

Computer & Network Security

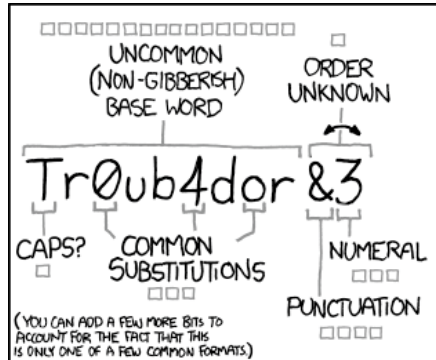
Lecture 7-1

Computers & Society (CPSC 430)

Kevin Leyton-Brown

<https://www.cs.ubc.ca/~kevinlb/teaching/cs430>

Password Strength



~28 BITS OF ENTROPY

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

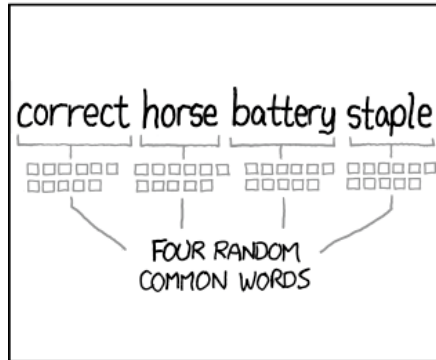
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)

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.

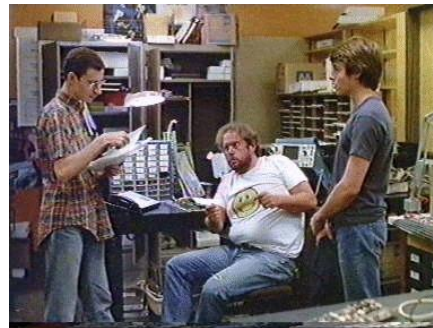
CORRECT!

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.

Hackers

- **Hacker (original meaning):**
 - Explorer, risk-taker, technical virtuoso
 - Values free exchange of information; mistrusts authority; values technical skill; holds an optimistic view of technology
- **Hacker (ultimate meaning):**
 - Teenagers accessing corporate or government computers
 - Stealing and/or destroying confidential information
- **What hasn't changed: hackers' public image**



Ethics of Hacking

- Parallels between hackers/phreaks & MP3 downloaders
 - Establishment overvalues intellectual property
 - Use of technology as a “joy ride”
 - Breaking certain laws considered not that big a deal
 - (Guess what the police, RIAA thinks about these arguments?)
- *Have you ever hacked anything?*
- *Which, if any, forms of hacking do you consider ethical?*
- *Is it wrong to learn hacking or phreaking skills, if these skills are never put to use?*

Malware: Evil Code that can Run on Your Computer

- **Viruses**

- What is a virus?
- *Have you ever (knowingly) gotten one?*

- **Worms**

- What is a worm? How is it different from a virus?
- *Is it wrong to distribute a virus or worm that doesn't harm anyone?*

- **Trojan Horses**

- What is a Trojan horse? How is it different from the first two?

- *Do the victims of a virus/worm/Trojan horse share responsibility for being attacked if their system is not up to date?*

Malware II: More Evil Code

- **Spyware/Adware**

- What is spyware? What is adware?
- *Is it ever moral to install spyware/adware on a user's computer without their consent?*

- **General-purpose Defensive Measures**

- security patches
- anti-malware tools
- firewalls
- *Anything else?*