Password Management

Richard Wall

HHICC – Presentation

Feb 13th 2023

Don't believe Hollywood.
No one can partially guess your password.

- They either guess the entire thing or nothing.

- They cannot break part of the password and then break the other parts. It's all or nothing.

- md5 hashes for Password123 and password123

Password123 =
a907ac8f85bbece3069a52a39947b287

password123 =
7576f3a00f6de47b0c72c5baf2d505b0

- What makes a good password?

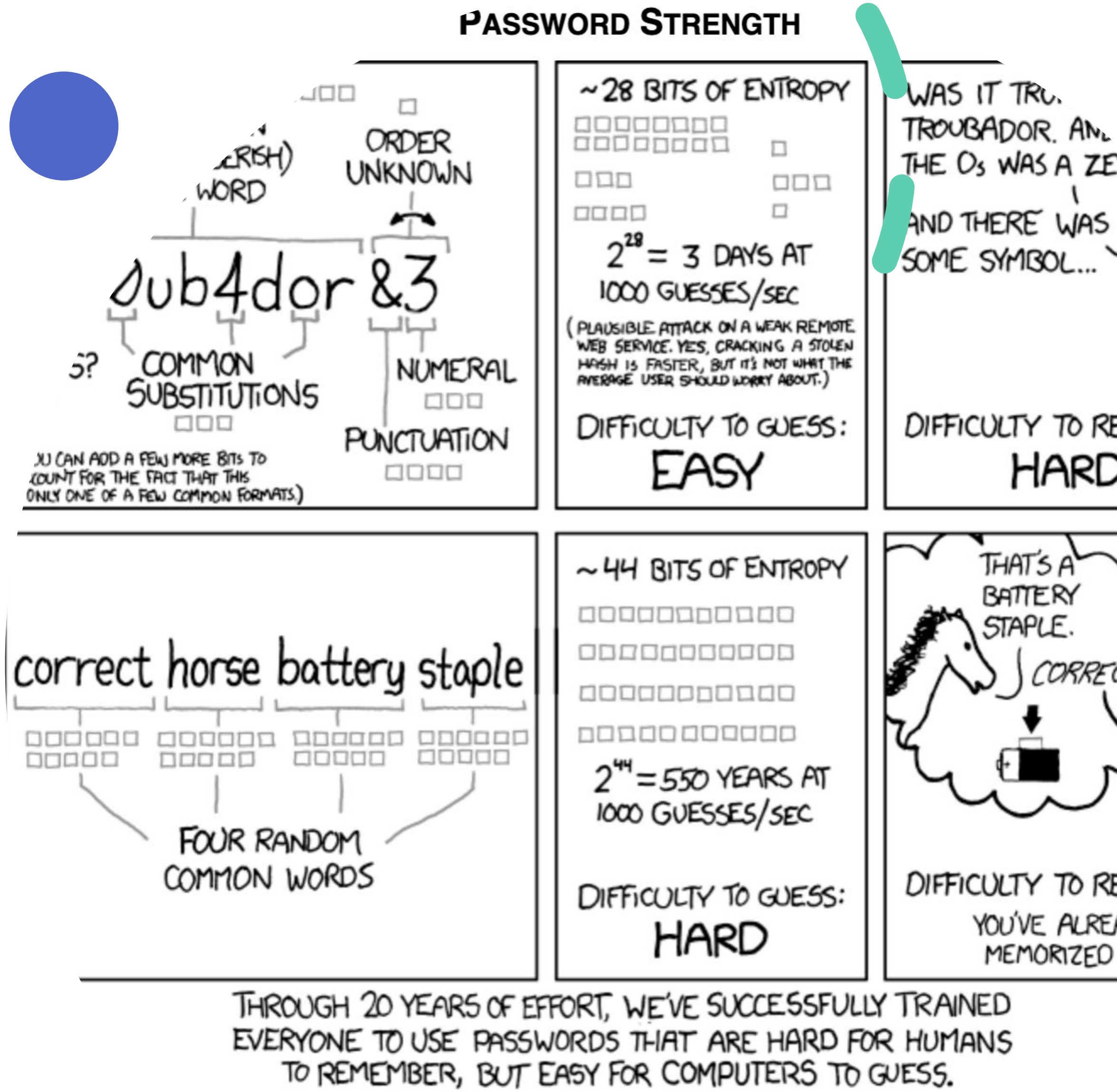
- Generally: A long password makes a strong password

- A long password would be over 9 characters, but don't be fooled.

