Lecture 7-1
Computer and Network Security

Addison-Wesley
is an imprint of
PEARSON

Participation Quiz

You are the conductor of a train. It is headed down on one track where you see 5 workers fixing the track. They cannot hear, see, or feel the train coming. You know for a fact that the train is going fast enough to kill them if a collision occurs. However, you notice there is an alternate track ahead that you can switch the train onto. It has 1 worker and again, she cannot hear, see, or feel the train coming. Do you make the switch to the alternate track?

A: Make the switch, 5 live and 1 dies

B: Do not make the switch, 5 die and 1 lives

Participation Quiz

You are a doctor working at a hospital. You have 5 patients. They are in dire need of an organ; a different one for each patient. They need a new organ immediately or they will die. Thinking fast, you remember that there is a patient of yours next door who just came for a check-up. He is asleep. You know that if you do not take his organs for transplant your 5 patients will die. If you do take the organs, they will survive (and for the sake of argument, assume they will have a normal life after transplant). There are no other options. Do you take the organs?

A: Take the organs, 5 live and 1 dies

B: Leave the patient alone, 5 die and 1 lives

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

Phreaks

- Phone phreak: person who manipulates phone system
  - Stealing or guessing long-distance telephone access codes
  - Use a “blue box” to get free access to long-distance lines: 2600 Hz (anyone remember 2600 Magazine?)
- 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?)

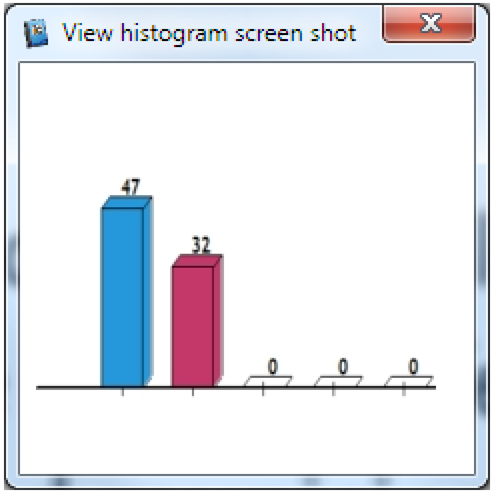
- *Have you ever hacked anything?*
- *Which, if any, forms of hacking do you consider ethical?*
- *Is it wrong to learn hacking or phreaking skills, if these skills are never put to use?*

Open Wifi, Sidejacking and Firesheep

- Open wifi: unencrypted radio broadcast
  - If the connection itself is not encrypted, anyone connected to the same access point can see all packets
  - Often login is encrypted, rest of session is not
- Sidejacking: capturing cookie used to maintain a session
  - If you’re logged in to a site that uses such an open cookie, I get all of your access rights
- Firesheep
  - free Firefox plugin, makes sidejacking easy for average users
  - author’s intention was to encourage websites to adopt better security practices
  - *What do you think of the ethics of his action?*

Computer and Network Security

"Canadians should have the right to vote online in federal, provincial and municipal elections."



Based on slides © 2011 Pearson Education, Inc. Publishing as Pearson Addison-Wesley

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 home 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

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**
- **Why:**
  - **Cybercrime: professionalization of malware**
    - renting botnets (DDoS; spam)
    - stealing credit card numbers, passwords
  - **Cyberwarfare: states as actors or targets**
    - North Korea vs USA gov, corporate sites (2009)
    - Russia vs Georgia during and after South Ossetia war (2008)
    - Stuxnet (2009-)
    - A variety of government, activist sites during Arab Spring (2011)
    - Anonymous