Using YubiKey and FIDO2 With OpenSSH

13:00 9 March 2024

Sean Malloy

Introduction

```
package main

import "fmt"

type Presenter struct {
    Name      string
    Employeer string
    Title     string
}

func main() {
    x := Presenter{}
    x.Name = "Sean Malloy"
    x.Employeer = "Red Hat"
    x.Title = "Technical Account Manager"
    fmt.Println(x.Name)
    fmt.Println(x.Employeer)
    fmt.Println(x.Title)
}
```

Run

2

What Problem Are We Trying To Solve?

You are using SSH public key authentication and you
want to prevent your private key from being stolen.

What are your options?
- Use a tradional(i.e. stored on disk) SSH key pair with a passphrase
- Build an under ground bunker with no internet access and never leave
- Use a hardware security token to store your private SSH key

3

What is a YubiKey?

A YubiKey is a hardware security token that adds an extra layer of security to online services. It looks like a USB thumb drive and is manufactured by Yubico, a hardware security vendor.

www.yubico.com/why-yubico/for-individuals/ (https://www.yubico.com/why-yubico/for-individuals/)

What is a FIDO2?

Fast IDentity Online 2 (FIDO2) is a set of specifications that allows users to authenticate to online services using common devices. It's an open standard that uses cryptographic credentials to protect users and organizations from cybercrimes.

fidoalliance.org/fido2/ (https://fidoalliance.org/fido2/)

5

What is OpenSSH?

OpenSSH is the premier connectivity tool for remote login with the SSH protocol. It encrypts all traffic to eliminate eavesdropping, connection hijacking, and other attacks. In addition, OpenSSH provides a large suite of secure tunneling capabilities, several authentication methods, and sophisticated configuration options.

www.openssh.com/ (https://www.openssh.com/)

6

Software and Hardware Used

- Fedora 39 Linux Distribution fedoraproject.org/ (https://fedoraproject.org/)
- OpenSSH 9.3p1 www.openssh.com/ (https://www.openssh.com/)
- YubiKey Manager (ykman) 5.3.0 github.com/Yubico/yubikey-manager (https://github.com/Yubico/yubikey-manager)
- Yubikey 5 Series (Nano) www.yubico.com/ (https://www.yubico.com/)
- OpenSSH version 8.2 is the first relase to support FIDO2.

```
#!/bin/bash

# Must run as root
dnf install -y yubikey-manager openssh-clients
```

Run

7

Basics

Set a PIN for the YubiKey:
$ ykman fido access change-pin # a PIN is optional

Generate a SSH key pair:
$ ssh-keygen -t ed25519-sk

Copy the public key:
$ scp ~/.ssh/id_ed25519_sk.pub $SERVER:

8

Resident vs. Non-Resident Keys

- A FIDO key consist of two parts a key handle and a private key
- By default OpenSSH creates non-resident(non-discoverable) keys(key handle on disk, private key on YubiKey)
- OpenSSH can also create a resident(discoverable) key(key handle and private key on YubiKey)

Generate a resident SSH key pair:
$ ssh-keygen -t ed25519-sk -O resident

Retrive key handle from YubiKey for a resident key:
$ cd .ssh
$ ssh-keygen -K

9

Requiring A PIN

Generate a SSH key pair:
$ ssh-keygen -t ed25519-sk -O resident -O verify-required

Start ssh-agent and SSH:
$ eval "$(ssh-agent)"
$ ssh $SERVER

The PubkeyAuthOptions configuration option can be used in the /etc/ssh/sshd_conifg file to require all FIDO2 SSH keys to require PIN verification. The PubkeyAuthOptions configuration option can also be used inside a Match block in sshd_config.

As an alternative the verify-required option can be used in a ~/.ssh/authorized_keys file to require PIN verification for a specific SSH key.

References

- www.openssh.com/ (https://www.openssh.com/)
- www.yubico.com/ (https://www.yubico.com/)
- developers.yubico.com/SSH/ (https://developers.yubico.com/SSH/)
- developers.yubico.com/SSH/Securing_SSH_with_FIDO2.html (https://developers.yubico.com/SSH/Securing_SSH_with_FIDO2.html)
- man ssh-keygen
- man sshd
- man sshd_config

Questions

???

12

Thank you

Sean Malloy
spinelli85@gmail.com (mailto:spinelli85@gmail.com)
http://spmalloy.com (http://spmalloy.com)
@spmalloy (http://twitter.com/spmalloy)