History of pass-words

- pass-WORD
- Originally used by people, esp. friend vs foe
- Used along with username in original digital accounts

How passwords have evolved

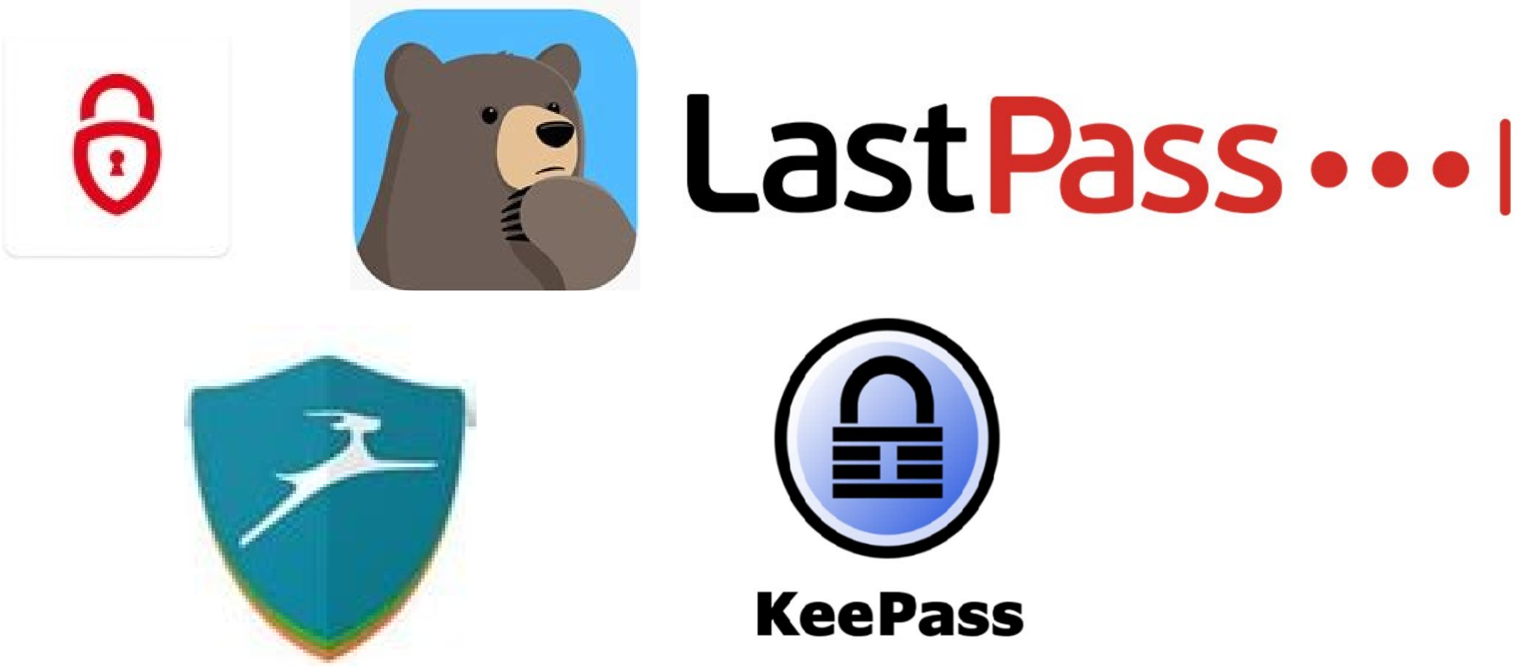
- Secret word
  - Dictionary attack
- Word + stuff
  - Dictionary attack with rules
- More complicated word + stuff
  - Rules, password spraying, steal passwords
- Long string of random characters
  - Reasonably, can only be stolen

How your passwords can be stolen

- Not limited to:
  - Phishing
  - Other types of social engineering
  - Not using httpS
  - Taken from un-encrypted cookies
  - Stolen from website/server
  - Brute-forced with rules

Solution #1: Password Managers

- Never repeat important passwords



- Start downloading one now, we'll be creating accounts in a minute

Math time!

- 8

Math time!

- 8
- 26

Math time!

- 8
- 26
- 26^8 = 208,827,064,576 – few minutes

Math time!

- 8
- 26
- 26^8 = 208,827,064,576 – few minutes
- 52^8 = 53,459,728,531,456 – few hours

Math time!

- 8
- 26
- 26^8 = 208,827,064,576 – few minutes
- 52^8 = 53,459,728,531,456 – few hours
- 96^8 = 7,213,895,789,838,336 – few months

Math time!

- 8
- 26
- 26^8 = 208,827,064,576 – few minutes
- 52^8 = 53,459,728,531,456 – few hours
- 96^8 = 7,213,895,789,838,336 – few months
- 96^12?

