Week 9 - Wednesday

COMP 4290

Last time

- Mandatory access control
  - Bell-La Padula
  - Chinese Wall
  - Biba
- Rootkits

Questions?

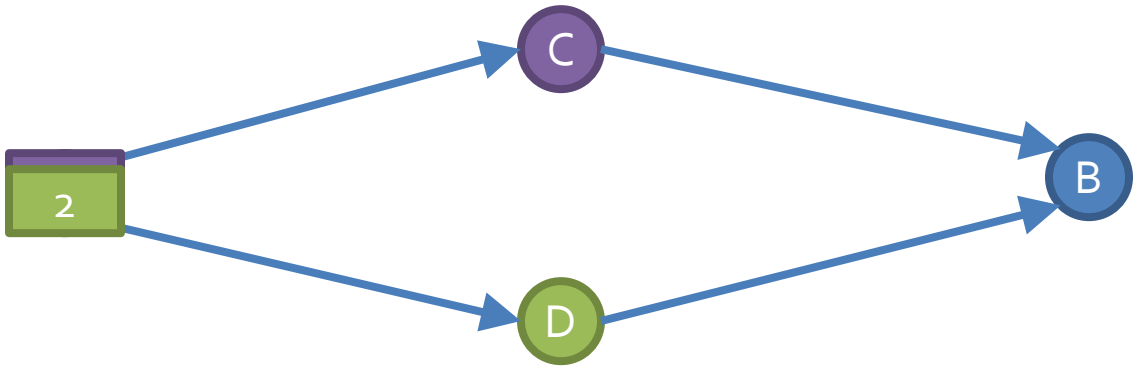
Project 2

Austin Rheyne Presents

Network Basics

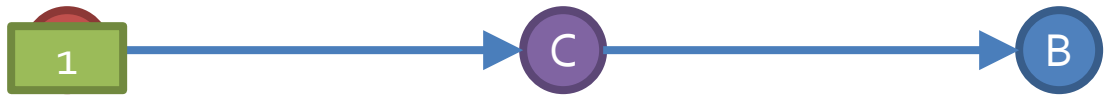
Packet switched

- The Internet is a packet switched system
- This means that individual pieces of data (called packets) are sent on the network
  - Each packet knows where it is going
  - A collection of packets going from point A to point B might not all travel the same route



Circuit switched

- Phone lines are circuit switched
- This means that a specific circuit is set up for a specific communication
- Operators used to do this by hand
- Now it is done automatically
- Only one path for data



Circuit vs. packet switching

- Which one is faster?
  - Circuit switching
- Which one is more predictable?
  - Circuit switching
- So, why is the Internet packet switched?
  - More adaptable

ARPA

- The Advanced Research Projects Agency was created in 1958 to respond to the Russians launching Sputnik
- The ARPANET connected its first two major nodes over 10 years later
- Packet switched was used so that the network could still communicate after a nuclear strike

Network strength

- If a single cut can case a network to go down, that network is vulnerable to a **single point of failure**
- Most important networks like electrical systems have redundancy so that this doesn't happen to a whole city
  - **Resilience** or fault **tolerance**

Terminology

- A **computer network** is at least two computers connected together
  - Often one is a **server** and the other is a **client**
- A computer system in a network is called a **node**
- The processor in a node is called a **host**
- A connection between two hosts is a **link**

Network characteristics

- **Anonymity**: We don't know who we're dealing with
- **Automation**: Communication may be entirely between machines without human supervision
- **Distance**: Communications are not significantly impacted by distance
- **Opaqueness**: It is hard to tell how far away other users are and to be sure that someone claiming to be the same user as before is

