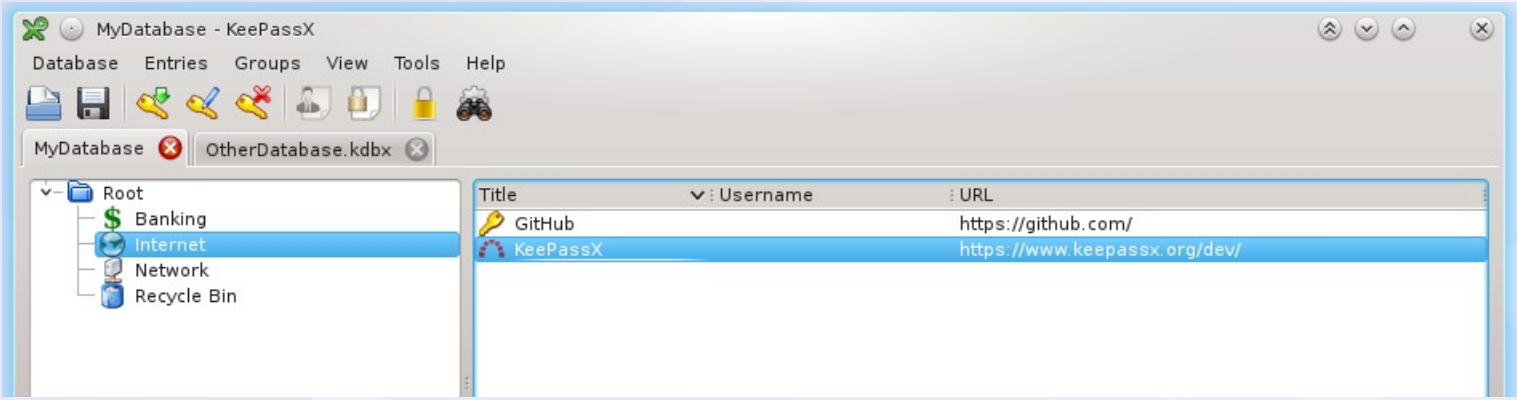
HW password manager

založen na Trezor tokenu

Ondrej Mikle • ondrej.mikle@gmail.com • 20.4.2016

Password managery

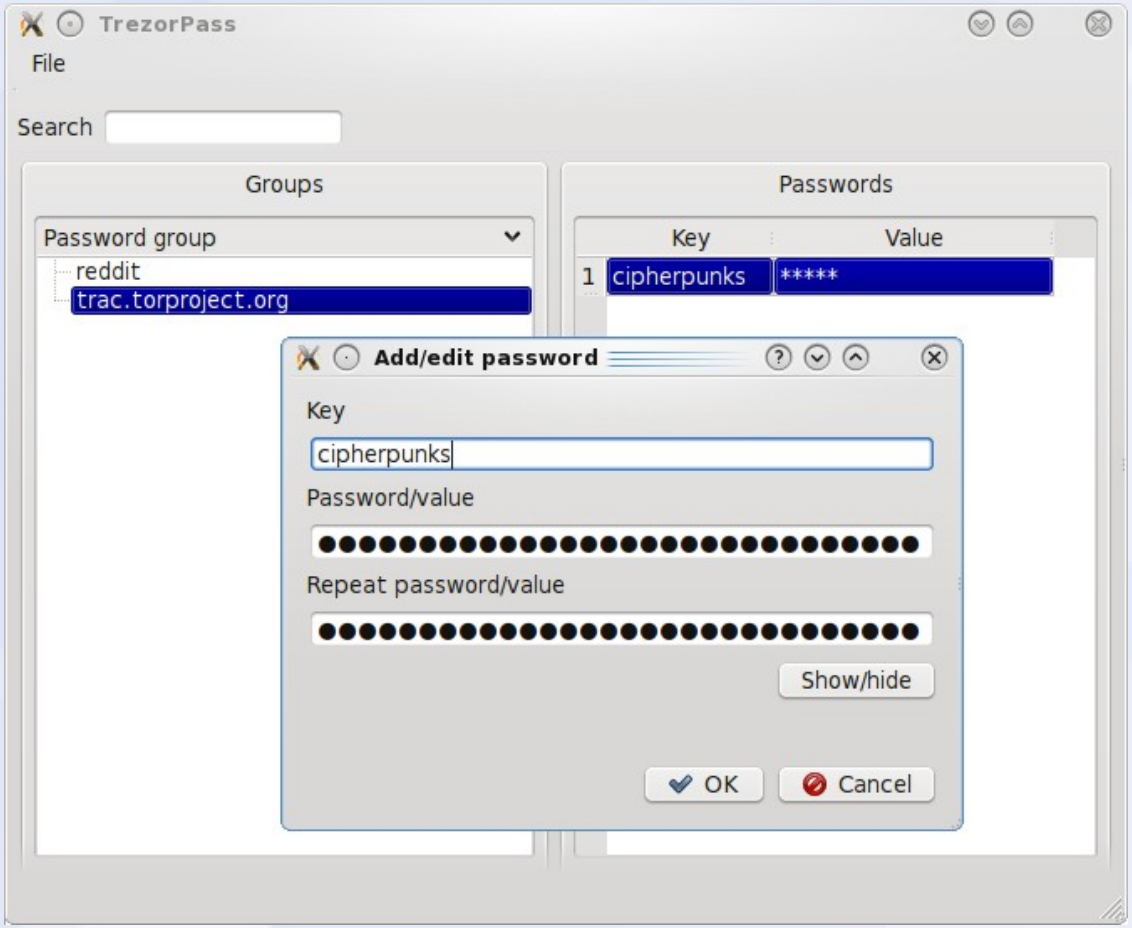
- protože hesla se nemají opakovat a stovky hesel si nikdo nezapamatuje
- Keepass(X), Lastpass, 1-password...



Trezor token

- původně určen pro platby bitcoiny
- připojuje se přes USB (USB hidraw)
- ARM procesor – STM32F2
- první sektory zamknuty – bootloader, seed pro generování klíčů
  - aby to nešlo vyčíst JTAG-em
  - firmware podepsán

TrezorPass


TrezorPass
File
Search
Groups
Password group
reddit
trac.torproject.org
Passwords
Key
Value
1
cipherpunks
*****
Add/edit password
Key
cipherpunks
Password/value
Repeat password/value
Show/hide
OK
Cancel

Rozdíl proti SW pwd managerům

- PIN není možné sniffnout pro malware
  - zobrazuje se permutovaně na displayi
- passphrase slouží jako další část k seedu pro generování klíče
- každé odšifrování passwordu vyžaduje fyzické potvrzení na Trezoru
  - malware nemůže sniffnout všechny hesla najednou (výhoda proti SW managerům)
- implementace v pythonu (PyQt 4)

Implementace

- šifrovaná databáze hesel se ukládá na disk
- šifruje Trezor, klíč nikdy neopustí Trezor
- hesla šifrována s AES-CBC, každá skupina hesel má jiný klíč
- HMAC pro kontrolu integrity
  - Encrypt-then-MAC
- zálohovací RSA klíč, aby šlo exportovat
  - privátní část dešifrovatelná jen Trezorem

Stav SW

- je to proof-of-concept
- bude brzy oficiální ostrá verze (ne ode mne)

Děkuji za pozornost

Ondrej Mikle • ondrej.mikle@gmail.com

Odkazy

- https://github.com/hiviah/TrezorPass