WTF 2FA SSH

MÁSFÉL FAKTOR LETT, MARADHAT?

Veres-Szentkirályi András **2020-11-14**

$ whoami

Veres-Szentkirályi András

- OSCP, GWAPT, SISE
- Silent Signal alapító
- pentester, toolmaker

SSH

silent signal

- RFC 4503: SSH transzport réteg – titkosítás, szerver autentikáció
  - MITM lehetőség: fake szerver, kliens nem ellenőrzi a fingerprint
- RFC 4502: SSH autentikációs réteg – kliens autentikáció
  - MITM lehetőség: rosszindulatú/kompromittált szerver, credential relay/reuse
- Tipikus SSH autentikáció:
  - jelszó: egyszerű, olcsó, könnyen integrálható (PAM, AD)
  - kulcsfájl: nem sokkal bonyolultabb, fake szerver ellen is véd (!)

2FA

silent signal

- ismert definíció: kettőt választunk a {tudás, birtoklás, biometria} halmazból
- birtoklás: sokféle lehet, akár kaparós sorsjegy-szerű kártya is
- klasszikus: statikus kód beírása
  - SMS olcsó és elterjedt
  - phishing ellen nem sokat véd
- modern: interaktív, kriptográfián alapuló
- U2F (Universal 2nd Factor)
  - FIDO szövetség
  - publikus kulcs alapú
  - WebAuthn: phishing-álló szabvány webre

SSH + 2FA

silent signal

Megoldás neve	Szerver igény	Szerver ellen	Előny	Hátrány
HOTP	egyedi	nem véd	akár papíron is működik	állapot kell
TOTP	egyedi	nem véd	állapotmentes	óra kell
egyedi	egyedi	attól függ	attól függ	fizetős, konfigolós
PGP	nincs	véd	meglévő hw/sw/kulcsok	PGP
Krypton	nincs	véd	egyszerű és ingyenes	app limitációk
U2F	új verzió	véd	olcsó és biztonságos	kompatibilitás
Yubikey Agent	nincs	véd	Just works™	drágább hardver

HOTP/TOTP/egyéb egyediek

silent signal

- szerveroldali támogatást igényelnek mind
- HOTP és TOTP szabványos, sok implementáció létezik
  - szerveroldal: `https://wiki.archlinux.org/index.php/Pam_oath`
  - kliensoldal: `apt install oathtool`, Google Authenticator
  - hardveres megoldás: Yubikey
- egyedi (nagyrészt proprietary) megoldások
  - single point of failure?
  - megéri?

PGP

silent signal

- PGP: van aláírási primitív, sok hw/sw/kulcs
- SSH: autentikációhoz alá kell írni egy challenge értéket
- match made in heaven?
- RSA, ECDSA legalább használható
- PGP: szabványosság előny és hátrány
- `https://serverfault.com/questions/60064/using-pgp-keys-for-ssh`

Krypton

silent signal

- `https://krypt.co/`
- előnyök és hátrányok egy mondatban: Android és iOS app
- app limitációk: egyetlen kulcs, ami RSA *vagy* Ed25519
  - ha csak egy szervered is van, ami csak RSA-t támogat, nincs választásod
  - cross-server fingerprinting, ki hova tud bemenni, lásd GitHub
- bónusz: WebAuthn böngésző plugin

U2F

silent signal

- bár ECDSA ill. EdDSA, de nem a megszokott „körítésben”
- OpenSSH 8.2-től támogatott csak, szerver- *és* kliensoldal támogatása is szükséges
- privacy win: „∞” kulcs, valójában egy szimmetrikus mesterkulcs + offload kliensre
- drágább hardveren security tradeoff: kliensről kulcs feltöltése („rezidens” kulcsok)
- `https://github.com/openssh/openssh-portable/blob/master/PROTOCOL.u2f`
- `https://buttondown.email/cryptography-dispatches/archive/cryptography-dispatches-openssh-82-just-works/`

Yubikey Agent

silent signal

- Yubikey hardver U2F-től független ECDSA/RSA megoldását használja
  - előny: kulcs hardveren, cipelhető mindenfelé
  - hátrány: limitált kulcsmennyiség, privacy gondok
- bónusz: ugyanazon a hardveren WebAuthn, TOTP is
- Just Works™
- `https://github.com/FiloSottile/yubikey-agent`

Összefoglalás: ismerős dia

silent signal

Megoldás neve	Szerver igény	Szerver ellen	Előny	Hátrány
HOTP	egyedi	nem véd	akár papíron is működik	állapot kell
TOTP	egyedi	nem véd	állapotmentes	óra kell
egyedi	egyedi	attól függ	attól függ	fizetős, konfigolós
PGP	nincs	véd	meglévő hw/sw/kulcsok	PGP
Krypton	nincs	véd	egyszerű és ingyenes	app limitációk
U2F	új verzió	véd	olcsó és biztonságos	kompatibilitás
Yubikey Agent	nincs	véd	Just works™	drágább hardver

KÖSZÖNÖM!

VERES-SZENTKIRÁLYI ANDRÁS

vsza@silentsignal.hu

facebook.com/silentsignal.hu

@SilentSignalHU

@dn3t

silent signal