Shape and size

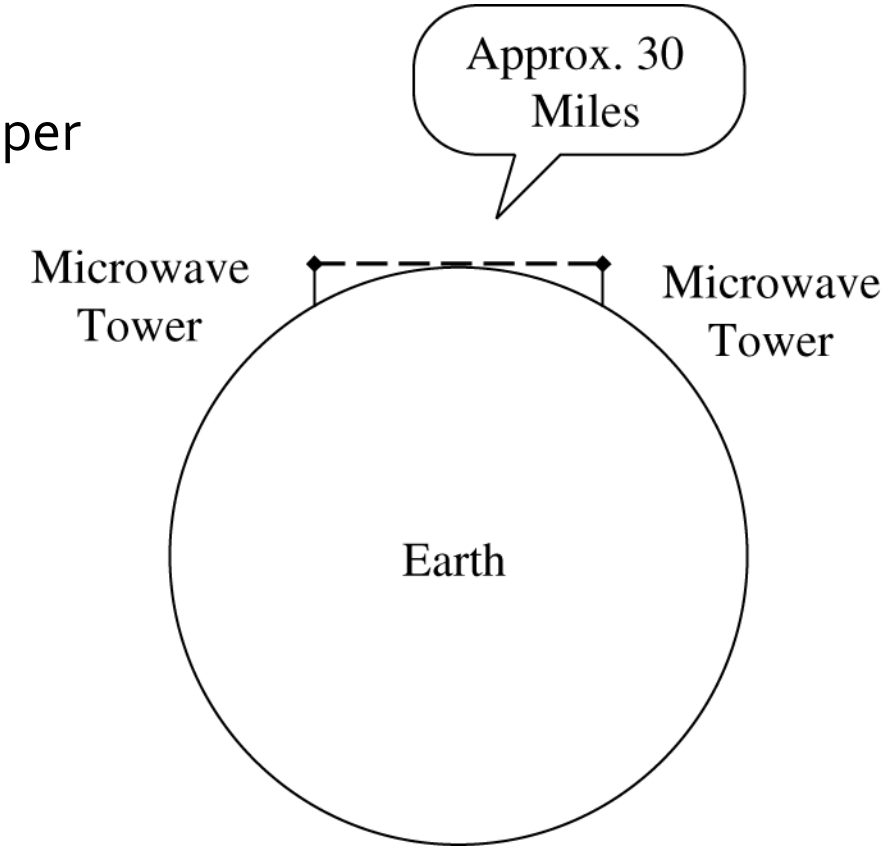
- The arrangement of a network, in terms of its links, is called its **topology**
- The boundary separates systems that are on a network from those that are not
  - With the Internet, this line is blurry
- It is hard to know who owns hosts in a network
  - Makes enforcing the law difficult
- How is a network controlled? Who does it?

Communication

- **Analog** or **digital**
  - A **modem** converts between the two
  - Portmanteau of "modulator-demodulator"
- Copper wire is the main workhorse
  - **Twisted pair** is a pair of insulated copper wires
    - Limit of about 10 Mbps and about 300 feet without a boost
  - **Coaxial cable** has a single wire surrounded by an insulation jacket covered by a grounded braid of wire
    - **Repeaters** or **amplifiers** are needed periodically to prevent signal degradation

