ZERO-TRUST SSH ADMINISZTRÁCIÓ

MI A STATE OF THE ART 2023-BAN?

silent signal

Veres-Szentkirályi András 2023-02-27

$ whoami

Veres-Szentkirályi András

- CISSP, OSCP, GWAPT, SISE
- Senior IT biztonsági szakértő
- Silent Signal társalapító
- pentester, toolmaker, kiberpápa

Menetrend

1. Buzzword bingo
2. Autentikációs módok és támadói modellek
3. Anti-patterns
4. Tokenek és a gép
5. Tanúsítványok
6. What could possibly go wrong?
7. Útravaló

Zero trust?

silent signal

- Perimeter: ami kívül van, rossz, ami belül van, jó
- Trust boundary
  - OS: userek közt? `plink` parancssori jelszó vs. `ps aux`?
  - Példa: screen lock vs. bármilyen más program

Webauthn, FIDO2, CTAP, U2F?

silent signal

- Webauthn: JS API publikus kulcs alapú autentikációhoz
- FIDO2: Webauthn + CTAP
- CTAP: Client To Authenticator Protocol USB, NFC, BLE, stb. kulcsokhoz
- U2F: Universal 2nd Factor
- stateless: key handle-be belepakolható titkosítva a privát kulcs
- olcsó kulcsok: 10-20 USD
- webre phishing-álló biztonság: hostnév hash is paraméter

Menetrend

1. Buzzword bingo
2. Autentikációs módok és támadói modellek
3. Anti-patterns
4. Tokenek és a gép
5. Tanúsítványok
6. What could possibly go wrong?
7. Útravaló

Jelszó

silent signal

- off-line brute force: megszerzett hashből jelszó
- on-line brute force: SSH-n ritka a kizárási házirend
- keylogger: fertőzött kliens- vagy szervergépen
- MITM támadás: ki ellenőrzi a szerver publikus kulcsát?
- tetszőleges fentivel kombinálva: password reuse

Kulcsfájl

silent signal

- brute force: RSA 2048 bit alatt + DSA + jelszavas védelemre
- keylogger: jelszavas védelemre
- fertőzött kliens: fájllopás (szerver is lehet kliens!)
- előre kipróbálható, melyik publikus kulcs hova jó
  - `https://github.com/dnet.keys`
  - vö. CVE-2016-20012 “the vendor does not recognize user enumeration as a vulnerability for this product”

Chipkártya

silent signal

- brute force: hardveres kizárási házirend
- keylogger: PIN kódra (ha nem az olvasón írja be)
- fertőzött kliens: megszemélyesítés (agent forward esetén szerver is!)
- előre kipróbálható, melyik publikus kulcs hova jó
  - `https://github.com/dnet.keys`
  - vö. CVE-2016-20012 “the vendor does not recognize user enumeration as a vulnerability for this product”

Modern token

- brute force: hardveres kizárási házirend
- keylogger: PIV esetén PIN kódra
- fertőzött kliens: fizikai érintés hiányában bukó (agent forward dettó)
  - vö. CVE-2021-36368
- előre kipróbálható, melyik publikus kulcs hova jó
  - U2F esetén hostonként eltérő kulcsok

Menetrend

1. Buzzword bingo
2. Autentikációs módok és támadói modellek
3. Anti-patterns
4. Tokenek és a gép
5. Tanúsítványok
6. What could possibly go wrong?
7. Útravaló

Legacy 2FA

silent signal

- OTP: SMS, YubiOTP, HOTP, TOTP (incl. Google Authenticator)
  - SMS: szolgáltatón keresztüli támadások
  - triviálisan phishingelhető
- push alapú mobilapp megoldások
  - MFA fatigue, MFA bombing támadások
  - szolgáltató mint SPoF: confidentiality + availability
- compliance: pipa
- olcsóság (?), műszaki korlátok
- megoldás: modern 2FA

Kulcsfájlok, chipkártya

silent signal

- biztonságosabbnak hirdetett a jelszavakhoz képest
  - technikai user esetén valóban korlátozható `authorized_keys` fájlban
- jelszóval védhető (?)
- nincs (automatikus) lejárat
- agyonszemetelt `authorized_keys` fájlok
- kulcsfájlokat adja magát felmásolni más gépekre is (vö. zero trust)
- megoldás: modern token + tanúsítvány

SSH agent forwarding

silent signal

- `ssh -A bastion.cegneve.hu`
- zero trust: miért bízom a szerverben?
- jelez nekem az agent, ha autentikálnak vele?
- middleboxok: this is why we can't have nice things
- megoldás: `ProxyJump`
  - + `ControlMaster`

PuTTY/WinSCP/...

silent signal

- volt idő, amikor a legjobb megoldás volt Windowsra
- nem támogat tanúsítványt
- hardvertoken: külön PuTTY fork CAC néven
- megoldás: Windows 10-től hivatalos OpenSSH az OS része

