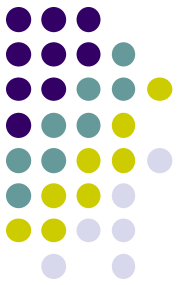# ELEN 4017

Network Fundamentals

Lecture 6 & 7
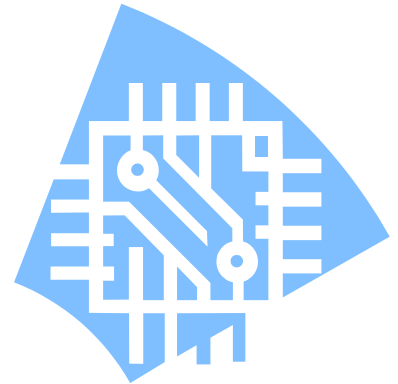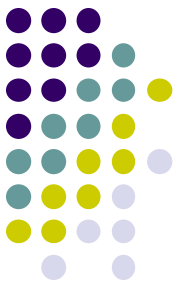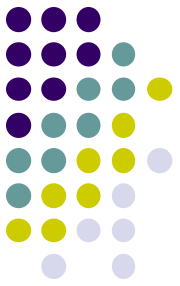
Purpose of lecture

- Continuation of roadmap for course
- Kurose chapter 1

Outline

- Networks under attack
- History of networking and the Internet

Network Security

- The field of 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
- Internet not originally designed with (much) 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!

Bad guys can put malware into hosts via Internet
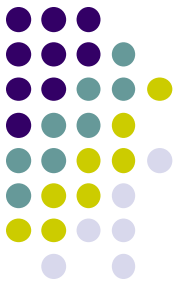
- Malware can get in host from a virus, worm, or trojan horse.

- Spyware malware can record keystrokes, web sites visited, upload info to collection site.

- Infected host can be enrolled in a botnet, used for spam and DDoS attacks.

- Malware is often self-replicating: from an infected host, seeks entry into other hosts

Bad guys can put malware into hosts via Internet

- Trojan horse
    - Hidden part of some otherwise useful software
    - Today often on a Web page (Active-X, plugin)
- Virus
    - infection by receiving object (e.g., e-mail attachment), actively executing
    - self-replicating: propagate itself to other hosts, users

- Worm:
    - infection by **passively** receiving object that gets itself executed
    - self- replicating: propagates to other hosts, users

Sapphire Worm: aggregate scans/sec
in first 5 minutes of outbreak (CAIDA, UWisc data)
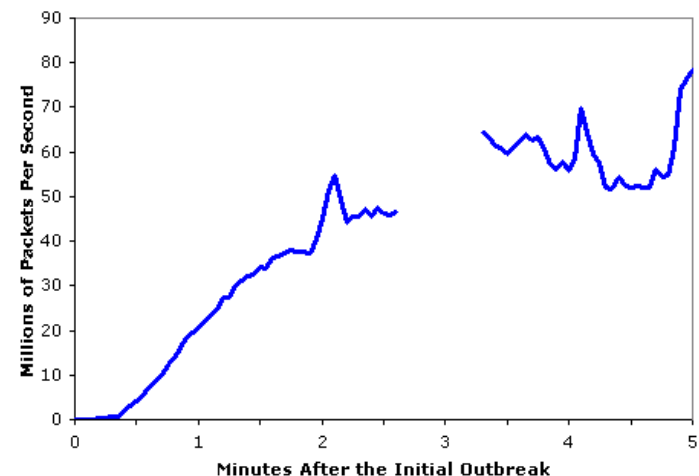
Bad guys can attack servers and network infrastructure

- 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 toward target from compromised hosts

