Lecture 9 security continued

- demo: video iPod
- iPod passed around class
- "splotchy look" resulting from lossy compressed video
- a brief tour of video iPod controls
- question: Do the headphones need to be in for continuous play?
- answer: It seems to pause the video.
- Announcements: section: disinfecting a PC, workshop: digital photography
- Digital cameras
    - showed samples from Dan's website
    - spoke about types of digital cameras
    - use flash memory in digital cameras
    - flash media readers
    - typical memory sizes: 256 MB, 512 MB, 1 GB
    - optical zoom vs. digital zoom
    - file formats: JPEG, TIFF, RAW
- defenses against threats to privacy and security
    - Scrubbing, “wiping”
        - Overwrite existing data
        - Allows secure deletion of data
        - Darik’s Boot and Nuke
    - Firewall

  - Conventional sense: blocks passage of flames from one building to another
  - In a similar spirit, this firewall prevents information flowing from one network to another
  - Traditionally installed between the network and the whole internet.
  - Allows companies to block (and allow) certain services
  - This functions by blocking connections between ports:
    - HTTP: port 80
    - SSH: 22
    - SMTP: 25
    - HTTPS: 443
  - Watch all packets and drops (ignores) packets destined for blocked ports.
- Proxy Server
  - A proxy server does something on your behalf.
  - Your router acts as a proxy server – when you contact CNN, your router intercepts the request and submits it for you. When CNN replies, it does not reply directly to you but to your router.
- VPN – "Virtual Private Network"
  - Like a tunnel between one network (or computer) and another network.
  - An encrypted (secure, scrambled) channel to create an illusion that a machine is connected directly to a network even if it is not physically close.

        - Means that the machine will have an IP address given to it from the remote network.
    - Companies will often use this for traveling employees to secure their data.
- Wireless Networks (WEP and WPA)
    - Protect your wireless network with a password so that other people within range cannot connect to your network
    - Its also possible for people to sniff packets and collect any data traffic submitted on the wireless network.
    - WEP and WPA encrypt your data, but they are broken. Someone with enough time can crack the encryption.
    - Wireless networks are inherently less secure than wired networks.
- Cryptography
    - Caesar Cipher (ROT-13) – take every letter in your message and shift it over by a certain number of letters. In the case of ROP-13, the shift is 13 characters.
        - Relatively Insecure
    - SSL (via HTTPS, port 443) encodes messages before they are sent over the Internet. The messages are said to be encrypted.
        - Type of encryption: RSA
        - Works with 2^{1024} bit keys (Caesar cipher has only 25 different keys)
        - It would take a long time to find the proper cipher with a 2^{1024} key!

- In many cases, it is much more difficult to break encryption rather than find some other method to harvest data.
  - ATM machines with fake card readers

- Virus Scanners
  - Protects against computer viruses.
  - Requires up-to-date virus definitions in order to protect your computer against new threats
  - Also protects against worms
    - Worms can propagate so quickly they can infect entire networks of machines in 15 minutes.
  - Thousands of viruses and worms exist.
  - A virus or worm can theoretically
    - format your hard drive
    - erase data
    - literally break your computer by exploiting overclocking, causing a machine to overheat
  - "script kiddies" download wizards that allow easy creation of viruses
- Software Piracy Protection
  - Product activation or CD Keys protect software from being pirated
    - "Cracked" software breaks this protection
  - Windows Updates
    - Don't require verification of legality of the software

        - Probably because thousands or millions of defenseless machines on the Internet could become a threat
    - Windows Activation
        - Transmits information about your computer to Microsoft
        - Microsoft associates this information with the CD Key to prevent installation on other machines
- Problem Set 6
    - A fun but (possibly) challenging pset hoping to get you to think like the bad guy ☺
    - To get you to think how your network or machine can be compromised