Authentification 2 facteurs avec token USB

Matthieu Herrb

Capitoul - 13 octobre 2016

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

Plan

Authentification - rappels

Définition

Vérification de l'identité d'une entité (personne, ordinateur...), afin d'autoriser l'accès de cette entité à des ressources (systèmes, réseaux, applications...)

Facteurs

- quelque chose qu'on connaît (mot de passe, clé secrète,...)
- quelque chose qu'on possède (carte à puce, token USB,...)
- une caractéristique intrinsèque (biométrie: empreintes digitales, iris, contour de la main...)

Authentification - problèmes

Limitations des mots de passe (un seul facteur)

- multiplicité
- vol (brute force, key-logger, phishing,...)

Solutions

- fédération(s) d'identité(s) (multiplicité)
- gestionnaires de mots de passe (keepass, 1passwd, dashlane, mooltipass,...)
- facteurs multiples (au moins 2) (fragilité du mot de passe)

Authentification deux facteurs

Nombreuses technologies

- One Time Password token : grille, « calculette », ...
- Cartes à puce / tokens USB 1ère génération : technologie PKCS#11,....
- envoi de SMS

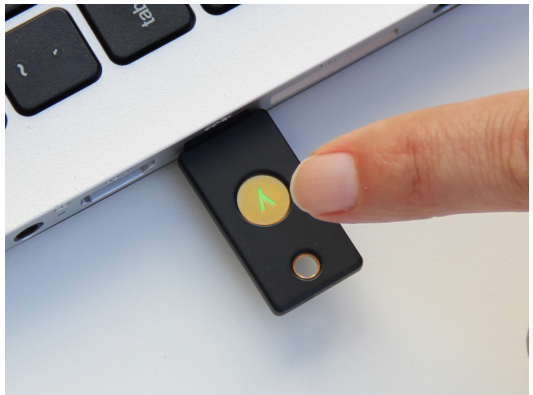
Problèmes

- Utilisation laborieuse ($\Rightarrow$ rejet par les utilisateurs)
- Un seul service à la fois
- Vulnérabilités résiduelles (attaques connues & utilisées)

