Password Strength

- **Tr0ub4dor & $3**
  - Caps?
  - Common Substitutions
  - Numerical
  - Punctuation
  - ~28 bits of entropy
  - $2^{28} = 3$ days at 1000 guesses/sec
  - Difficulty to guess: Easy
  - Difficulty to remember: Hard
  - Was it trojan? No, troubador, and one of the Os was a zero?
  - And there was some symbol...

- **Correct Horse Battery Staple**
  - Four random common words
  - ~44 bits of entropy
  - $2^{44} = 530$ years at 1000 guesses/sec
  - Difficulty to guess: Hard
  - 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?*

• **Drive-by Downloads**
  – What is a drive-by download?
  – *What do you think the best defenses are against them?*

• **General-purpose Defensive Measures**
  – security patches
  – anti-malware tools
  – firewalls
  – *Anything else?*
Attacks: how mean computers hurt nice computers

• How:
  – Phishing
    ▪ Have you been targeted? Has an attack been successful?
  – [Distributed] Denial of Service
  – Ransomware attacks

• Why:
  – Cybercrime: professionalization of malware
    ▪ renting botnets (DDoS; spam)
    ▪ stealing credit card numbers, passwords