Menetrend

1. Buzzword bingo
2. Autentikációs módok és támadói modellek
3. Anti-patterns
4. Tokenek és a gép
5. Tanúsítványok
6. What could possibly go wrong?
7. Útravaló

PKCS#11

silent signal

- ideális esetben mindenhez jár driver
- tipikusan RSA és ECDSA támogatás
- OpenSSH alapértelmezetten támogatja
- OS és vendorfüggő élmény

OpenPGP

silent signal

- PGP vs. OpenPGP vs. GnuPG vs. GPG
- szabványos interfész
- GnuPG képes OpenSSH agent interfészt emulálni
  - tanúsítványokkal (lásd később) meggyűlik a baja
  - érdekes megoldás Android + NFC kombinációra:
    `https://play.google.com/store/apps/details?id=org.sufficientlysecure.termbot`
- GnuPG “felhasználói élmény”
- RSA és ECDSA mellett EdDSA támogatás
- encrypt, sign, auth kulcso
- signature counter

Minden más

silent signal

- Webauthn/CTAP
  - új szabvány, visszafelé nem kompatibilis
  - ECDSA, EdDSA
  - OpenSSH beépítetten támogatja
    `https://github.com/openssh/openssh-portable/blob/master/PROTOCOL.u2f`
  - nem minden kulcs támogat FIDO2 PIN-t
  - stateless minden előnye és hátránya (vö. resident keys)
- gyártóspecifikus megoldások
  - Yubikey: `https://github.com/FiloSottile/yubikey-agent`
  - Secure Enclave: `https://github.com/maxgoedjen/secretive`

Menetrend

1. Buzzword bingo
2. Autentikációs módok és támadói modellek
3. Anti-patterns
4. Tokenek és a gép
5. Tanúsítványok
6. What could possibly go wrong?
7. Útravaló

Általános alapok

silent signal

- PKI: publikus-privát kulcspárok, lásd kulcsfájl
- Probléma: jó-jó, de hogyan terítem hatékonyan a publikus kulcsokat?
  - “signing …is not a tooling problem, but a trust and key distribution problem” (Filippo Valsorda) `https://docs.google.com/document/d/11yHom20CrsuX8KQJXBBw04s80Unjv8zCg_A7sPAX_9Y/preview`
- CA: bizalmi lánc vége, lehet külső/belső
- Issuer: aláírja, Subject attribútumai mely publikus kulcshoz köthetők
  - érvényesség: tipikusan tól-ig időbélyegek + visszavonás
  - egyediség: sorozatszám
- Cél: autentikáció – akár egyik, akár mindkét végpont
- X.509: legnépszerűbb szabvány, IPsec, SSL/TLS, OpenVPN

SSH tanúsítványok

silent signal

- egyszerűség: formátum + architektúra
- subject: principal
- `man ssh-keygen`
- host certificate
  - TOFU helyett
  - kulcs alapú autentikáció esetén lényegtelen
  - principal = hostname
- user certificate
  - `authorized_keys` helyett
  - számunkra jóval érdekesebb
  - principal = username **vagy** `AuthorizedPrincipals`
  - su(do) helyett is!

SSH user cert kifejezőereje

silent signal

- tanúsítványban szabályozható attribútumok
  - `force-command`
  - `permit-agent-forwarding`
  - `permit-port-forwarding`
  - `permit-X11-forwarding`
  - `permit-user-rc`
  - `permit-pty`
  - `source-address` (szigorúan csak hardeningként!)
- konfigurációban (jobban) szabályozható attribútumok
  - `PermitOpen` + `PermitListen`
  - `AllowStreamLocalForwarding`
  - `ChrootDirectory` (vö. `ForceCommand internal-sftp`)

With great power …

silent signal

- …comes a great Electricity Bill
- CA: tanuljunk a nagyoktól – Certificate Transparency
- input/dependency: CA issuance policy
- fő veszély: policy-nak ellentmondó tanúsítványkibocsátás
  - ne lehessen csendben, nyom nélkül!
- kriptográfia: letagadhatatlanság
- vasutas ihlet: signature counter
  - HSM-eknél alap (nem olcsó!)
  - OpenPGP aláíró kulcsra

Menetrend

1. Buzzword bingo
2. Autentikációs módok és támadói modellek
3. Anti-patterns
4. Tokenek és a gép
5. Tanúsítványok
6. What could possibly go wrong?
7. Útravaló

Attestation

silent signal

- tokenekben van CSPRNG
  - vö. CVE-2017-15361 a.k.a. ROCA
  - de tudnak kívülről is kulcsot fogadni
- hogyan bizonyítható, hogy nincs még egy példány …
  - …amire nem érvényes a counter?
- attestation: kriptográfiai bizonyíték
  - egy publikus kulcsot egy eszközhöz köt
- Yubikey: X.509 (ASN.1 DER)
- Webauthn/CTAP: CBOR

Availability?

