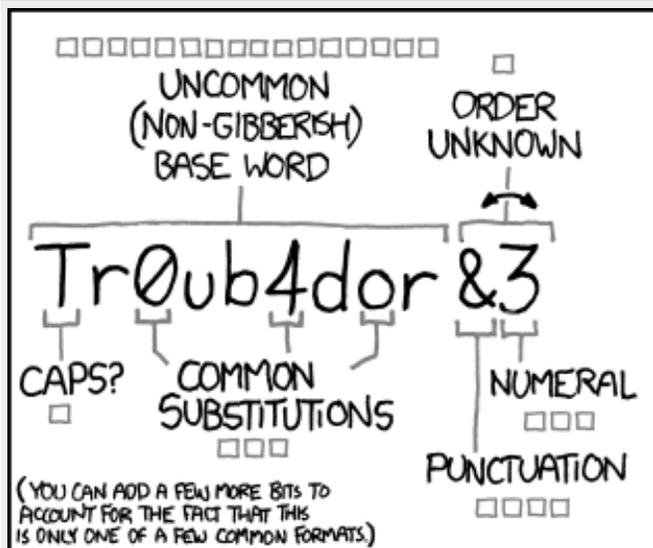


KeePassX **(lightning)**

Danny Robson



~28 BITS OF ENTROPY

□□□□□□□□ □

□□□□□□□□ □□□

□□□□ □

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

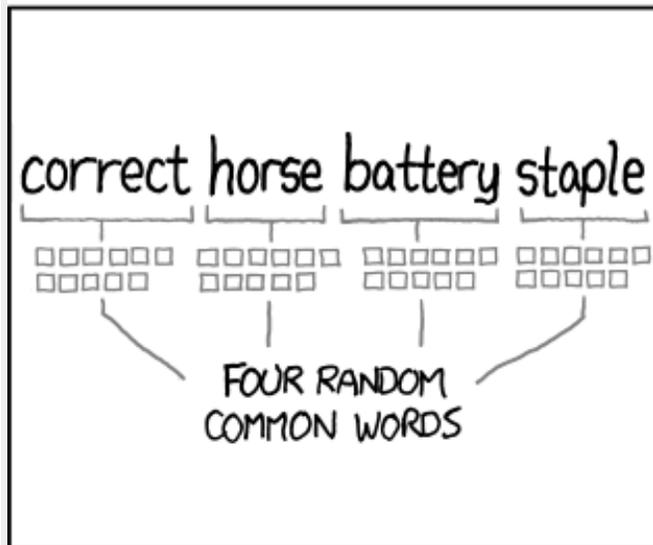
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

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.

Survey

- How long is your password?
- How random is your password?
- How long since you last changed your password?
- How many passwords do you use?

What?

KeePassX is a cross-platform GUI for secure password:

- generation
- storage/query
- input

Demo

Tricks

- Store in OwnCloud/Seafile/etc
- Use the query features
- Use timed expiration

Links

- <https://www.keepassx.org/>
- <https://haveibeenpwned.com/>