Lecture 7-1
Computer and Network Security

Addison-Wesley
is an imprint of
PEARSON

Participation Quiz

Which destination would you choose?

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?*

Encryption

- Method for concealing the content of a message
- Symmetric encryption:
  - Single key used to encrypt and decrypt a message
  - Problem: How does sender get key to receiver?
- Public-Key encryption (e.g., RSA):
  - Each person has two keys: public and private
  - To send ***R*** a message, encrypt it with ***R***'s public key
  - ***R*** decrypts message with ***R***'s private key
  - No need to communicate private keys
- SSL (https://...) is based on public-key encryption:
  - Upon connection, server reports its public key and a trusted certificate authority that can verify it. The client may verify the key.
  - The client encrypts a random number with the server's public key and sends the result to the server.
  - The server decrypts it with its private key.
  - From the random number, both parties generate key material for encryption and decryption.

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?*