Plan

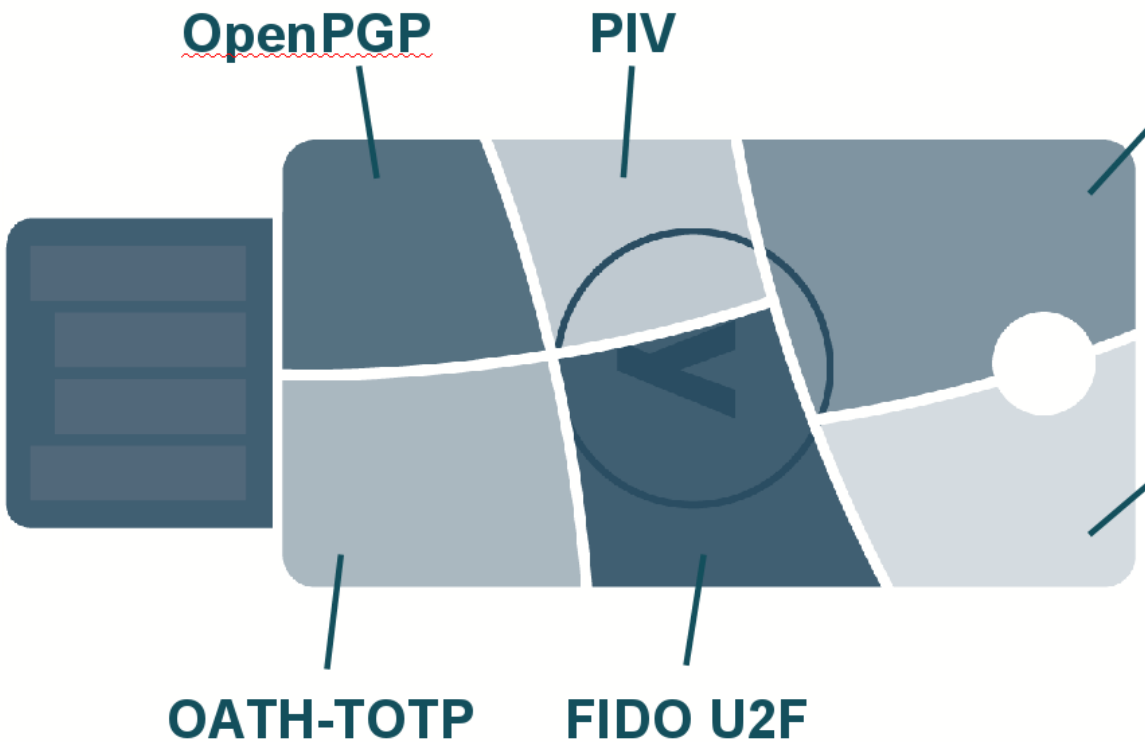
Yubikeys

Yubikey 4



Yubikey Nano

yubikey NEO

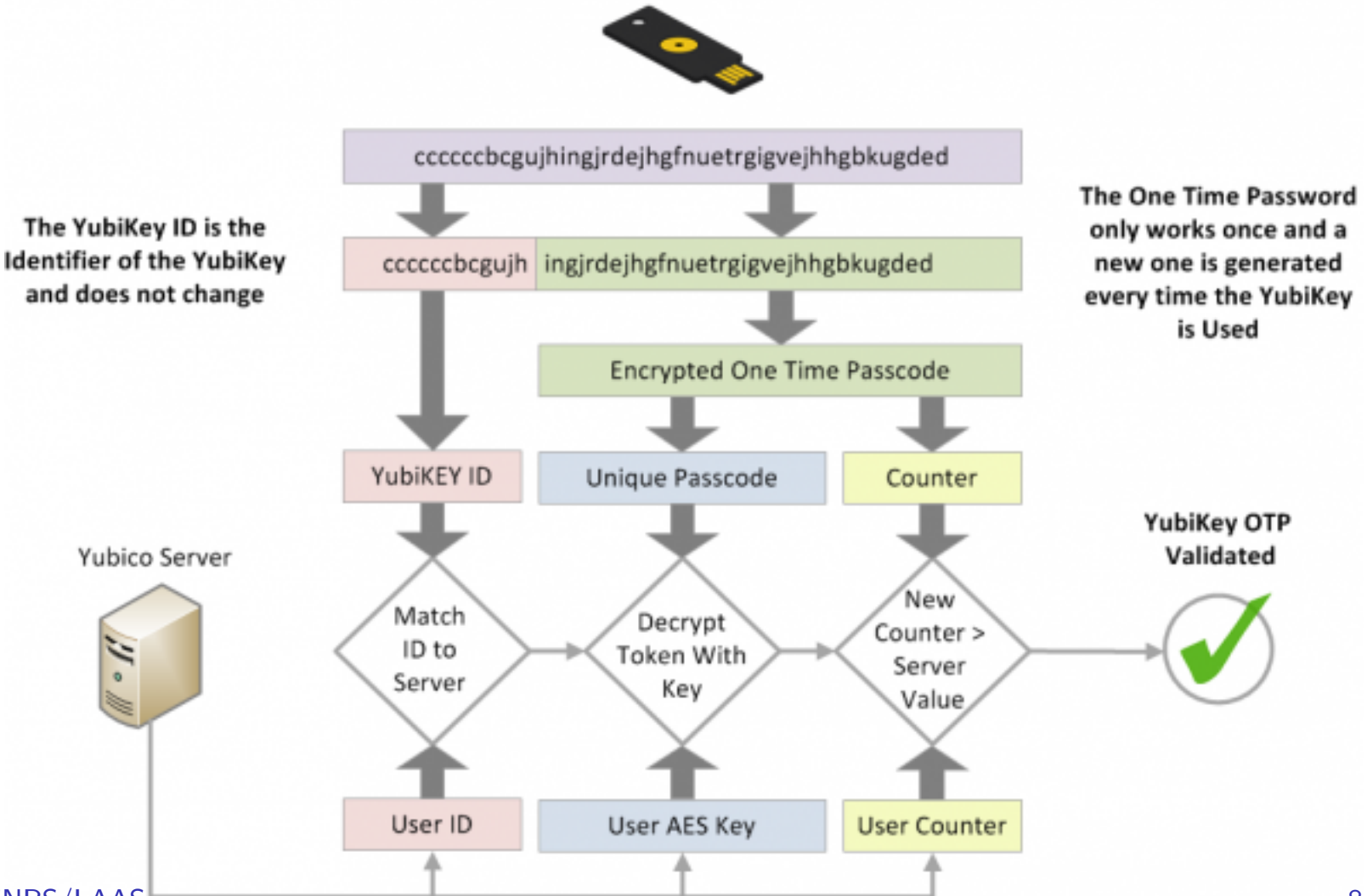


Config Set 1
Yubico OTP
OATH-HOTP
Challenge-Response
Static Credential

Config Set 2
Yubico OTP
OATH-HOTP
Challenge-Response
