

Computer & Network Security

Lecture 7-1

Computers & Society (CPSC 430)

Kevin Leyton-Brown

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

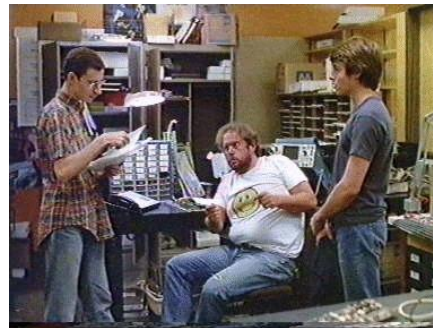
Password Strength

<p>□□□□□□□□□□□□□□ □ UNCOMMON (NON-GIBBERISH) BASE WORD ORDER UNKNOWN</p> <p>Tr0ub4dor&3</p> <p>CAPS? COMMON SUBSTITUTIONS NUMERAL PUNCTUATION</p> <p>(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)</p>	<p>~28 BITS OF ENTROPY</p> <p>□□□□□□□□ □ □□□□□□□□ □ □□ □ □ □ □ □□□□ □ □</p> <p>$2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$</p> <p>(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.)</p> <p>DIFFICULTY TO GUESS: EASY</p>	<p>WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE 0s WAS A ZERO?</p> <p>AND THERE WAS SOME SYMBOL...</p> <p>DIFFICULTY TO REMEMBER: HARD</p>
<p>correct horse battery staple</p> <p>□□□□ □□□□ □□□□ □□□□</p> <p>FOUR RANDOM COMMON WORDS</p>	<p>~44 BITS OF ENTROPY</p> <p>□□□□□□□□ □□ □□□□□□□□ □□ □□□□□□□□ □□ □□□□□□□□ □□</p> <p>$2^{44} = 550 \text{ YEARS AT } 1000 \text{ GUESSES/SEC}$</p> <p>DIFFICULTY TO GUESS: HARD</p>	<p>THAT'S A BATTERY STAPLE.</p> <p>CORRECT.</p> <p>DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT</p>

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**



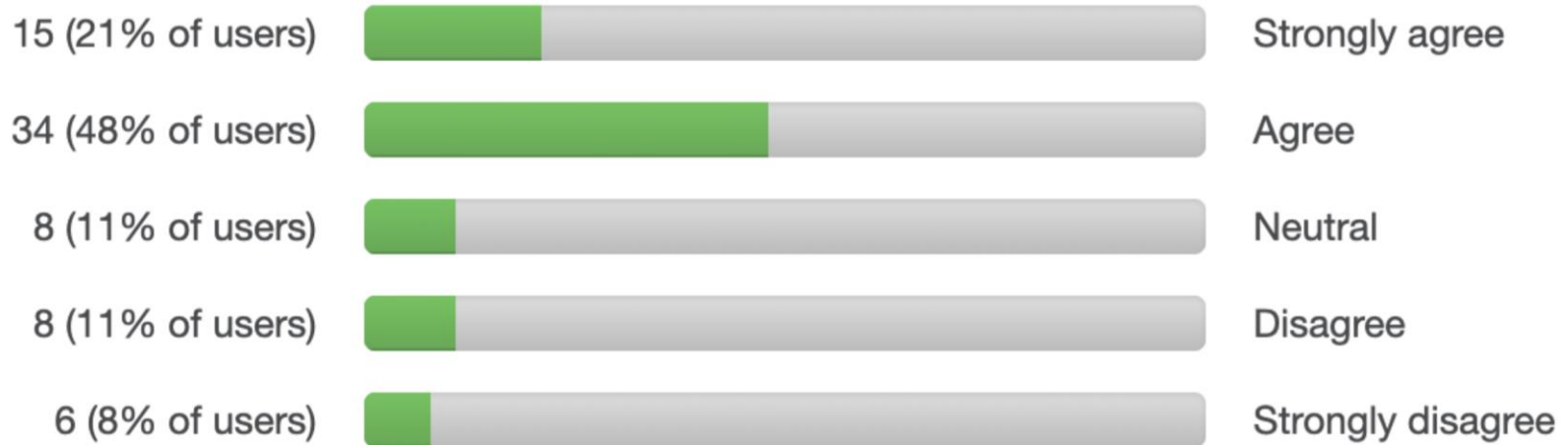
Ethics of Hacking

- 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?*

Computer and Network Security

“Canadians should be able to vote online in federal, provincial and municipal elections.”

A total of **71** vote(s) in **1465** hours



Online Voting

- **Motivation:**

- More people would vote
- Votes would be counted more quickly
- Cost less money
- Avoid disputed elections like Florida 2000
- Eliminate ballot box tampering
- Software can prevent accidental over-, under-voting

- **Risks:**

- Gives unfair advantage to those with computers
- More difficult to preserve voter privacy
- More opportunities for vote selling
- Obvious target for a DDoS attack
- Security of election depends on security of home computers
- Susceptible to phony vote servers
- No paper copies of ballots for auditing or recounts