target
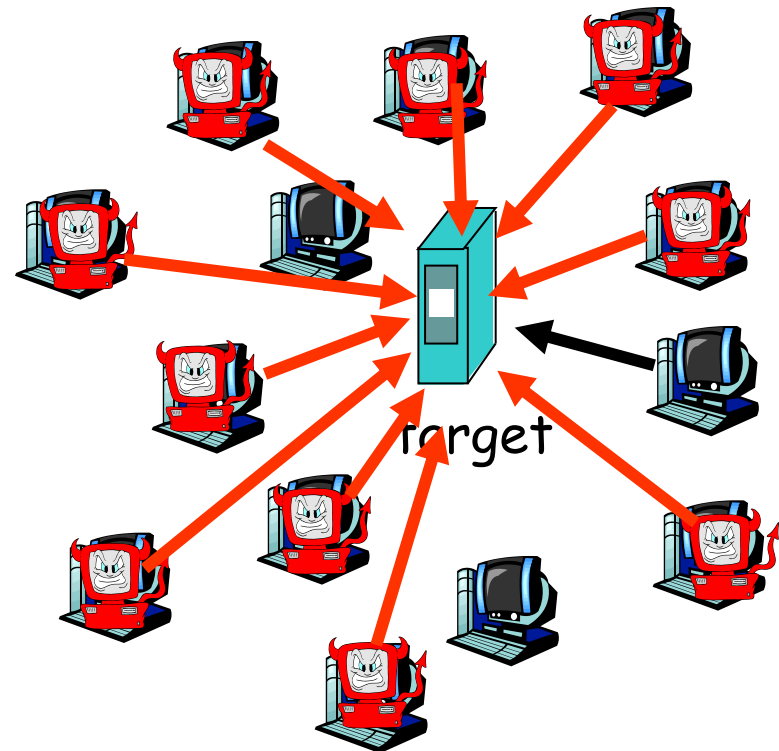
Bad guys can attack servers and network infrastructure
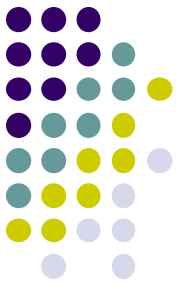
- Vulnerability attack
  - Exploit a vulnerability in a specific OS or application.
    - Dropping a SQL database.
  - Connection flooding
    - Establish a large number of open TCP connections.
    - Server runs out of resources.
  - Bandwidth flooding
    - Deluge of packets, overwhelm the access link. Prevents legitimate packets from reaching the server.

The bad guys can sniff packets

Packet sniffing:

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

A

C

src:B | dest:A | payload

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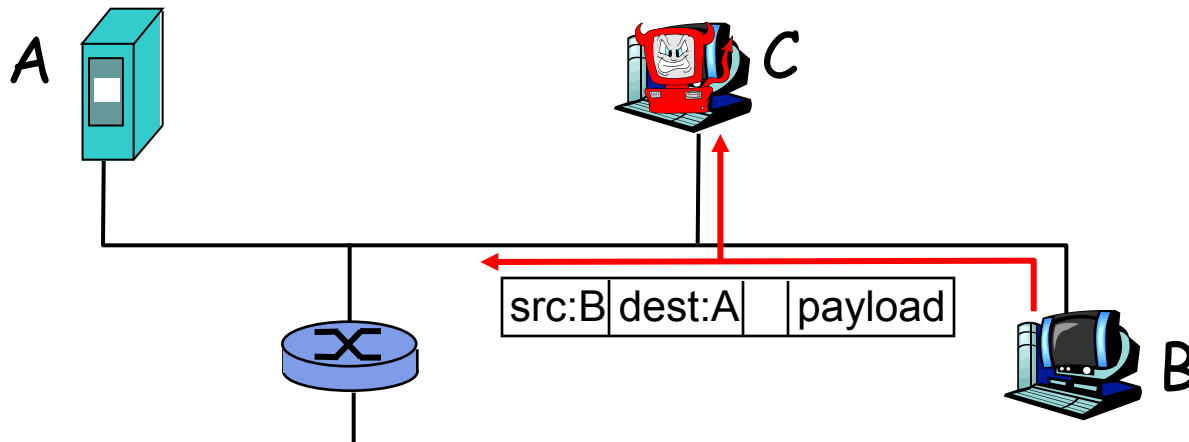
- Wireshark software used for end-of-chapter labs is a (free) packet-sniffer