Static Credential

Yubico OTP

- Mode « historique » des Yubikeys
- S'attache comme un clavier USB (HID)



OATH-OTP

TOTP

- Time-based One-time Password Algorithm
- RFC6238

HOTP

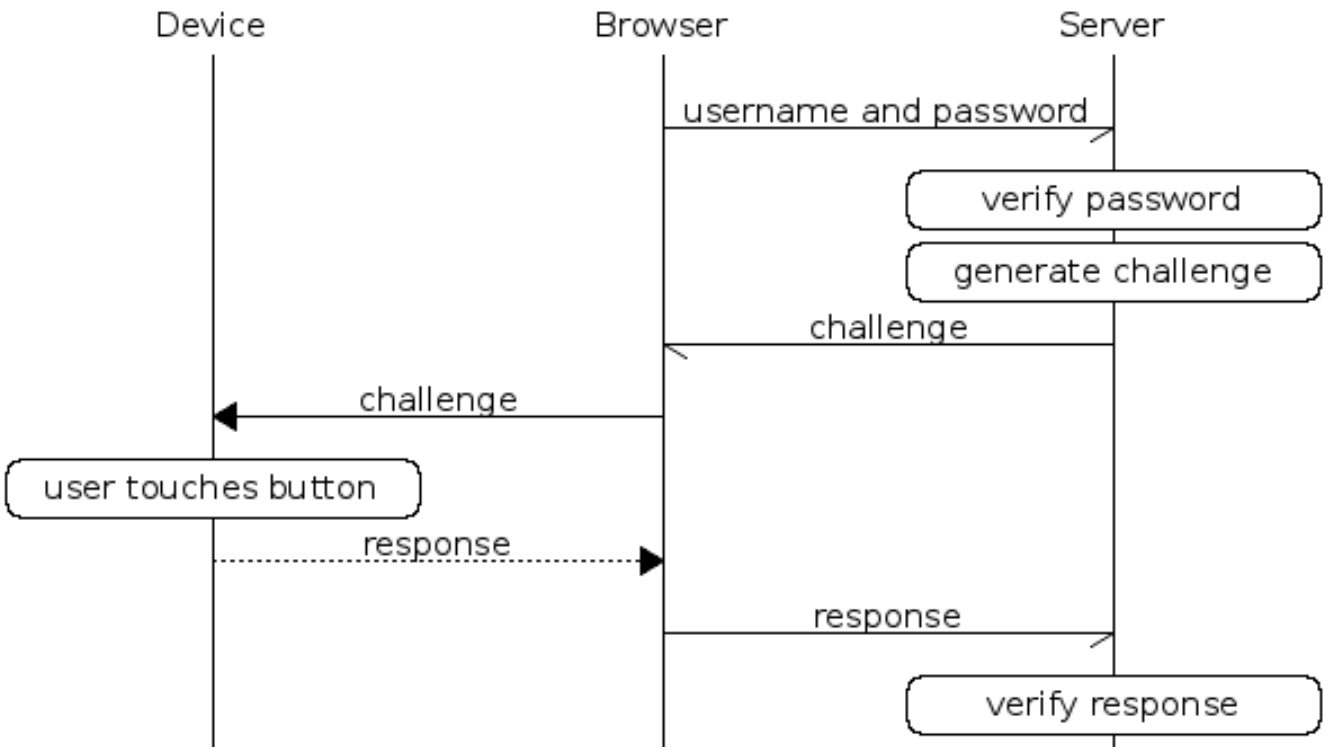
- HMAC-based one-time password
- RFC4226