- The most common password used is: "password1"

- It IS a 9 character password, but it is one of the first to be cracked because it is so commonly used.

- Password1, password1234 and password! are also very common passwords and should be avoided.


PASSWORD STRENGTH
(...ERISH) ...WORD
ORDER UNKNOWN
Dub4dor&3
5?
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 TRO... TROUBADOR. AN... THE 0s WAS A ZE...
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO RE... 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.
CORRE...
DIFFICULTY TO RE... YOU'VE ALRE... MEMORIZED...
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.

- Password Entropy. How easy is it to guess a password?

  - If you only use lower case letters you are only using a 26 letter character set.

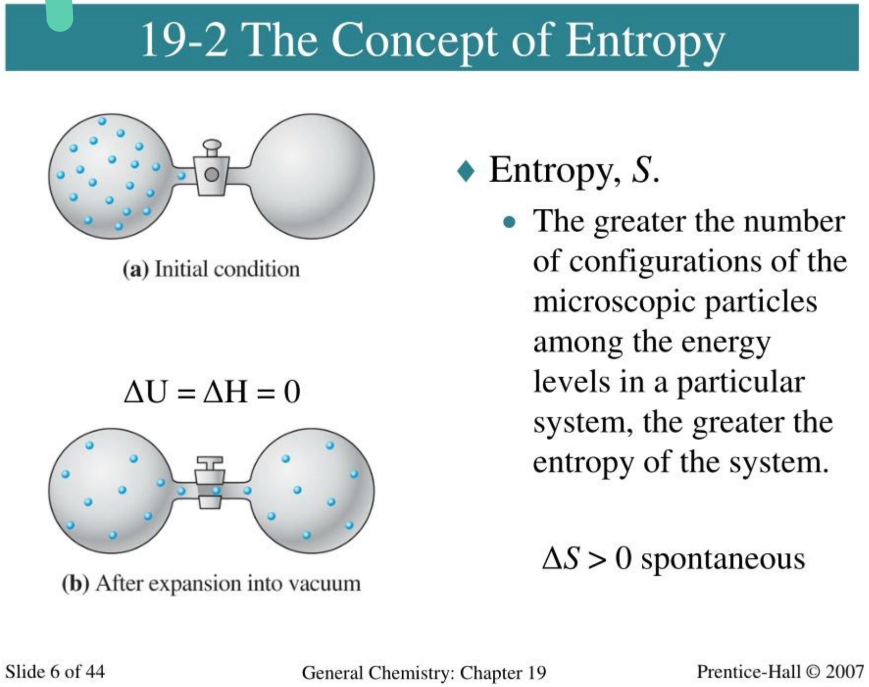
So: 26^(number of characters in the password)

  - If you add upper case letters and numbers you've increased the complexity to:

62^(number of characters in the password)

  - Adding the most common special characters brings the complexity to:

95^(number of characters in the password)



19-2 The Concept of Entropy

(a) Initial condition

$\Delta U = \Delta H = 0$

(b) After expansion into vacuum

- Entropy, *S*.
  - The greater the number of configurations of the microscopic particles among the energy levels in a particular system, the greater the entropy of the system.

$\Delta S > 0$ spontaneous

Slide 6 of 44 General Chemistry: Chapter 19 Prentice-Hall © 2007

Single dictionary words should be avoided no matter the length.

- 8 Characters - Necklace

- 28 characters - Antidisestablishmentarianism

- These words have the same level of entropy. 33,000^1 = 33,000

- It would only take 33,000 guesses to crack either of these passwords using a “dictionary” attack.

- Using truly random characters gives the best results but are hard to remember and type.

