Authentification avec clés FIDO2 / Webauthn

Matthieu Herrb

Capitoul - 11 février 2021

https://homepages.laas.fr/matthieu/talks/token-capitoul-2021.pdf

Introduction

- Suite d'une présentation Capitoul d'octobre 2016...
- Évolutions :
  - Mots de passe de plus en plus attaqués (spear-phishing,...)
  - Nouveaux standards FIDO2/Webauthn (2018)
  - Support applicatif qui s'améliore

Tourner la page des certificats pour l'authentification

- Au début des années 2000 au CNRS on a testé l'authentification renforcée par certificats de personnes.
  - Développement de l'IGC CNRS.
  - Authorités d'enregistrement dans les labos.
  - $\rightarrow$ pour délivrer des certicats de personnes (entre autres) pour de l'authentification sur les applications Web.
- Constat 20 ans après :
  - Le support des certificats personnels dans les navigateurs est resté difficile à utiliser pour la plupart des Michus
  - L'IGC CNRS n'est plus capable de délivrer des certificats modernes $\rightarrow$ abandon en cours.
  - Le support pour l'auth par certificats personnels dans les applis Web (Janus) devient difficile à maintenir.
  - Problème de reconnaissance des certificats émis par les partenaires.

FIDO2 et Webauthn

Webauthn ou Web Authentication API est un standard qui fait partie du cadriciel FIDO2 développé par le W3C et l'alliance FIDO avec les GAFAM.

- évolution de FIDO Legacy / U2F.
- peut être utilisé seul (remplace le mot de passe) ou en complément, selon le niveau de sécurité voulu.
- dérive les secrets cryptographiques à partir de l'URL du service $\rightarrow$ pas de stockage volumineux sur le clé physique.
- simplifie l'enregistrement des clés par les utilisateurs ou utilisatrices.

Avantage supplémentaire : coût des clés (10-20€ vs 50€ pour une Yubikey 5 NFC avec toutes les technos)

Reboot technologique

- Toutes les fonctionalités présentées ici sont aussi disponibles avec d'autres technologies d'authentification à 2 facteurs (OTP, PIV, PKCS#11,...)
- Souvent les clés du commerce supportent plusieurs technologies et doivent être configurées.
- Tout cela est source de confusion...
- Dans la suite on ne parle plus que de FIDO / Webauthn.
- Prédiction personnelle : les autres technologies vont progressivement disparaître

Produits:

- Yubikeys
- Solo Keys
- Nitro key

Authentification Linux

via PAM

Paquet

- libpam-u2f

Enrôler la clé

```
# pamu2fcfg -u <user> > /etc/u2f_mappings
```

configuration PAM /etc/pam.d/common-auth

```
auth sufficient pam_u2f.so authfile=/etc/u2f_mappings
```

ou

```
auth required pam_u2f.so authfile=/etc/u2f_mappings
```

Authentification OpenSSH

via authorized keys (OpenSSH $\geq$ 8.2)

Enrôler la clé

```
$ ssh-keygen -t ecdsa_sk
$ ssh-copy-id -i ~/.ssh/id_ecdsa_sk remote_host
```