PASS-phrases

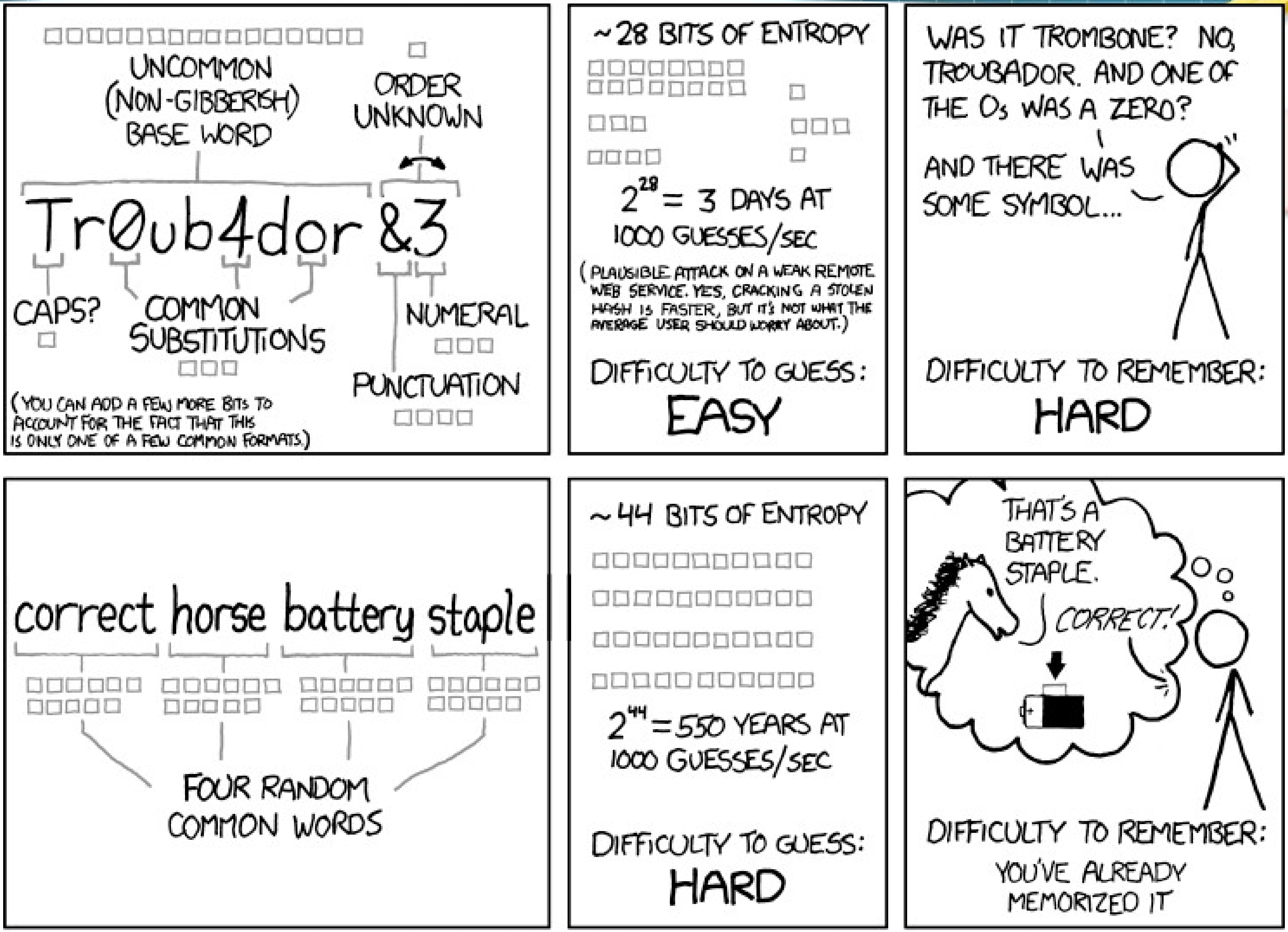
- Characters work, but what if we used something else?

PASS-phrases

- Characters work, but what if we used something else?
- 7000

PASS-phrases

- Characters work, but what if we used something else?
- 7000
- 7000^5 = 16,807,000,000,000,000,000 – eternity


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.

PASS-phrases

- Characters work, but what if we used something else?
- 7000
- 7000^5 = 16,807,000,000,000,000,000 – eternity
- Easier to remember
- Dice-Ware

Multi-Factor Authentication (specifically 2FA)

- Important password can still be stolen
- How system quickly determine who you are?
- Something you:

  - Have
  - Know
  - Are

- Example:

So what should you do:

- Use PWMs on everything
- Use passphrases frequently
- 2FA as much as possible
- TELL EVERYONE