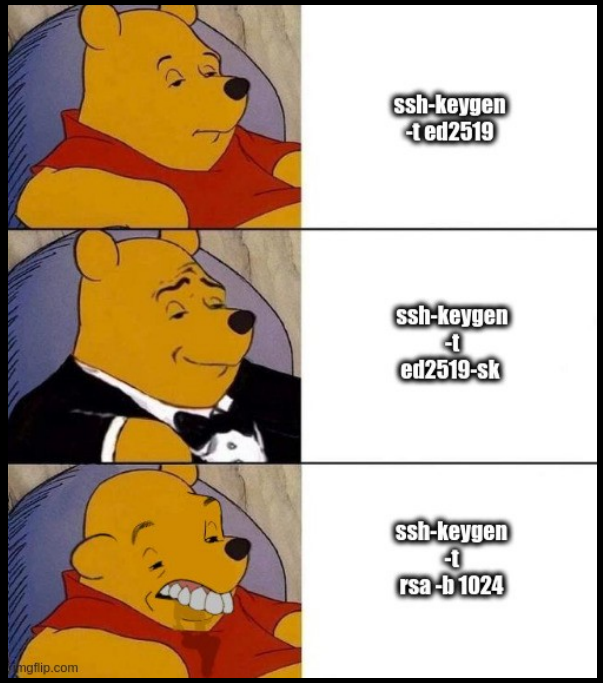
NIST Key Recommendations

Date	Security Strength	Symmetric Algorithms	Factoring Modulus	Discrete Logarithm Key	Discrete Logarithm Group	Elliptic Curve	Hash (A)	Hash (B)
Legacy [1]	80	2TDEA	1024	160	1024	160	SHA-1 [2]	
2019 - 2030	112	(3TDEA) [3] AES-128	2048	224	2048	224	SHA-224 SHA-512/224 SHA3-224	
2019 - 2030 & beyond	128	AES-128	3072	256	3072	256	SHA-256 SHA-512/256 SHA3-256	SHA-1 KMAC128
2019 - 2030 & beyond	192	AES-192	7680	384	7680	384	SHA-384 SHA3-384	SHA-224 SHA-512/224 SHA3-224
2019 - 2030 & beyond	256	AES-256	15360	512	15360	512	SHA-512 SHA3-512	SHA-256 SHA-512/256 SHA-384 SHA-512 SHA3-256 SHA3-384 SHA3-512 KMAC256

How to generate a key

Get that security out of my face

```
[~]-[main*]── - ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/jaxon/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/jaxon/.ssh/id_ed25519
Your public key has been saved in /home/jaxon/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:lIaquuu8oduHijYFdCVcX4VYplVq4RiDbzyfFvzGEhY jaxon@
The key's randomart image is:
+--[ED25519 256]--+
|   ..oo.oo*+o    |
| . o ... oXEo    |
|. .   ++=+.      |
| .    . B.=      |
|  . . . S *      |
|   o     = +     |
| .o.     . o     |
|+=o .            |
|@O+.             |
+----[SHA256]-----+
```



Generate a key on a YubiKey

- Discverable (Resident)

```
[/tmp]── ─ ssh-keygen -t ed25519-sk -O resident -O application=ssh:throwaway -O verify-required
Generating public/private ed25519-sk key pair.
You may need to touch your authenticator to authorize key generation.
Enter PIN for authenticator:
You may need to touch your authenticator again to authorize key generation.
Enter file in which to save the key (/home/jaxon/.ssh/id_ed25519_sk): /tmp/id_throwaway_sk
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /tmp/id_throwaway_sk
Your public key has been saved in /tmp/id_throwaway_sk.pub
The key fingerprint is:
SHA256:mjqwYcbMyQljJLgMmnfLV3EM2stnDYcHOIlUqantUUw jaxon@
The key's randomart image is:
+[ED25519-SK 256]-+
|.     ..oo*.      |
|+.     .oE oo     |
|*o     .=.+o o    |
|*o. . o.+. =      |
|.O = + oS o .     |
|  % + +o o        |
| o + oo.          |
|  . ...           |
|    ..            |
+----[SHA256]-----+
```

Requires OpenSSH ⩾ 8.3 & YubiKey Firmware ⩾ 5.2.3

Generate a key with a YubiKey

- Non-Discverable

```
[/tmp]── ─ ssh-keygen -t ed25519-sk
Generating public/private ed25519-sk key pair.
You may need to touch your authenticator to authorize key generation.
Enter PIN for authenticator:
You may need to touch your authenticator again to authorize key generation.
Enter file in which to save the key (/home/jaxon/.ssh/id_ed25519_sk): /tmp/id_donotuse_sk
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /tmp/id_donotuse_sk
Your public key has been saved in /tmp/id_donotuse_sk.pub
The key fingerprint is:
SHA256:5w6j3BWIHqb4PDhrmYStos6cHYiECXYJlGnS74hOoSE jaxon@a
The key's randomart image is:
+[ED25519-SK 256]-+
|.+o              |
|.+o .            |
|+. +             |
|Eo. .  . .       |
|=*.o  + S o      |
|*.=..+ . o .     |
|++.=. . o o      |
|=.Ooo. o =       |
|=*.+o.o . .      |
+----[SHA256]-----+
```