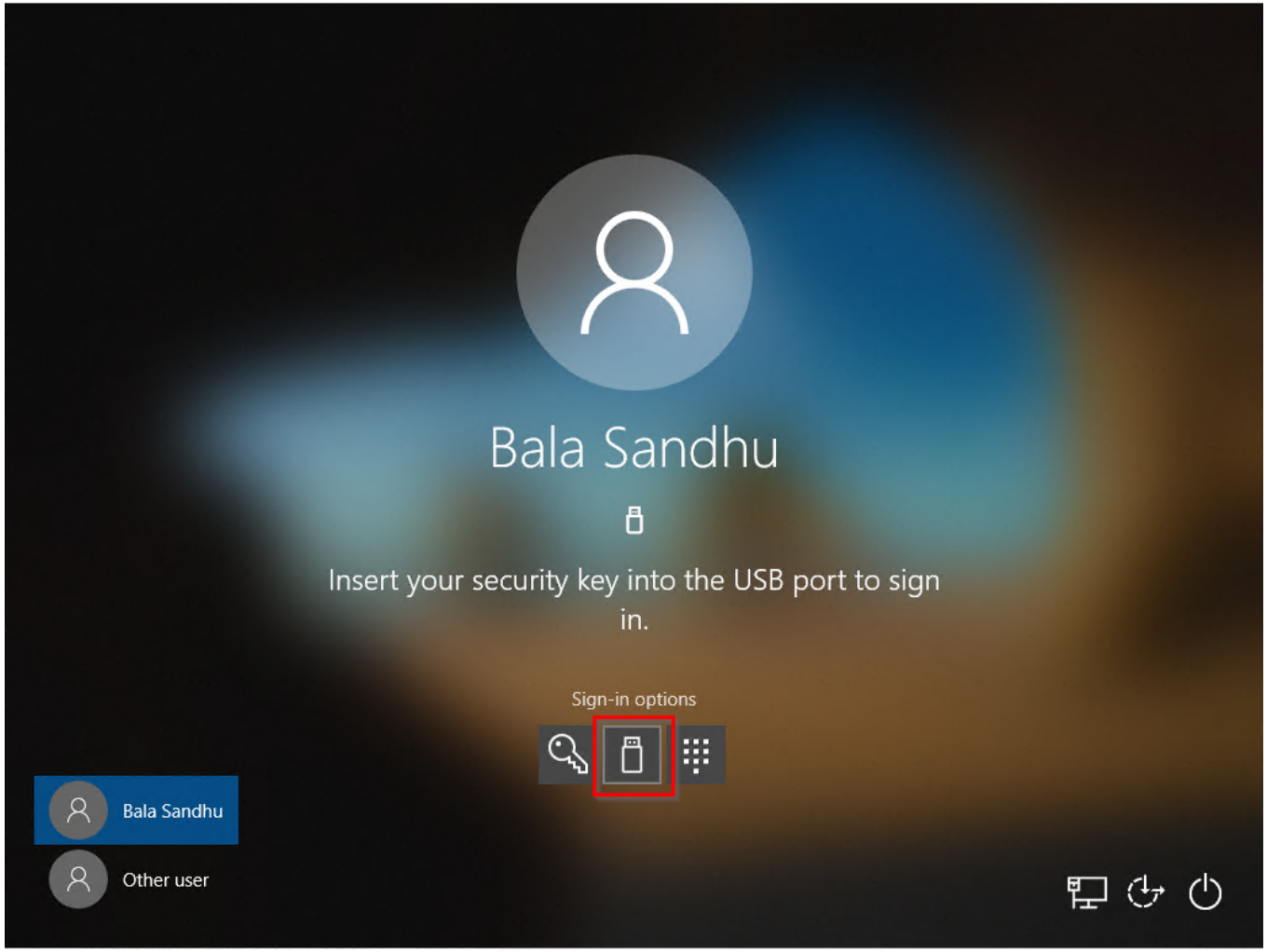
Mettre un mot de passe sur la clé pour vrai 2FA.

Utilisation

```
$ ssh remote_host
```

Authentification Windows

Via *Azure Active Directory* et Windows 10 1909 ou plus récent



⟶ Documentation

SSO Web

Disponible chez les GAFAM + Gitlab, Nextcloud,...

CAS / Shibboleth & Co pour nous : Pas sec...
supportent U2F/FIDO legacy mais pas encore FIDO2/Webauthn...

- Pas encore supporté dans LemonLDAP-NG
- support dans la version de développement du serveur CAS d'Apereo

Difficultés / Questions

- Pas évident de savoir si FIDO Legacy ou FIDO2 est utilisé (heureusement les clés supportent les 2)
- Planification pour déploiement de masse ?
  - affectation clés / utilisateurs.
  - re-utilisation après départ ?
  - gestion des clés perdues / volées ?
- Démarrer sur U2F / Fido Legacy ou attendre Webauthn ?

Conclusion

- Authentification par mot de passe seul - problématique
- Authentification sans mot de passe ou bien 2 facteurs ?
  - pas les mêmes risques entre poste fixe dans lieu sécurisé et portable
- (trop) nombreux protocoles pour l'authentification 2 facteurs
- Fido 2 / WebAuthn $\rightarrow$ Amélioration de l'expérience utilisateur $\rightarrow$ meilleure acceptation / appropriation ?
- Déploiement plus simple ?
- À suivre

Questions ?

Références

- Authentification 2 facteurs avec token USB, Matthieu Herrb, Capitoul, octobre 2016.
- Universal Two Factors Internals, Blog de Trammel Hudon, décembre 2020.
- Enable passwordless security key sign-in
- How to configure SSH with YubiKey Security Keys U2F Authentication on Ubuntu Cryptsus Blog, février 2020.
- WebAuthn A better alternative for securing our sensitive information online Duo Security, février 2019.
- pam-u2f Documentation Yubico.
- Unlocking LUKS2 volumes with TPM2, FIDO2, PKCS#11 Security Hardware on systemd 248, Blog 0pointer.net, janvier 2021.