Password Managers

A way to cope with dozens of online accounts

Felix Morsbach

Uppsala University

Sweden

CryptoParty #9

presentation of 23rd January 2020

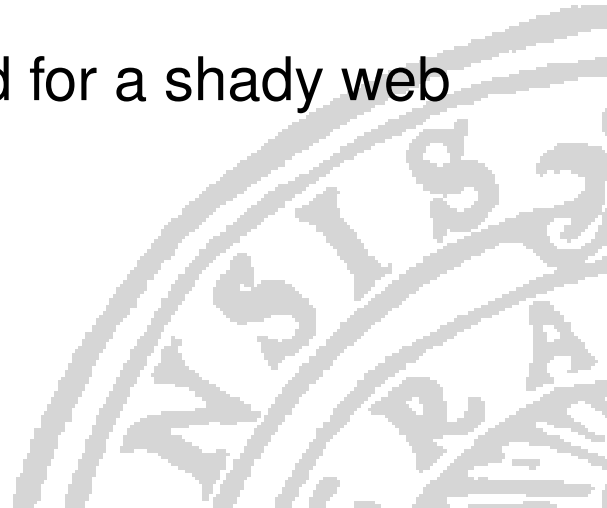
Outline

1. What is the problem?
2. How can one solve it?
3. What actually (not) to do?
4. Making it (more) usable

Reusing physical keys?

Imagine a world in which you would not need a keychain, one physical key for every lock you have access to!

- Would you use the same physical key to your house, your banking deposit, your car and your gym locker?
- So why would you use the same password for a shady web forum and your online banking?



Why reusing passwords is a bad idea

- Your online accounts will be compromised eventually
  - e.g. leaks/breaches/hacks happen all the time, and it will never stop
- One needs a lot of passwords ...
  $\rightarrow$ one for each service
  $\rightarrow$ good passwords are hard to remember
  $\rightarrow$ so you end up making them easy
- Or you end up "inventing the personal password system" that only you can understand
- All these are **toy** security mechanisms for a serious adversary

How can one solve it?

https://imgflip.com/i/2uc7d2

KeePass all the things!

- Use a **unique** and **strong** password for each service you use
- Manage and store them in one central and secure place
- Encrypt them with **one really good password**
  - Generate random passwords
  - If you don't have to remember them you can generate arbitrarily long password, **REALLY** long passwords

    b352cafe513543a7e6e17073aecfa26c55fdadaac
    35ceb3f6fde27a2b7bdd6e6de48575f6123617a41
    c467c0456cb99cc155a1aabbac222a9e4d0c6dc40
    e22f5f6fde27a2b7bdd6e6d2a9e4d0c6d13543ahe

One Option: KeePass

- free and open-source
  - OSI-certified
  - bug-bounties
- easy-to-use and light-weight
  - multiplatform support
  - multiple languages
  - browser add-ons
  - …
- A whole plate of features
  - configurable auto-type
  - multi-user support
  - plugins
  - …

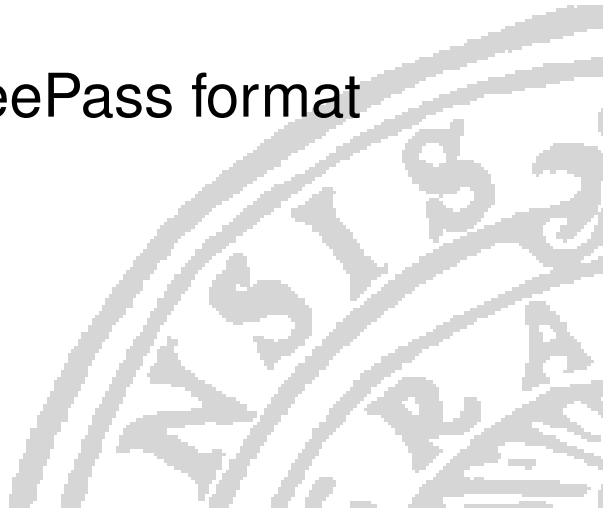
One Option: KeePass

- real desktop client
  - no forced web/cloud BS
  - your master password never leaves your computer/device
- A single encrypted file as database
  - everything gets encrypted
- Unlock via
  - Master password
  - Windows account
  - Key-file
- strong encryption (e.g. AES-256)
  - for more see

