Introduction to Security

Computer Networks
Term B10

Intro to Security Outline

- Network Security
- Malware
  - Spyware, viruses, worms and trojan horses, botnets
- Denial of Service and Distributed DOS Attacks
- Packet Sniffing
- Masquerading Attacks
- Man-in-the-Middle Attacks

Networks under Attack

- The "original" Internet (i,e., ARPANET) was not designed with security in mind.
  - The early vision was "a group of mutually trusting users attached to a transparent network".
    - ARPANET started out as academics and DoD users!!
  - Protocol and application designers are playing "catch-up".
- The Internet changed:
  - Added industrial management partners → ISP's
  - WWW made the Internet accessible to the masses.
- Bad guys can attack networks and attempt to wreak havoc on our daily lives.

Network Security

- **Network security** is about:
  - How bad guys can attack computer networks.
  - How we can defend networks against attacks.
  - How to design architectures that are immune to attacks.
- **Network security** is becoming more important as more individuals become dependent on the Internet and as the destructive nature of new attacks increases.
- Security issues exist at all layers!

Malware

- **Malware::** malicious "stuff" that enters our hosts from the Internet and infects our devices.
- **Spyware** collects private information (e.g., keystrokes and web sites visited) and uploads info to bad guy collection sites.
- An infected host can be enrolled in a **botnet**, used for spam and distributed denial-of-service (DDoS) attacks.
- Malware is often **self-replicating**: from an infected host, it seeks entry into other hosts.

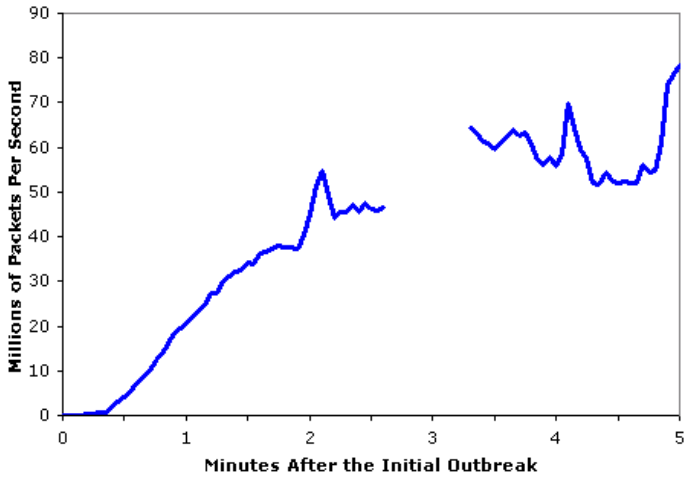
Malware from the Internet

- Malware can get into a host and spread in the form of a virus, worm, or trojan horse.
- Virus
  - Requires some form of user active execution.
  - Classic example: an email attachment containing malicious executable code that is triggered when the attachment is opened.
  - Self-replicating (e.g., via address book)

Worms and Trojan Horses

- **Worm**
  - Infects by passively receiving object via a vulnerable network application that runs the malware to create worm.
  - Self-replicates by searching for hosts running the same application.

Sapphire Worm: aggregate scans/sec
in first 5 minutes of outbreak (CAIDA, UWisc data)