The bad guys can use false source addresses
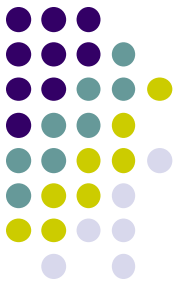
- *IP spoofing:* send packet with false source address
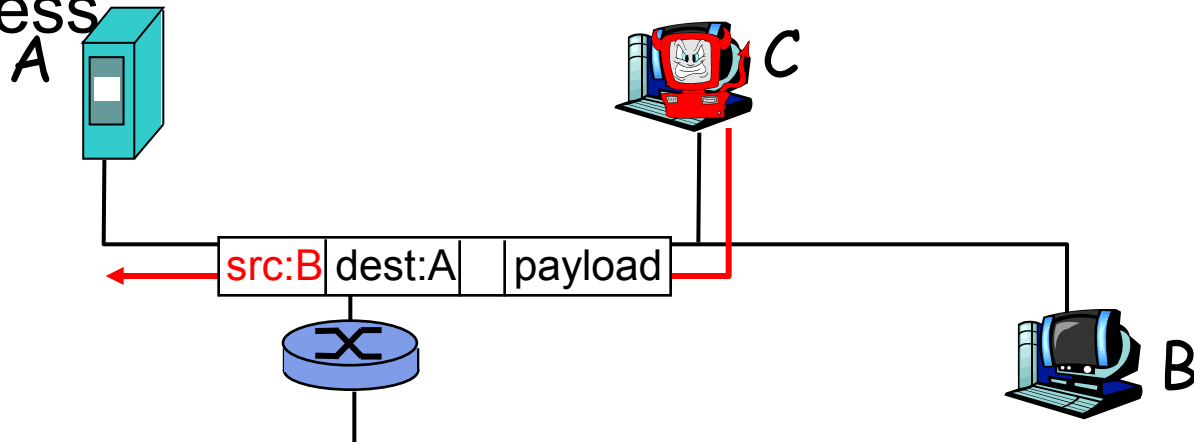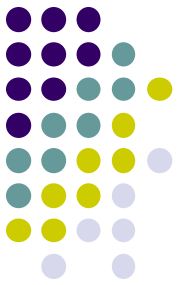
The bad guys can record and playback
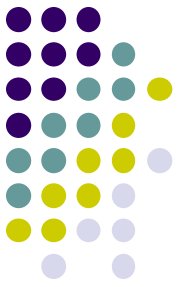
- *record-and-playback*: sniff sensitive info (e.g., password), and use later
  - password holder *is* that user from system point of view
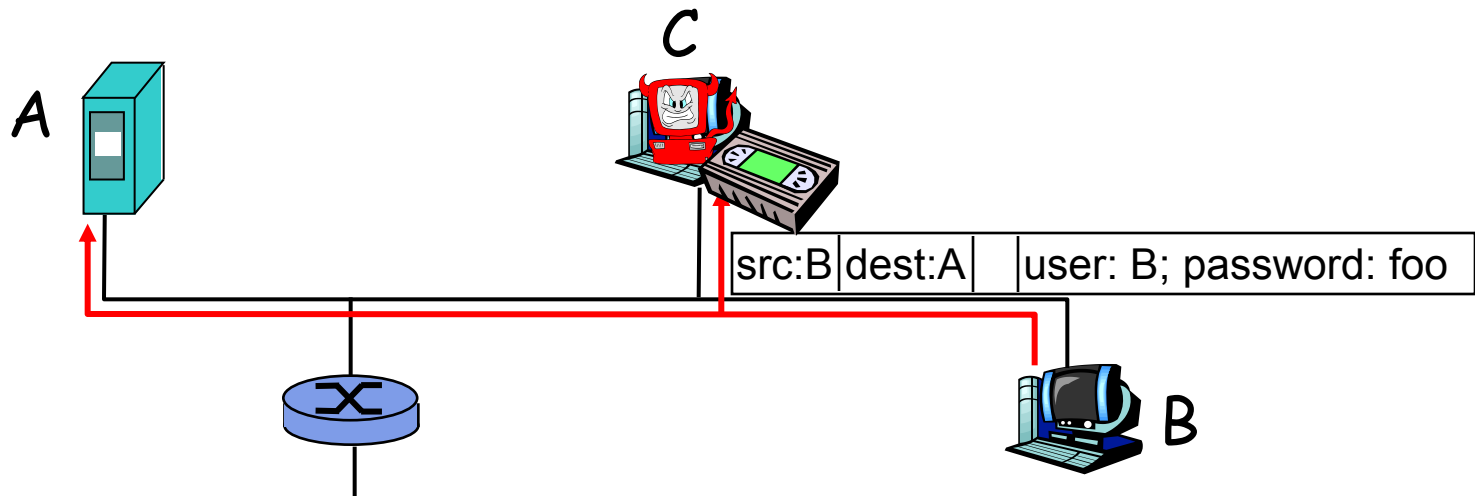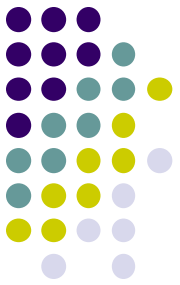
Internet History

