Přehled nástrojů pro kryptografii a ochranu soukromí

Beret

11.02.2013

Obsah

Pozn.: Tato prezentace je velmi strohá.

Ochrana uložených dat („off-line ochrana“)

Správa hesel

- šifrované klíčenky
  - Windows: KeePass
  - Linux: KeePassX, GNOME Keyring, KWallet
  - Mac OS: KeePassX, Keychain
- nutné hlavní heslo (nebo šifrovat disk)

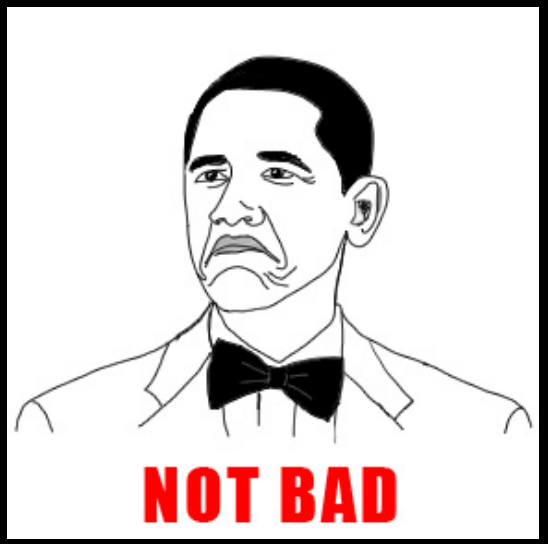
Jak silné má být heslo?

- Project Erebus v2.5
  - 143,8 miliard NTLM hashů za sekundu ($\log_2$ = 37,1)
  - 74,2 miliard MD5 hashů za sekundu ($\log_2$ = 36,1)
  - 25,9 miliard SHA-1 hashů za sekundu ($\log_2$ = 34,6)
  - cena 12 000 USD (cca 225 000 Kč)
  - za 24 hodin dokáže otestovat metodou brute-force:
    - všechna ASCII* hesla do Windows o délce do 8,14 znaku
    - všechna ASCII* hesla v hashi SHA-1 o délce do 7,76 znaku

* počítám abecedu o 95 znacích

Obecné šifrování

- symetrické šifry pro osobní data, sdílené soubory, …
- 7Zip – 256bit AES
- WinRAR – 128bit AES



- ZIP – **opatrně!**
  - WinZip 9.0+ a 7Zip umí 128bit AES a 256bit AES
  - spousta implementací dodnes používá slabou šifru
  - nejsou šifrovány názvy souborů

Obecné šifrování

- GNU Privacy Guard (GnuPG)
  - symetrická i asymetrická kryptografie na libovolné zprávy
  - decentralizované ověřování klíčů – „síť důvěry“
  - všemocný nástroj pro příkazovou řádku: `gpg`
  - grafické nadstavby (Gpg4Win)
  - lze použít na e-mail, soubory, pomocí copy+paste apod.

Šifrování disku

- celý diskový oddíl
- odemčení při startu a probuzení počítače
- ochrana heslem nebo klíčem na flash disku
- za běhu je transparentní
- nástroje:
  - TrueCrypt (Windows, Linux, Mac OS)
  - dm-crypt / LUKS (Linux)

Nástroje pro e-mail

OpenPGP

- PGP, OpenPGP a GnuPG je „skoro to samé“ :-)
- šifrování e-mailů end-to-end
- e-mailové klienty s přímou podporou:
  - Claws Mail (multiplatformní)
  - Evolution (GNOME v Linuxu)
  - K9 Mail (pro Android)
- e-mailové klienty s doplňkem:
  - Thunderbird – doplněk Enigmail

Otevírání příloh

- Evince
  - alternativa pro Adobe Reader
  - otevírá PDF

Schránka na jedno použití

- Mailinator.com
  - použijte adresu cokoliv@mailinator.com a
  - vyzvedněte si poštu na cokoliv.mailinator.com
  - e-maily se uchovávají cca jeden den

Nástroje pro web

Doplňky pro Firefox

- HTTPS Everywhere
- DNSSEC Validátor od CZ.NIC
- Ghostery
- FlashBlock
- AdBlock Plus
- NoScript
- Certificate Patrol

Vyhledávač

- DuckDuckGo

Nástroje pro Internet obecně

Tor

- anonymizační síť
- Tor Browser Bundle obsahuje:
  - samotný Tor
  - vyladěný Firefox
  - Vidalia Control Panel
- lze použít i jako proxy pro jiné aplikace
  - pozor na Tor leak
- pozor na korelaci vstupu a výstupu

Tor

- skryté služby
  - dostupné pouze uvnitř sítě Tor
  - doménová jména končící na `.onion`
  - The Hidden Wiki: `http://kpvz7ki2v5agwt35.onion/`

I2P – Invisible Internet Project

- anonymizační síť
- méně používaná než Tor
- zatím beta verze
- větší důraz na decentralizaci a skryté služby

VPN

- tunel z nebezpečné lokace do bezpečné lokace
  - vyžaduje důvěryhodný server
- protokoly:
  - OpenVPN – dobrý
  - PPTP – nebezpečný
  - proprietární – raději ne
- ve Windows „connect to workplace“
- FIT poskytuje VPN
  - přístup na IPv6
  - přístup k vědeckým knihovnám

Další tipy?