Generating a ED25519 SSH key with OpenSSH

Isaac Bythewood · 2022-05-07 · 2 min read

security

OpenSSH has deprecated RSA keys. Time to swap to ED25519 with a few quick commands as well as an easy way to ease into the swap with host key configurations.

With the release of OpenSSH 8.7 the `ssh-rsa` signature scheme has been deprecated.

> OpenSSH will disable the ssh-rsa signature scheme by default in the next release. In the SSH protocol, the "ssh-rsa" signature scheme uses the SHA-1 hash algorithm in conjunction with the RSA public key algorithm. It is now possible[1] to perform chosen-prefix attacks against the SHA-1 algorithm for less than USD$50K.

You can read more about that on their release notes.

That means we should probably generate new keys as soon as possible using the suggested ED25519. To do that is as simple as running:

```
cd ~/.ssh
ssh-keygen -t ed25519 -C "email@example.com"
```

While you get all your services updated with your new key you can still use your old key temporarily by adding an extra line to your `~/.ssh/config` file.

```
echo "PubkeyAcceptedKeyTypes +ssh-rsa" >> .ssh/config
```

If you have a lot of services that share SSH keys consider swapping out your most important ones first and then adding some extra lines to your `~/.ssh/config` file to use different keys for different hosts.

```
Host example.com
    HostName example.com
    User myuser
    IdentityFile ~/.ssh/id_rsa
Host example2.com
    HostName example2.com
    User myuser
    IdentityFile ~/.ssh/id_ed25519
```

To my understanding, if you follow security best practices and don't have port 22 open to the entire web on your servers then this deprecation isn't of immediate concern.