CS 372 Lecture #7

Overview of Networking:

- **introduction to network security**

Note: Many of the lecture slides are based on presentations that accompany *Computer Networking: A Top Down Approach,* 6th edition, by Jim Kurose & Keith Ross, Addison-Wesley, 2013.

Network Security

- The field of network security is about:
  - how computer networks can be attacked intentionally
  - how computer networks can be "attacked" unintentionally
  - how we can defend networks against attacks
  - how to design architectures that are immune to attacks
- The Internet was not originally designed with security in mind
  - *original vision:* "a group of mutually trusting users attached to a transparent network"
  - Internet protocol designers playing "catch-up"
  - Security considerations in all layers

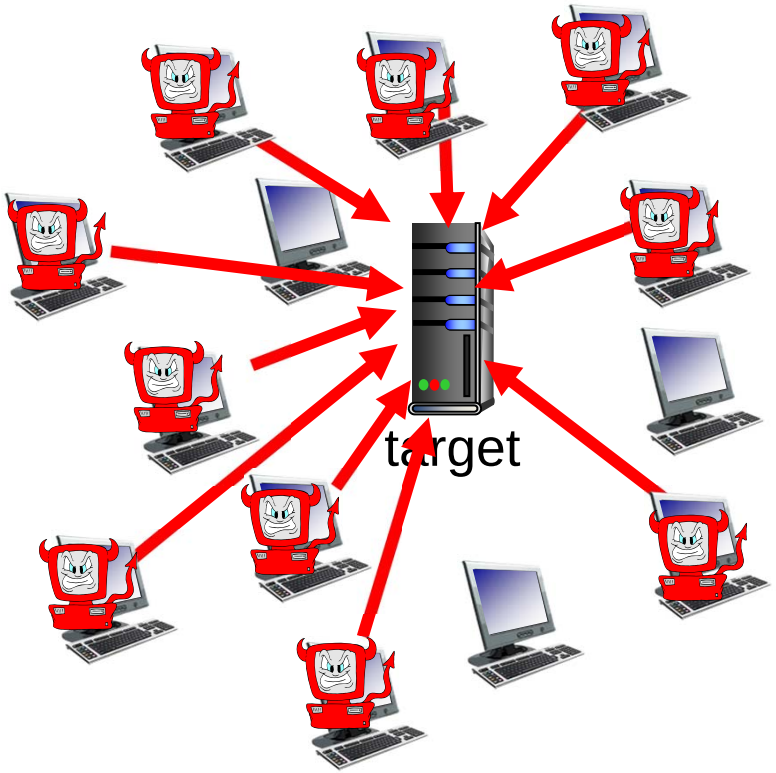
Attackers can put malware into hosts via Internet

- malware can get into a host from:
  - *virus:* self-replicating infection by receiving/executing object (e.g., e-mail attachment), usually corrupt files on a host
  - *worm:* self-replicating infection that executes itself as it travels around a network
- spyware malware can record keystrokes, web sites visited, upload info to collection site
- infected host can be enrolled in botnet
  - used for spam, Distributed Denial of Service (DDoS) attacks

Attackers can attack server, network infrastructure

Denial of Service (DoS): attackers make resources (server, bandwidth) unavailable to legitimate traffic by overwhelming resource with bogus traffic

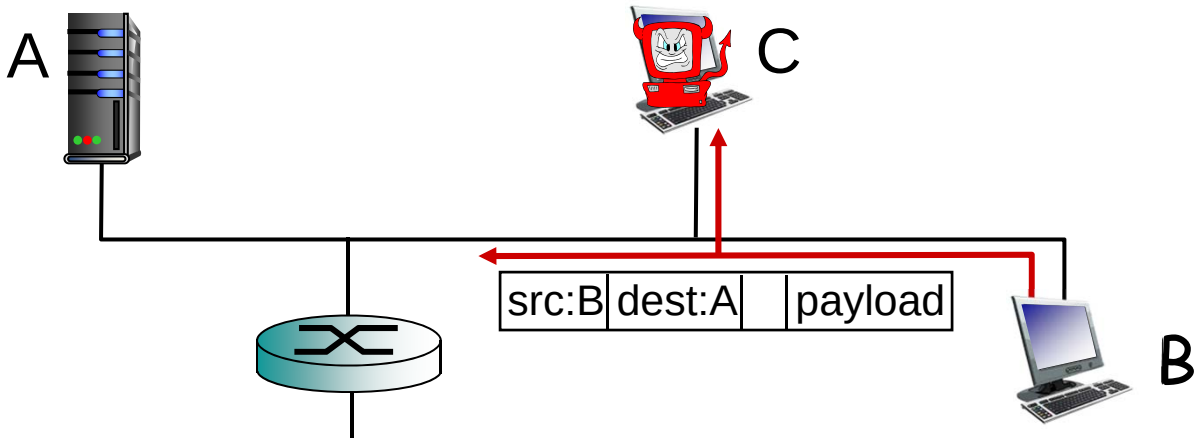
1. select target
2. break into hosts around the network (see botnet)
3. send packets to target from compromised hosts



Attackers can sniff packets

packet "sniffing":

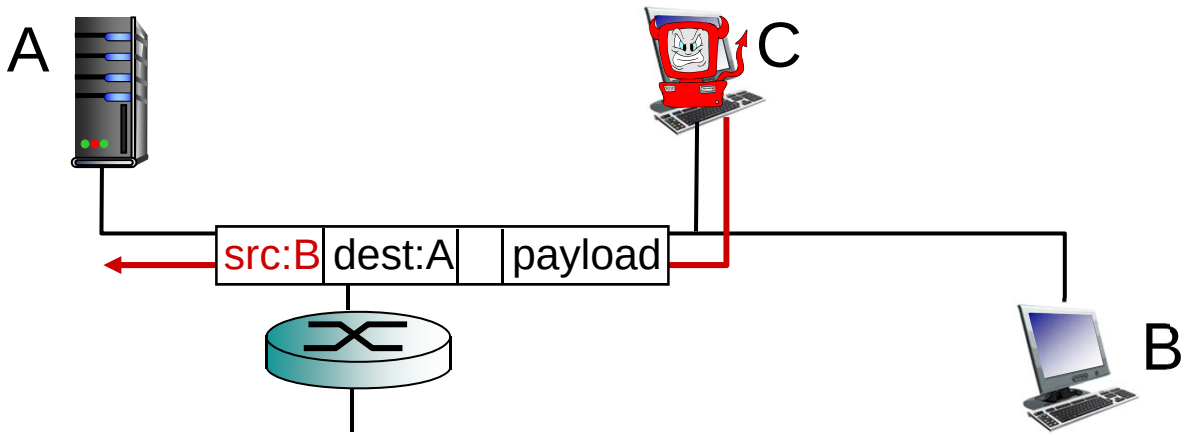
- broadcast media (shared ethernet, wireless)
- promiscuous network interface reads/records all packets (e.g., including passwords!) passing by



- wireshark software used for end-of-chapter labs is a (free) packet-sniffer

Attackers can use fake addresses

IP spoofing: send packet with false source address



… lots more on security (throughout, Chapter 8)

Summary Lecture #7

- Types of security threats
  - malware, spyware
  - denial of service
  - packet sniffing
  - address spoofing