silent signal

- “Remember: everything breaks, have a backup plan for when this YubiKey does.” – Filippo Valsorda
  - `https://github.com/FiloSottile/yubikey-agent/blame/6a3f4fc873150831b7b0e5de2efeb93c55605c72/setup.go#L195`
  - elvesztés, lopás, ESD, …
- user: bármikor kaphat új tanúsítványt az új eszközére
- CA: legyen legalább kettő, akárhány mehet a szerverekre
- BCP/DRP vs. confidentiality/integrity: mik a backupok?
  - fizikai szerver: FDE, konzol, alternatív boot
  - co-location hosting: személyzet, protokoll-specifikus titkok
  - cloud szerver: webes felület, jelszóvisszaállítás
  - utóbbi kettőnél: telefonszám, e-mail cím, domain név

Revocation

silent signal

- SSL/TLS: CRL, OCSP, OCSP Stapling
- SSH: KRL (Key Revocation List) – text source → binary KRL
- cert revocation: CA + (serial *vagy* ID)
  - tipikus példa: jóindulatú téves kibocsátás
- key revocation: publikus kulcs, SHA-1, SHA-256, fingerprint
  - tipikus példa: elhagyott token, kiszivárgott kulcsfájl
- (CA revocation: kiveszem a listából)
- lejárat után ideális esetben felesleges
- fail-secure – annak minden előnyével és hátrányával
- hogyan/hova/mikor terítsük: előre legyen terv!
  - pozitív mellékhatás: naprakész géplista

Naplózás

silent signal

- minden fontos adatot tartalmaz
  - felhasználónév
  - forrás IP cím
  - felhasználó publikus kulcsának algoritmusa és SHA-256 hash-e
  - tanúsítvány ID + sorozatszám
  - CA publikus kulcsának algoritmusa és SHA-256 hash-e
- remélhetőleg van központosított naplózás
- remélhetőleg fut logelemző
- növeljük a lebukás esélyét: gyanús kulcs és/vagy sorozatszám
- szorgalmi: *canary token* – hagyjunk pár cert + kulcs párt széjjel
  - vö. `command=/bin/false,restrict`
  - `https://canarytokens.com/`

Hardening bonbonok

silent signal

- OpenSSH track record kiváló, de ettől még ne hagyjuk feleslegesen elérhetőnek
- SCP helyett SFTP jobban hardenelhető
  - vö. CVE-2020-15778
- force command esetén elérhető az eredeti parancs `SSH_ORIGINAL_COMMAND` környezeti változóban
- `rsync` és `git` kiválóan hardenelhető forced commanddal
  - cserébe félrevezető hibaüzenetek, humans beware
- `AuthorizedKeysFile none` SSHd konfigurációval letiltható
  - erős *arbitrary file write* $\rightarrow$ *code exec/persistence* primitív

Menetrend

1. Buzzword bingo
2. Autentikációs módok és támadói modellek
3. Anti-patterns
4. Tokenek és a gép
5. Tanúsítványok
6. What could possibly go wrong?
7. Útravaló

Konkrét példa 1: ZSCA

silent signal

- `https://github.com/silentsignal/zsca`
- KKV szemmel írtuk magunknak
- Python command line + webes felület
- Yubikey mint kliens és CA
- korlátlan userek és CA-k: csak attestation után
- technikai usereknek kulcsfájl opció
- alapértelmezetten 90 napos tanúsítványok (vö. Let's Encrypt)
- OpenPGP signature counter
- KRL generálás

Konkrét példa 2: smallstep

silent signal

- `https://smallstep.com/blog/use-ssh-certificates/`
- Single Sign-On SSH
- nagyobb szervezetekre szabva
- `ssh target` → browser SSO login → egynapos cert
- Privileged esetre ötletként mehet hasonló akár 5 percessel is
  - just-in-time privileged access – “A model in which users receive temporary permissions to perform privileged tasks, which prevents malicious or unauthorized users from gaining access after the permissions have expired. Access is granted only when users need it.”
  - `https://learn.microsoft.com/en-us/azure/active-directory/privileged-identity-management/pim-configure`

Zárszó

silent signal

- nehéz a rendszereket átlátni
  - “In some sense, the cynical person would say that **the only person in computing that is paid to actually understand the system from top to bottom is the attacker**. Everybody else is usually paid to understand their part” – Halvar Flake
  - `https://youtu.be/8QRnOpjmneo?t=135`
- előremutató: zero-trust, modern tokenek, attestation, SSH user tanúsítványok, OpenSSH, `ProxyJump`, canary tokens
- oda kell figyelni rá: `permit-port-forward` vs. `PermitOpen` / `PermitListen`, KRL, naplózás, middleboxok
- kerülendő: perimeter, jelszó, OTP, “human” kulcsfájlok, agent forwarding, push 2FA, chipkártya, PuTTY/WinSCP

KÖSZÖNÖM!

VERES-SZENTKIRÁLYI ANDRÁS

vsza@silentsignal.hu

facebook.com/silentsignal.hu

@SilentSignalHU

@dn3t

silent signal