Week 3 Lecture Notes

Tuesday:

* Network Security
  + Field of network security
    - How bad guys can attack computer networks
    - How we can defend networks against attacks
    - How to design architectures that are immune to attacks
  + What is network security
    - Consistos of policie need to finish this note
* Network security objectives
  + Confidentiality: only sender, intended receiver should understand message contents
    - Sender encrypted message
    - Receiver decrypts message
  + Message integrity:
    - Sender, reiver want to ensure message not altered without detection
  + Authentication: sender receiver want to confirm identity of each other
  + Access and availability: services must be accessible and available to users
* Model for Network Security
  + Friends and Enemy Example
    - 3 people: Alice, Bob, Trudy
    - Bob and Alice are friends meaning to send a message
    - Trudy is a hacker with the intent to intercept this message
* Malware
  + Malware can get in host from a virus
    - Self replicating infection by receiving/ executing object
  + Spyware Malware
    - Can record keystrokes, websites visited
    - Upload info to collection site
  + Consequences
    - Infected host can be enrolled in botnet
      * Used for spam or distributed denial of service (DDoS Attacks)
* Denial of sercice attacks
  + Attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic
    - 1. Select target
    - 2. Break into hosts around the network
    - 3. Send packets to target
* Packet Interception
  + “Packet sniffing”
    - Broadcast media ( shared ethernet, wireless )
    - Promiscuous network interface reads/records all packets (including passwords) passing by
* Impersonation
  + Impersonator: can fake (spoof) source address in packet (or any field)
* Going back to the protocol stack