Cerf and Kahn's internetworking principles:

- minimalism, autonomy - no internal changes required to interconnect networks
- best effort service model
- stateless routers
- decentralized control

define today's Internet architecture

Purpose of lecture

- Future of the Internet
- Application Layer
  - Application trends

Application trends

- Applications are the reason that communications exist.

- Majority of software development is targeted at application layer.

- Trends:
  - 1980's – text email, remote access, file transfers
  - 1990's – World Wide Web (surfing, searching, E-commerce)
  - 2000's – P2P file sharing, social networking, video and multimedia, Internet telephony

Text based email
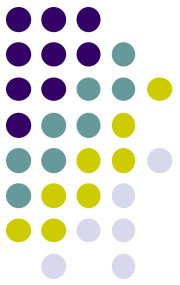
Remote access
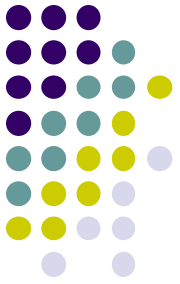
- Screencast
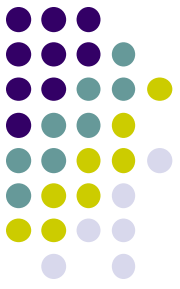
1990s – Birth of web

- Web browsing (surfing)
- HTTP/HTML defined the semantics of how web pages could be referenced and linked to other pages.
- Initial versions were geared towards basic static content.
- Retro fitted name – Web 1.0
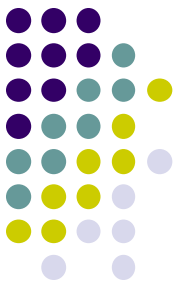
XML Schema

XML Schemas express shared vocabularies and allow machines to carry out rules made by people. They provide a means for defining the structure, detail. XML Schema was approved as a W3C Recommendation on 2 May 2001 and a second edition incorporating many errata was published on 2

The XML Schema Working Group, part of the XML Activity, is responsible for the W3C's work on this topic -- for details see the Working Group's cha XML Schema Interest Group, a forum for the discussion of technical issues relating to the development of XML Schema. It also has a charter.

See also: Robin Cover's index of XML Schema materials.

**XML Schema 1.1
Status**

Ref: http://www.w3.org/XML/Schema

Search

News / Blogs

E-Commerce (music, travel)

Public authoring

- Change in publishing model.
- Collaborative knowledge sharing
- Wikipedia
- Twitter

Webmail / IRC

- Free internet email is hugely successful.
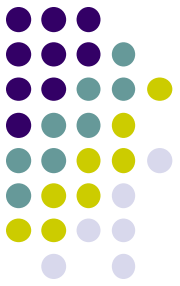- Resurgence in Internet Relay Chat (relying on presence information of contacts)

2000s

- Burst of dotcom bubble
- Innovative applications entering space.

Social networking

Extensibility / Personalization
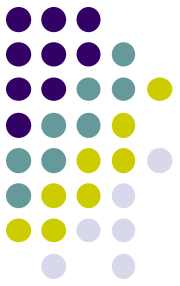
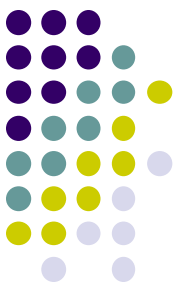# **Multimedia**

- YouTube
- Hulu

File sharing / VoIP/ P2P
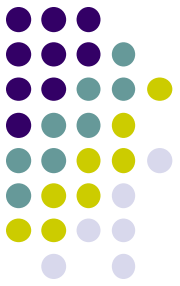
- Napster
- BitTorrent
- Skype

Web 2.0

- What is it ?

- What other applications ?

Future of the Internet

http://www.ted.com/talks/tim_berners_lee_on_the_next_web.html

Watch this to learn about how the web is evolving