$\rightarrow$ Yubico Authenticator (Android/NFC - Desktop/USB)

supporté par Google, DropBox, Gandi,...

FIDO U2F

Standard de la FIDO Alliance (Google, Yubico, NXP)
Authentification Web, PAM, bientôt MS-Windows



PIV

- Personal Identity Verification
- NIST SP 800-73 document
- Utilise PKCS#11
- Authentification AD (smartcard) Windows
- Support Linux via OpenSC
- Peut être utilisé comme HSM pour une AC X.509.

Voir : YubiKey PIV Deployment Guide

OpenPGP

- Interface compatible PKCS#11 pour stocker clés PGP ou SSH
- Support OpenSSH, PAM, GnuPG 2.x, Thunderbird,....

Récapitulatif

	OTP	U2F	OATH	PGP	PIV
PAM	X	X	X	X	X
Auth. Windows					X
Auth. Web	X	X	X		
CAS	X				
Shibboleth		X	X		
Chiffrement				X	X
AC (HSM)					X

The Nitrokey Family

	Nitrokey Storage	Nitrokey Pro	Nitrokey Start	Nitrokey HSM	Nitrokey U2F
					
Open source	✓	✓	✓	✓	
Tamper-resistant smart card	✓	✓		✓	
S/MIME email and hard disk encryption (X.509, PKCS#11)	✓	✓	✓	✓	
OpenPGP/ GnuPG email encryption	✓	✓	✓		
Secure login (One Time Passwords)	✓	✓			
Password Manager	✓	✓			
Encrypted mass storage	✓				
Hidden volumes	✓				
Firmware updates and verification	✓				
RSA key length [bit]	1024 - 4096	1024 - 4096	2048	1024 - 2048	
Number of RSA key pairs	3	3	3	48	
Number of ECC key pairs				60	
PKI/CA management features				✓	
Secure login (Universal 2nd Factor - U2F)					✓
Price		€ 49.00	€ 29.00	€ 49.00	€ 9.00

Plan

Conclusion

- Authentification par mot de passe seul - problématique
- (trop) nombreux protocoles pour l'authentification 2 facteurs
- Amélioration de l'expérience utilisateur $\rightarrow$ meilleure acceptation / appropriation ?
- Déploiement pas forcément simple
- À suivre

Plan

Références

- État de l'art de l'authentification renforcée, D. Algave et al, JRES 2013.
- Yubikey : https://www.yubico.com/
- Nitrokey : https://www.nitrokey.com/
- PGP & SSH keys on a Yubikey neo https://www.esev.com/blog/post/2015-01-pgp-ssh-key-on-yubikey-neo/
- GPG with smart cards https://www.jfry.me/articles/2015/gpg-smartcard/
- Yubikey PIV Introduction https://developers.yubico.com/yubico-piv-tool/YubiKey_PIV_introduction.html
- U2F avec drupal : https://www.drupal.org/project/u2f