Yubikey

Ondřej Caletka

cesnet

5. listopadu 2019

Bezpečnostní tokeny

- zařízení držící tajný kryptografický materiál
- odolnost proti rozebrání, změně firmware
- dotyková ploška pro ověření přítomnosti uživatele
- volitelně autentizace uživatele PINem nebo biometricky

cesnet

Yubikey

- nejběžnější druh tokenu
- podpora mnoha samostatných metod autentizace
- několik forem pro nejrůznější aplikace:
  - Yubikey 5 NFC – USB-A + NFC
  - Yubikey 5C – USB-C
  - Yubikey 5 Nano – minimální velikost
  - Yubikey 5Ci – USB-C + Lightning
  - Security Key NFC – USB-A + NFC – pouze FIDO

cesnet

Podporované autentizační metody 1/2

- Yubico OTP
  - token emuluje klávesnici
  - po dotyku vygeneruje jednorázové heslo
  - vyžaduje centrální autentizační server
- OATH HOTP/TOTP
  - jednorázová hesla známá např. z Google Authenticator
  - token nemá hodiny; vyžaduje speciální aplikaci Yubico Authenticator
- FIDO U2F
  - otevřený standard autentizace k webovým službám
  - vyžaduje podporu v prohlížeči
  - autentizované služby jsou na sobě nezávislé
  - odolnost proti phishingu

cesnet

Podporované autentizační metody 2/2

- FIDO2 (Webauthn + CTAP2) – vylepšené U2F
  - podpora autentizace uživatele PINem
  - podpora přihlášení bez hesla (strong 1FA)
  - podpora přihlášení bez uživatelského jména
- Personal Identity Verification
  - emulace smartcard ve čtečce
  - podpora RSA a ECDSA
  - standardní softwarové rozhraní PKCS#11
- OpenPGP card
  - emulace smartcard ve čtečce
  - nativní podpora v GnuPG

cesnet

Yubikey jako OpenPGP karta

- RSA klíče o velikosti 4096bitů (starší verze pouze 2048bitů)
- výchozí PIN uživatele 123456
- výchozí PIN správce 12345678

cesnet

Problémy s připojením ke kartě

- token implementuje USB protokol CCID
- standardně se používá ovladač PCSC lite
- GnuPG kromě toho obsahuje i vlastní implementaci CCID (scdaemon)
- GnuPG vyžaduje exkluzivní přístup k USB zařízení – kolize s prohlížečem implementujícím FIDO

cesnet

Více tokenů se stejnými klíči

- GnuPG vytváří *stub* klíče pro každý token při volání `gpg --card-edit`
- Při přechodu na jinou kartu je třeba *stuby* najít a smazat.

cesnet

Děkuji za pozornost

Ondřej Caletka
Ondrej.Caletka@cesnet.cz
https://**Ondřej.Caletka.cz**