Password Hygiene

CUCUG
Quentin Barnes
July 17, 2025

Yet Another Hack, Google This Time

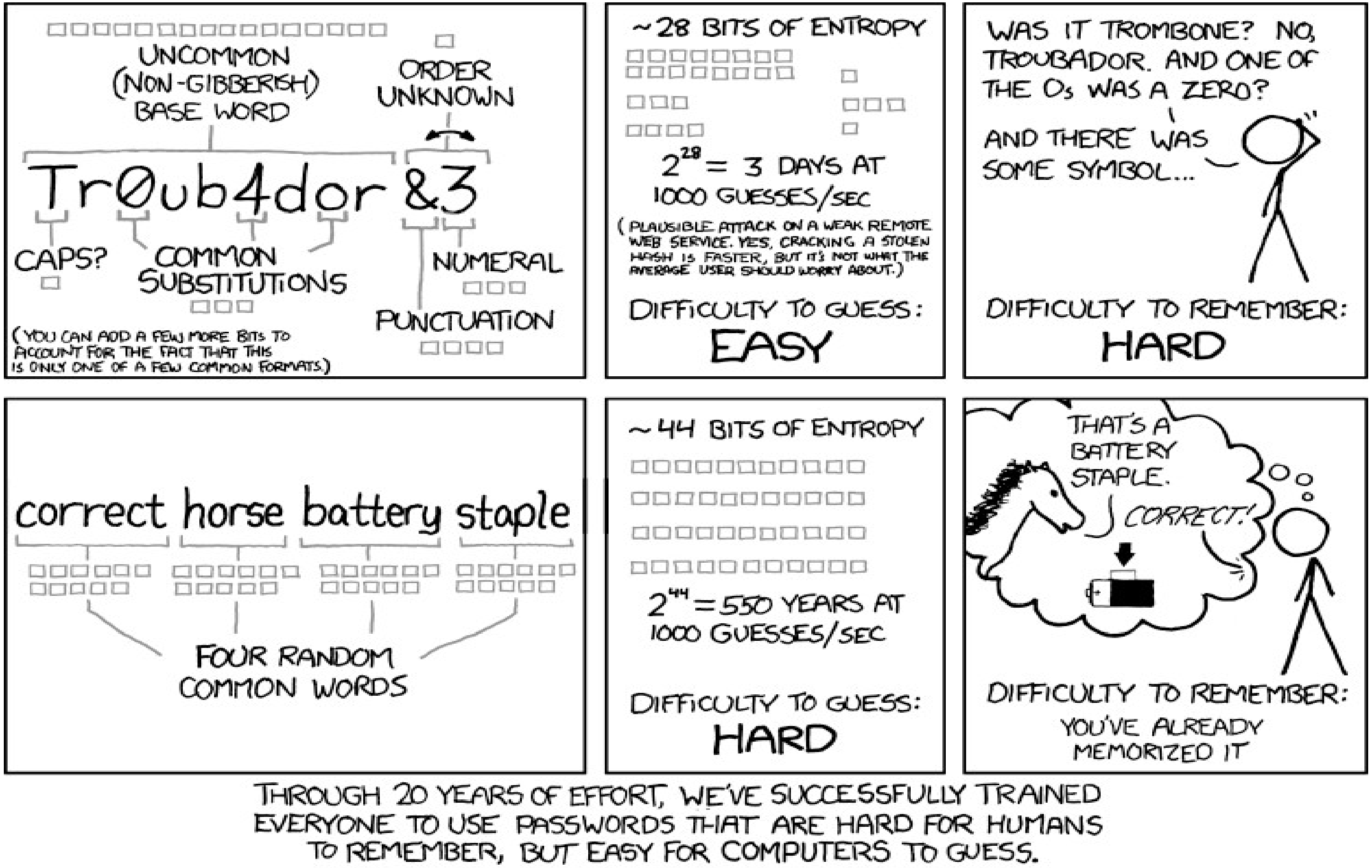
- Was reading our newsletter today
- “Gmail Warning Just Dropped-Reset Your Password ASAP” article
- Today seems like a good day to talk about “password hygiene”

Easy to Remember Passwords

- People make passwords themselves about them themselves
  - Pet’s/friend’s/relative’s name or favorite locations
  - Adding special date strings (MMDD) to a base password
  - Adding a sequence digit to the previous password
  - Slightly modifying password based on site’s/product’s name
  - Reusing passwords between different services
- Making passwords like these are saying “hack me!”

So People Use Random Passwords

-
  ```
  $ pwmake 60
  bIcsUByriz64G
  ```
- Now what can you do with that?
- Hard to remember, especially dozens of them!
- Write it down on post it notes?
- Typing it on a phone keyboard is annoying


UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor &3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 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 Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER: HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 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.

https://xkcd.com/936/

Making Password Phrases

- Diceware word list
  - https://theworld.com/~reinhold/dicewarewordlist.pdf
- Real 5d6 dice
- “d20 Calculator” app

Password Phrases

- Ok, so random password phrases good
- But so, so many to make them all unique
- Password managers to the rescue!
  - Only one phrase needed to unlock it

Common Password Managers

- 1Password
- Lastpass
- NordPass
- KeePass
- Proton Pass
- Bitwarden

Bitwarden

- Multi-platform / Cross-platform
  - Browsers, MS Windows, MacOS, Linux, iOS, Android
- Free as in beer (no cost for personal use)
- Free as in freedom (FOSS)
- Multitude of tools
  - Built-in generator for passphrases
  - Easy import / export
- Cloud and self-hosting

Demo!