Requires OpenSSH ⩾ 8.2p1 & YubiKey Firmware ⩾ 5.2.3

How to copy your key


```
[/tmp]── - ssh-copy-id -i id_do_not_use_ed25519 unix1
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "id_do_not_use_ed25519.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
jphaws@unix1.csc.calpoly.edu's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'unix1'"
and check to make sure that only the key(s) you wanted were added.
```

Security Best Practices

But passwords are hard...

- 1 key per unique host/application
- Password protect your keys

What is an SSH Agent?

- ssh-agent:
  - A program to hold private keys used for public key authentication.
  - Through use of environment variables the agent can be located and automatically used for authentication when logging in to other machines using ssh(1).

How to set up an SSH agent

A question as old as time

```
jphaws@unix5:~ $ eval $(ssh-agent)
Agent pid 30346
jphaws@unix5:~ $ ssh-agent -k
unset SSH_AUTH_SOCK;
unset SSH_AGENT_PID;
echo Agent pid 30346 killed;
```

Bonus 1: SSH Config

Now featuring my ssh config file

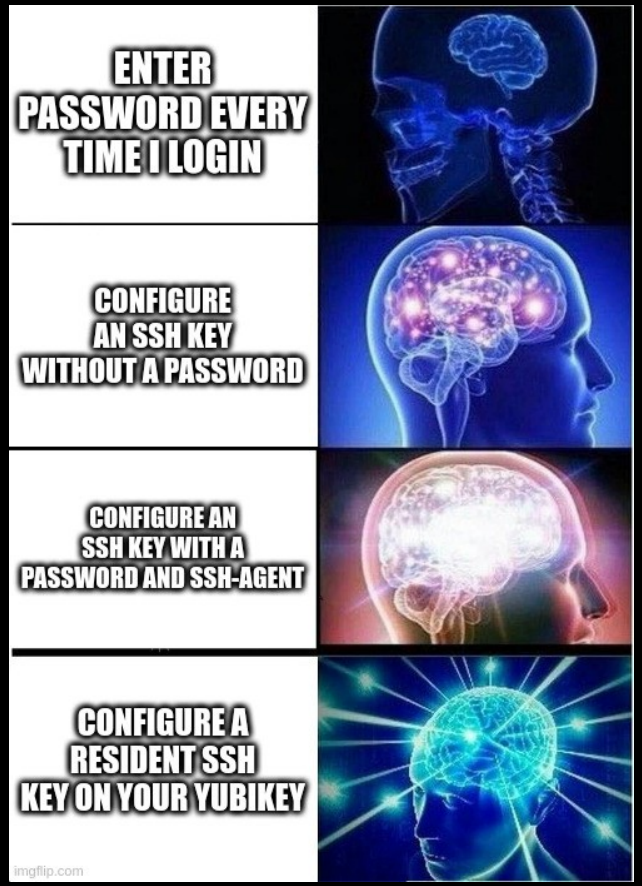
```
[~]-[main*]── - cat .ssh/config

SetEnv TERM=xterm-256color
Include conf.d/*
```

```
[~]-[main*]── - cat .ssh/conf.d/config
Host unix*
     HostName %h.csc.calpoly.edu
     User jphaws
     IdentityFile ~/.ssh/id_unix_ed

Host github.com
     HostName github.com
     User git
     IdentityFile ~/.ssh/id_ed25519_sk_rk_git_5c
     IdentitiesOnly yes
     IdentityAgent /usr/local/var/run/yubikey-agent.sock

Host github.com
     HostName github.com
     User git
     IdentityFile ~/.ssh/id_ed25519_sk_rk_git_5
     IdentitiesOnly yes
     IdentityAgent /usr/local/var/run/yubikey-agent.sock
```

Bonus 2: SSH tools

- scp
- git
- Putty
- Teleport

Bonus 3: Galaxy Brain SSH Keys



Resources

Who knew the man pages were so useful...

- man ssh-keygen
- man ssh-copy-id
- man ssh-agent
- man ssh-add
- man ssh
- https://goteleport.com/blog/comparing-ssh-keys/
- https://wiki.archlinux.org/title/SSH_keys
- https://developers.yubico.com/SSH/Securing_SSH_with_FIDO2.html

> _ exit

logout
Connection to Jaxon closed.

Thanks for watching