- Upper Case + Lower Case + Numbers + Special Characters

- 20 Characters - %U@nv7UitrMuSvW4t7p5

- Guesses needed to crack password lengths:

- 95^8 = 6,634,204,312,890,625
- 95^9 = 630,249,409,724,609,400
- 95^10 = 59,873,693,923,837,890,000
- 95^12 = 5,403,600,876,626,370,000,000,000
- 95^15 = 463,291,230,159,753,400,000,000,000,000
- 95^20 = 3,584,859,224,085,422,000,000,000,000,000,000,000,000

- Diceware Password generation: https://www.eff.org/files/2016/07/18/eff_large_wordlist.txt

- Word list of 7776 words.
- Five dice and each roll gives one word.

- Succulent-Panoramic-Floss-Foothold-Gloomy-Gleaming

- 7776^4 = 3,656,158,440,062,976
- 7776^5 = 28,430,288,029,929,700,000
- 7776^6 = 221,073,919,720,733,400,000,000
- 7776^7 = 1,719,070,799,748,422,000,000,000,000

- Add a number to make it more complex
- Succulent-Panoramic-Floss4-Foothold-Gloomy-Gleaming

Password creation tricks:

Rhyming:

- toeheadedBoyzlovetheirtoys!
- My gal is my best pal. = Mygalismy#1pal?
- My beau is a little slow. = Mybeauisalittle2slow

Palindromes like passwords:

- $carface-ecafracS

Movie references:

- Scarface has a scar. = $carfacehasascar!

More Password creation tricks:

Say hello to my little friend! = Sayhell02mylittlefiend!

- Music references:

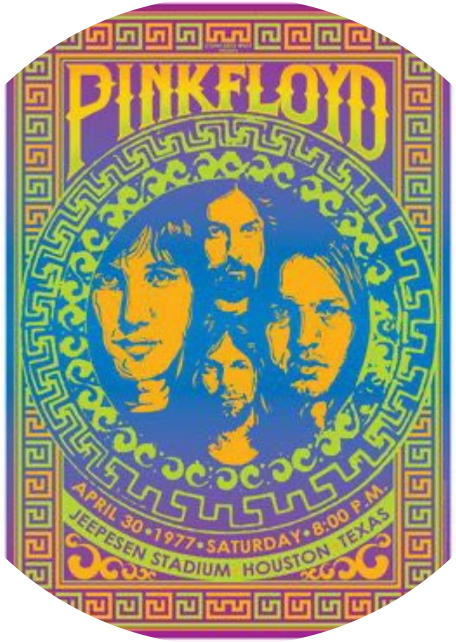
NikkiStixxdoesdrummingtrix!

Stairway to Heaven = Hairway2steven!

Pink Floyd Concert in Jeppesen Stadium on 4/30/77. It poured down rain on us. I went with my brother and his girlfriend.

pink@jepN77wasAwesome!

- Think of passwords before you need them.


PINKFLOYD
APRIL 30 • 1977 • SATURDAY • 8:00 P.M.
JEEPESEN STADIUM HOUSTON TEXAS

What does it take to break a password?

- They don't "break" the password. They make a guess, hash the guess and compare the hash to the hash that was stolen.

- Two programs that are often used to crack passwords:

John the Ripper and **Hashcat**.

- The fastest that I've seen to date can generate nearly 400 billion guesses per second. This was done on a rig set up for crypto-mining and has 25 graphics cards installed.

- A reasonably fast computer can generate about 3.5 million guesses per second.

Making passwords harder to crack

- PBKDF2 (Password-Based Key Derivation Function 1 and 2)

- Is a method to slowdown the number of guesses that can be performed each second.

- The PBKDF2 value should be set between 600,000 and 1,000,000

- The computer used for cracking a password has to iterate each guess to the number that the PBKDF2 is set to, so instead of making billions of guesses per second it can only make thousands of guesses per second.

More Security

- 2fa - Two Factor Authentication is a second form of authentication to secure your accounts if your password gets stolen. They are usually a 6 or 7 digit code that is sent to your phone or email.

- TOTP – Time-based One Time Password is similar to 2fa however it uses third part apps or hardware keys to generate the password.

YubiKey 5C NFC

Password Managers:

- Apple Keychain
- 1Password
- Bitwarden
- Keepass, Dashlane, Lastpass
- Windows?