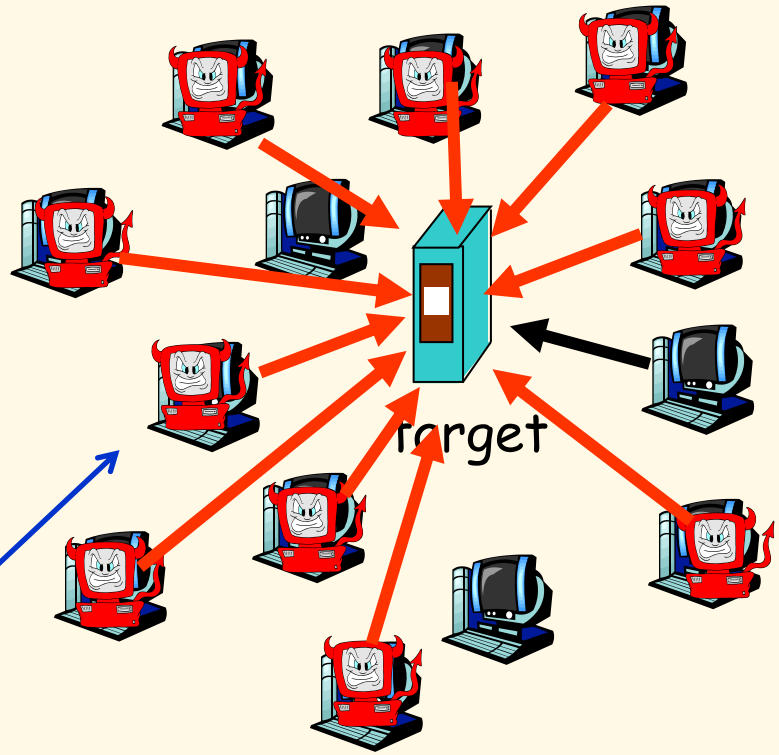


- **Trojan horse**
  - Hidden in some otherwise useful software.
  - Often found today on a Web page (Active-X, plugin).

Denial-of-Service Attack

- Denial-of-service (DoS) renders resources (server, link) unusable by legitimate users by overwhelming the resource with bogus traffic.

1. select target
2. break into hosts around the network (see botnet)
3. send packets toward target from compromised hosts



Distributed DoS (DDoS)

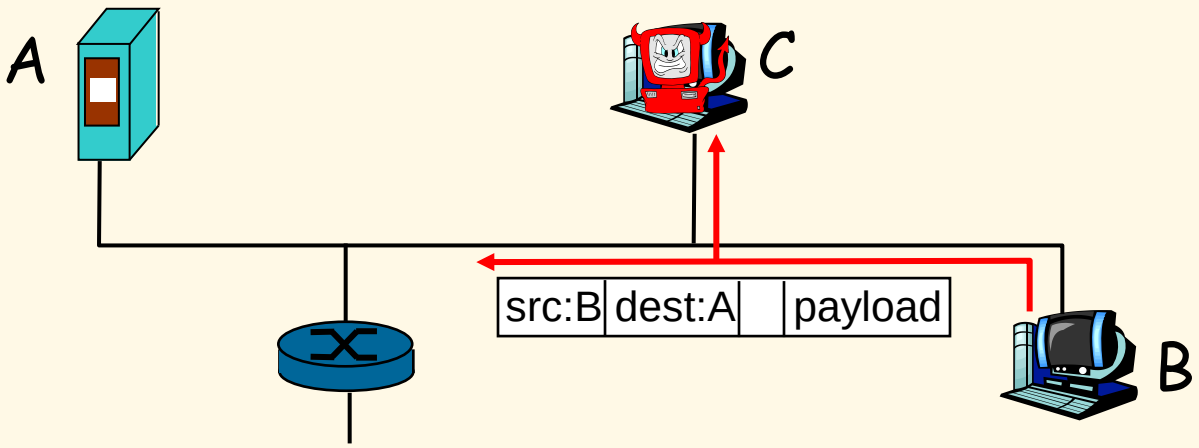
Denial-of-Service Attack

- Three categories:
  - Vulnerability attack:: attack application with well-crafted messages (result – service stops or host crashes).
  - Bandwidth flooding:: deluge victim with so many messages such that target's access link gets clogged.
  - Connection flooding:: initiate so many half-open or open TCP connections that target stops accepting legitimate connections.

