



KeePass 2

A free, open-source, light-weight and easy-to-use password manager

Felix Morsbach

Uppsala University
Sweden

CryptoParty #1
presentation of 22nd February 2019



Outline

Why?

How?

What (not)?

Demo

Where?

1. Why?

2. How?

3. What (not)?

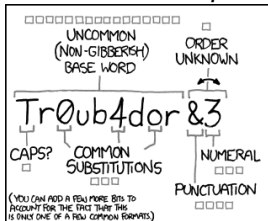
4. Demo

5. Where?



Password strength

<https://xkcd.com/936/>



~28 BITS OF ENTROPY

$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$

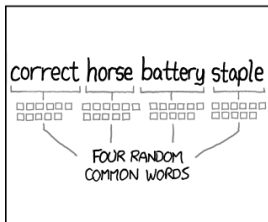
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

DIFFICULTY TO GUESS: **EASY**

WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?

AND THERE WAS SOME SYMBOL...

DIFFICULTY TO REMEMBER: **HARD**



~44 BITS OF ENTROPY

$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$

DIFFICULTY TO GUESS: **HARD**

THAT'S A BATTERY STAPLE.

CORRECT.

DIFFICULTY TO REMEMBER: **YOU'VE ALREADY MEMORIZED IT**

THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

- Why?
- How?
- What (not)?
- Demo
- Where?



No reuse

Why?

How?

What (not)?

Demo

Where?

- Leaks happen all time
 - And it will never stop

- One needs a lot of passwords . . .
 - good passwords are hard to remember
 - make them easy

- Don't rely on "the personal password system"

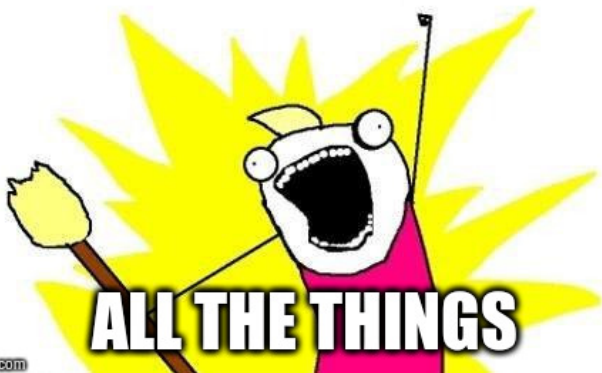
- Would you use the same physical key to your house, your banking deposit and your public storage entity?

- Same password for a shady web forum and your bank?



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

KEE PASS



Why?

How?

What (not)?

Demo

Where?



KeePass all the things!

Why?

How?

What (not)?

Demo

Where?

- Use a unique password for each service you use
- One central and secure place to store all your passwords
- If you don't have to remember it you can generate arbitrarily long password
 - REALLY long passwords

```
b352cafe513543a7e6e17073aecfa26c55fdadaac  
35ceb3f6fde27a2b7bdd6e6de48575f6123617a41  
c467c0456cb99cc155a1aabbac222a9e4d0c6dc40  
e22f5f6fde27a2b7bdd6e6d2a9e4d0c6d13543ahe
```



<https://imgflip.com/i/2uc7xf>

YOU GET A UNIQUE & SECURE PW

**AND YOU
GET A UNIQUE
& SECURE PW**

**AND YOU
GET A UNIQUE
& SECURE PW**

EVERYONE GETS A UNIQUE & SECURE PW

imgflip.com

Why?

How?

What (not)?

Demo

Where?



KeePass2

Why?

How?

What (not)?

Demo

Where?

- 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
 - additional fields like URL
 - groups
 - import & export
 - multi-user support
 - plugins
 - ...



KeePass2

Why?

How?

What (not)?

Demo

Where?

- real desktop client
 - no forced web/cloud BS

- 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>



Trust issues?

Why?

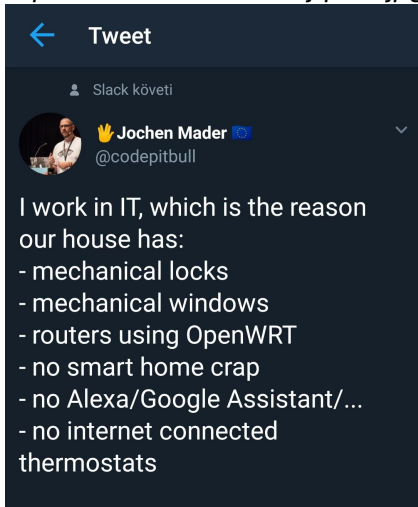
How?

What (not)?

Demo

Where?

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





What (not)?

Why?

How?

What (not)?

Demo

Where?

- Generally: Everything

- Exceptions:
 - Email (the root of your digital life)
 - Banking

- Don't put all your eggs in one basket
 - Security in depth



UPPSALA
UNIVERSITET

Demo

Why?

How?

What (not)?

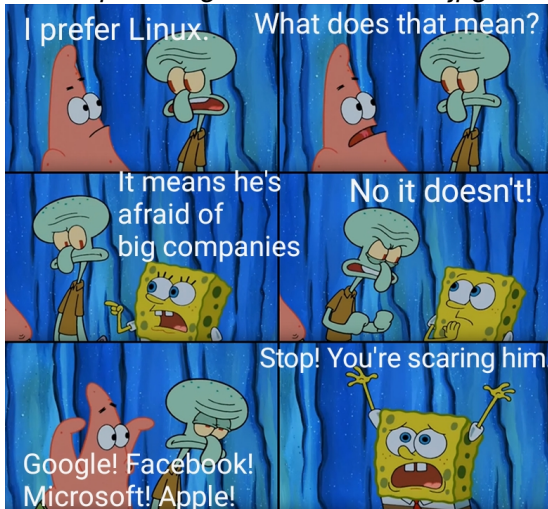
Demo

Where?



Synchronization

<https://i.imgur.com/WJ114cM.jpg>



Why?

How?

What (not)?

Demo

Where?



Synchronization and Usage

- Lock database with key-file AND password
 - **BACKUP** the key-file locally

- Synchronize database with your favourite cloud solution between devices (e.g. google, onedrive or dropbox)

- Distribute key files manually to each device you intend to use

- Change passwords on a regular basis
 - use *expires* feature