    https://keepass.info/help/base/security.html

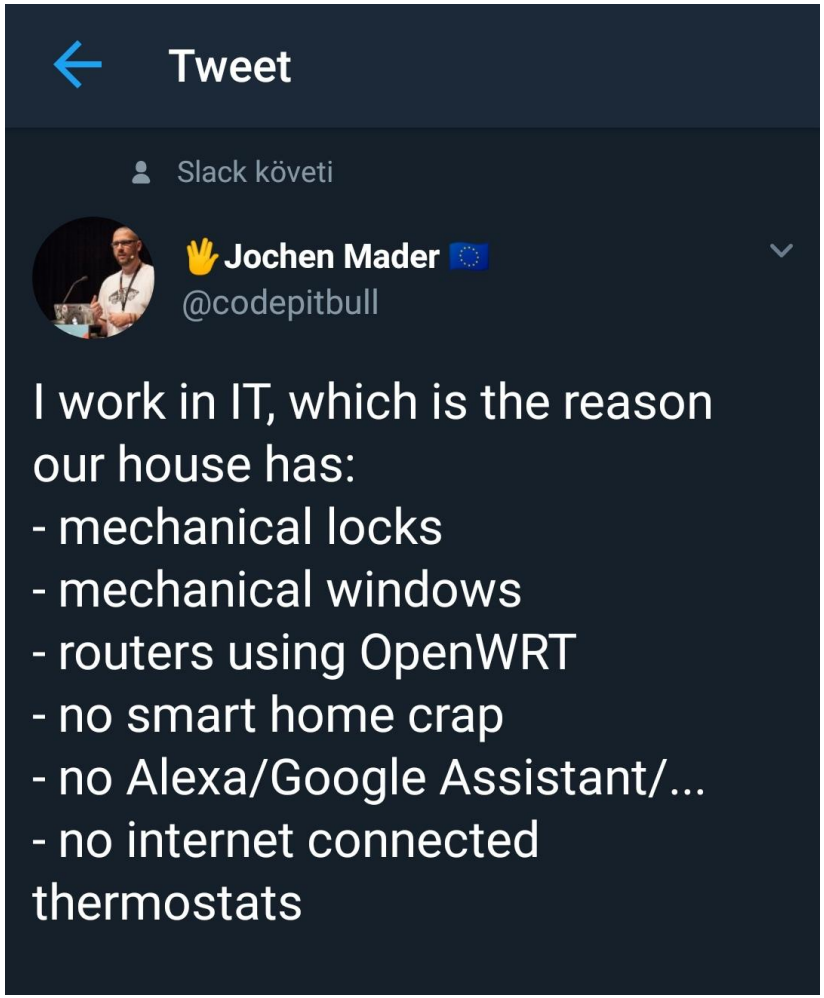
Another Option: KeePassXC

- KeePass is developed in C#, non-native execution on Linux/MacOS
  - can be run through the Mono runtime libraries, but no native look & feel, auto-type etc.
- KeePassXC is developed in C++ with native cross platform support
- Completely compatible with the original KeePass format
- not as feature rich, no plugins



What actually (not) to do?

https://i.redd.it/r5b7xwtvjqb21.jpg



What to store, what not?

- Generally: Everything
- SSH key phrases + Key Agent feature
- Exceptions:
  - Email (the root of your digital life)
  - Banking
  - Anything super important
- Don’t put all your eggs in one basket
  - Security in depth

Multi-Device Synchronization

Multiple options, non is KeePass specific:

- Synchronize with your favourite cloud solution between devices (e.g. Google, OneDrive or Dropbox)
- Host your own ”cloud” solution for synchronization (e.g. Nextcloud)
- Use a P2P synchronization like Syncthing
- (Manual synchronize via Thumb drive/cable)

Going the extra mile

- Additionally lock database with key-file
  - **BACKUP** the key-file locally
- Distribute key files manually to each device you intend to use
- Change passwords on a regular basis
  - use *expires* feature to remind you