Utilisation d'une YubiKey comme clé SSH avec FIDO2

Prérequis

Vérifier que OpenSSH 8.2 ou supérieur est installé sur le client et le serveur.

```
ssh -V
```

Vérifier la compatibilité de la YubiKey

Deux types de paires de clés sont compatibles avec FIDO2 : `ecdsa-sk` et `ed25519-sk`.

- L'extension -sk signifie "security key".
- Le type `ed25519-sk` nécessite une YubiKey avec le firmware 5.2.3 ou supérieur.

> Les clés `ed25519-sk` nécessitent une YubiKey avec un **firmware en version 5.2.3 ou supérieure**, compatible FIDO2.

Pour afficher la version du firmware de la YubiKey :

```
lsusb -v 2>/dev/null | grep -A2 Yubico | grep "bcdDevice" | awk '{print $2}'
```

Installer les dépendances nécessaires

```
sudo apt install libfido2-dev
```

Générer une paire de clés SSH avec FIDO2

Créer une clé SSH sécurisée par YubiKey :

```
ssh-keygen -t ed25519-sk -C "$(hostname)-$(date +'%Y%m%d')-yubikey1"
```

Une partie de la clé privée est stockée dans la YubiKey. Elle repose sur un mécanisme de défi-réponse sécurisé. La clé publique, un handle et des données d’attestation sont générés.

Copier la clé publique sur un serveur

Sous Linux :

```
ssh-copy-id -i ~/.ssh/id_ed25519-sk.pub user@serveur
```

Sous Windows (PowerShell) :

```
type $env:USERPROFILE.ssh\id_ed25519-sk.pub | ssh user@serveur "mkdir -p ~/.ssh && cat >> ~/.ssh/authorized_keys"
```

Remplacer user@serveur par les informations du serveur cible.

Sources

https://forums.lawrencesystems.com/t/ssh-with-yubikey-fido-u2f-authentication/13024

https://developers.yubico.com/SSH/Securing_SSH_with_FIDO2.html

---

Revision #3
Created 2025-05-11 19:03:58 UTC by Axolito
Updated 2025-05-11 19:38:54 UTC by Axolito