CRYPTO PARTY

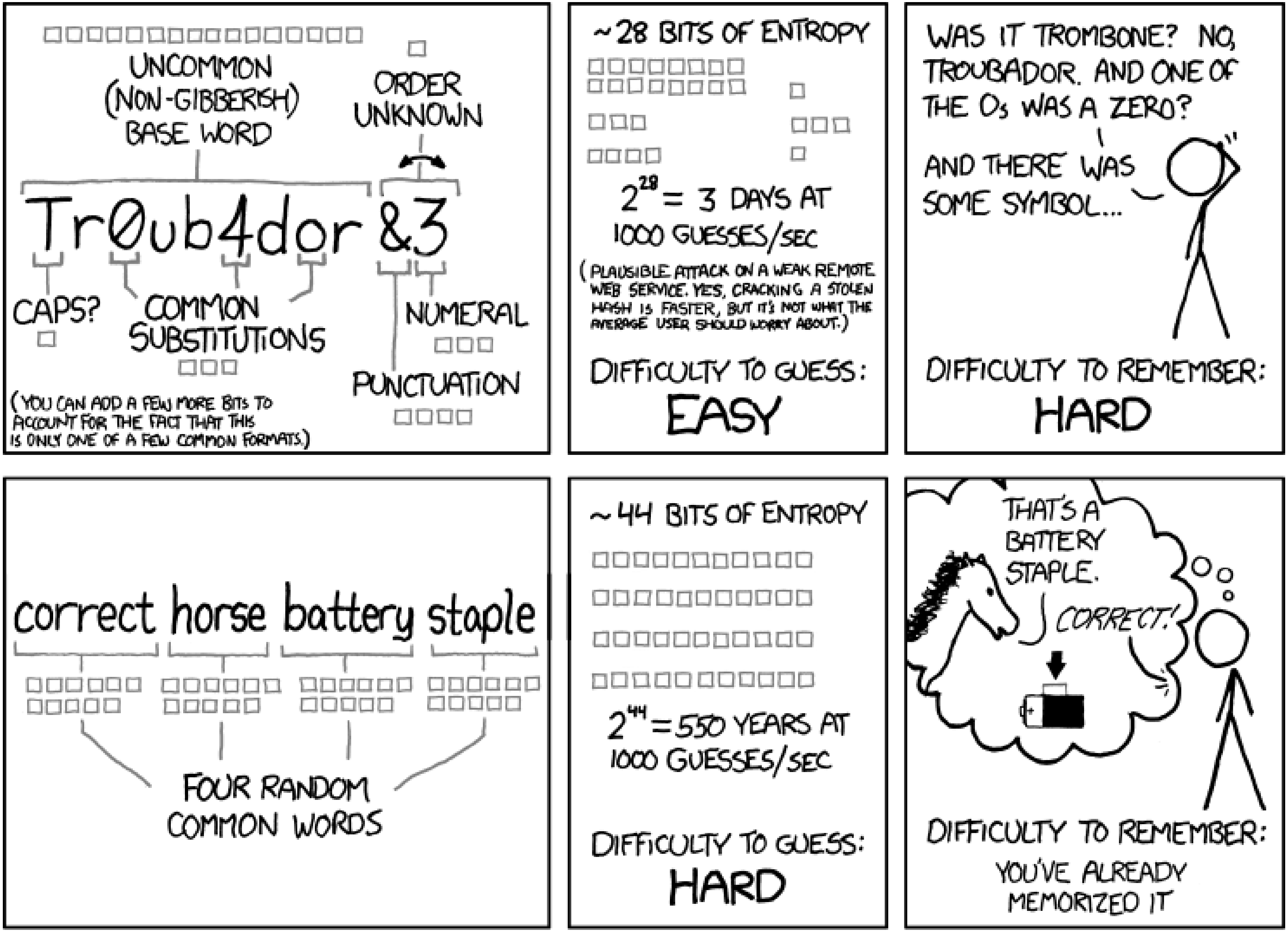
Passwords

Passwords

- Creating good passwords
- Syncing your passwords
- Multi-Factor Authentication

~~Passwords~~ Passphrases

- If you have a short password, your encryption doesn't matter.
- Technology to crack passwords today is very fast, and only gets faster
- Length is the easiest way to have a strong passphrase
- “correct horse battery staple” = easy for people, hard for computers


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.

Syncing your password

- Password manager (KeePassX, Lastpass)
- Write them down in a journal

Two Factor Authentication

Resources

- https://www.cryptoparty.in/Boston
- https://PrivacyTools.io
- https://prism-break.org/en/
- https://emailselfdefense.fsf.org/en/index.html
- https://www.torproject.org
- Surveillance Self-Defense guide: https://ssd.eff.org/
- https://whispersystems.org/
- https://panopticlick.eff.org/

Licenses

- This presentation is released to the Public Domain under the terms of CC0 1.0
- https://creativecommons.org/publicdomain/zero/1.0/
- Except for the XKCD comic which is CC BY-NC 2.5
- https://creativecommons.org/licenses/by-nc/2.5/