Bad Guy Packet Sniffing

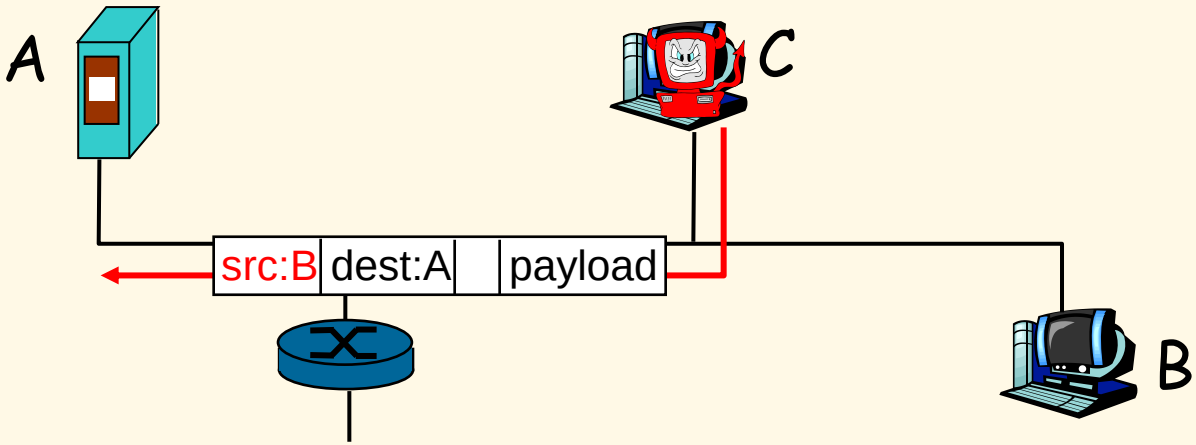
Packet sniffing:: passive receiver that records a copy of every packet that goes by (e.g., Wireshark)

- broadcast media (shared Ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



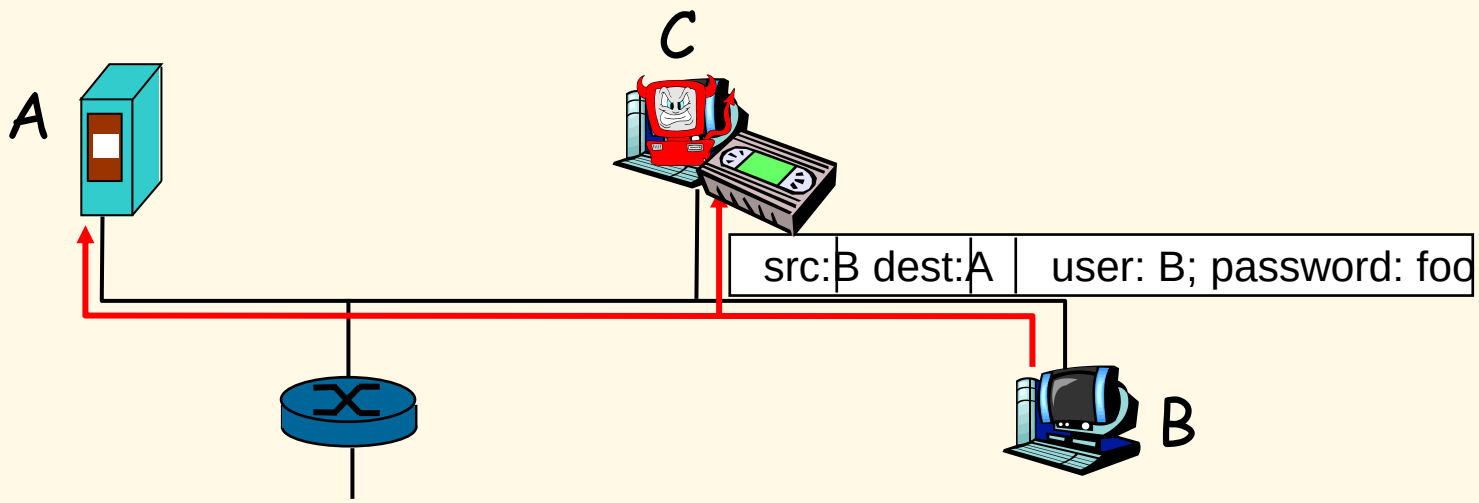
Masquerade Attack

- **IP spoofing::** send a packet with false source address



Man-in-the-Middle Attack

- **record-and-playback::** sniff sensitive info (e.g., password), and use later
  - Bad guy password holder *is* that user from system point of view



Intro to Security Summary

- Network Security
- Malware
  - Spyware, viruses, worms and trojan horses, botnets
- DoS and DDOS Attacks
- Packet Sniffing (promiscuous mode)
- Masquerading Attacks (IP spoofing)
- Man-in-the-Middle Attacks
  - Record and playback