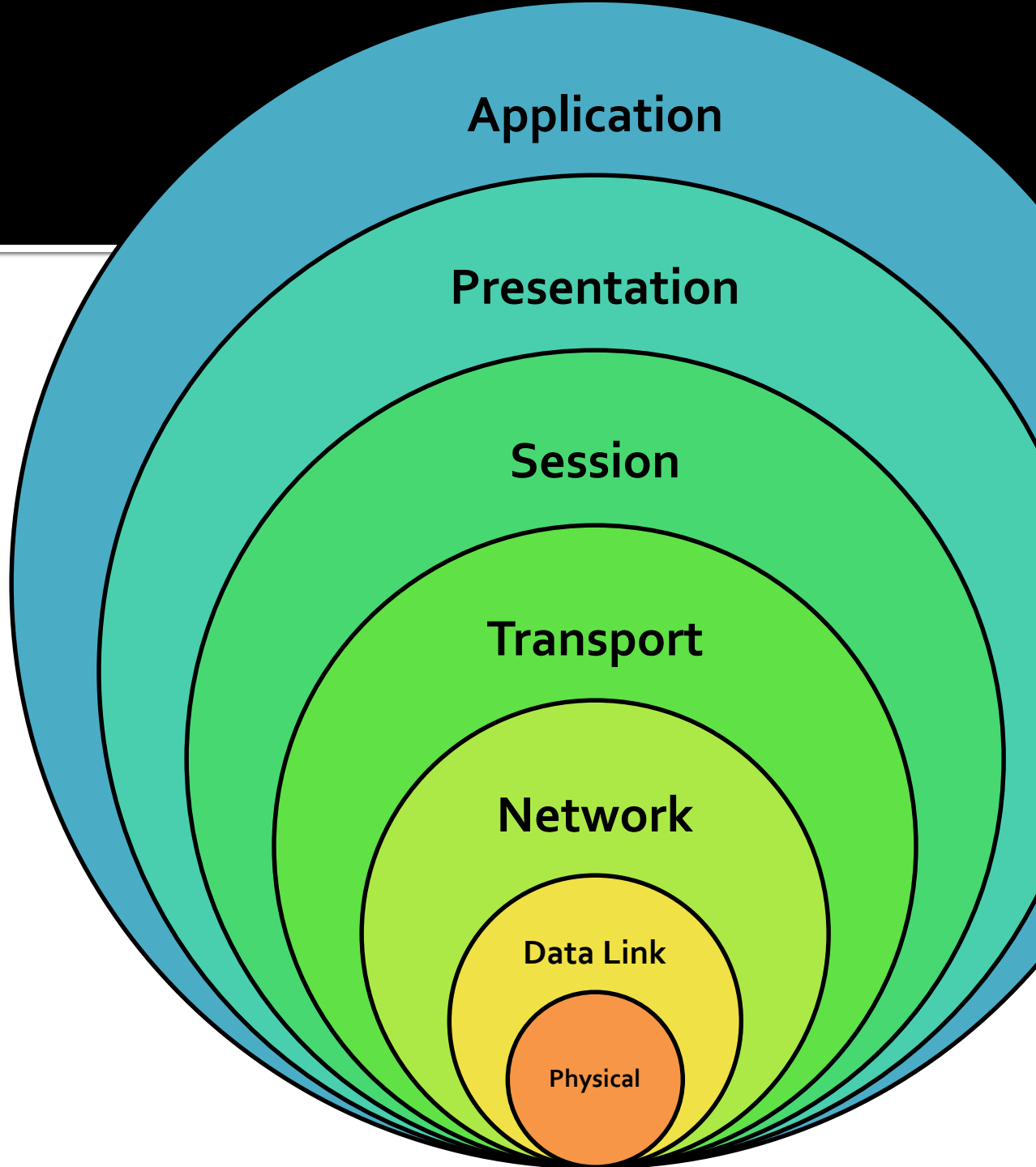
Other media

- Optical fiber
  - Carries light instead of electricity
  - Higher bandwidth and less signal degradation than copper
  - Replacing aging copper lines
- Wireless
  - Good for short distance
  - Uses radio signals
- Microwave
  - Strong signals
  - Requires line of sight
- Infrared
  - Similar to microwave but weaker signals
- Satellites
  - Need **geosynchronous** orbits
  - Secure applications need smaller **footprints** than broadcasts



Protocols

- There are many different communication protocols
- The OSI reference model is an idealized model of how different parts of communication can be abstracted into 7 layers
- Imagine that each layer is talking to another parallel layer called a **peer** on another computer
- Only the physical layer is a real connection between the two



Layers

- Protocols and standards define each layer
- Not every layer is always used
- Sometimes user errors are referred to as Layer 8 problems

Layer	Name	Activity	Example
7	**Application**	User-level data	HTTP
6	**Presentation**	Data appearance, some encryption	TLS
5	**Session**	Sessions, sequencing, recovery	IPC and part of TCP
4	**Transport**	Flow control, end-to-end error detection	TCP
3	**Network**	Routing, blocking into packets	IP
2	**Data Link**	Data delivery, packets into frames, transmission error recovery	Ethernet
1	**Physical**	Physical communication, bit transmission	Electrons in copper

TCP/IP

- The OSI model is conceptual
- Most network communication uses TCP/IP
- We can view TCP/IP as four layers:

Layer	Action	Responsibilities	Protocol
Application	Prepare messages	User interaction	HTTP, FTP, etc.
Transport	Convert messages to packets	Sequencing, reliability, error correction	TCP or UDP
Internet	Convert packets to datagrams	Flow control, routing	IP
Physical	Transmit datagrams as bits	Data communication	

TCP/IP

- **Transmission Control Protocol (TCP)**
  - Creates a reliable communication session
  - Wraps information into packets
  - Uses **port** numbers to connect processes to information streams
- **User Datagram Protocol (UDP)**
  - Alternative to TCP that is unreliable but has low overhead

- **Internet Protocol (IP)**
  - Allows for unreliable transport
  - Wraps packets into datagrams
  - Uses IP addresses for routing

Addressing

- A message datagram is sent to a **domain name** such as **`google.com`**
- The **Domain Name System (DNS)** converts **`google.com`** into an IP address such as **`74.125.226.229`**
- The server at **`74.125.226.229`** receives the datagram and unwraps the corresponding packet
- The packet has a port number (probably port **`443`**, for HTTPS), which is delivered to whatever program is communicating on port **`443`**

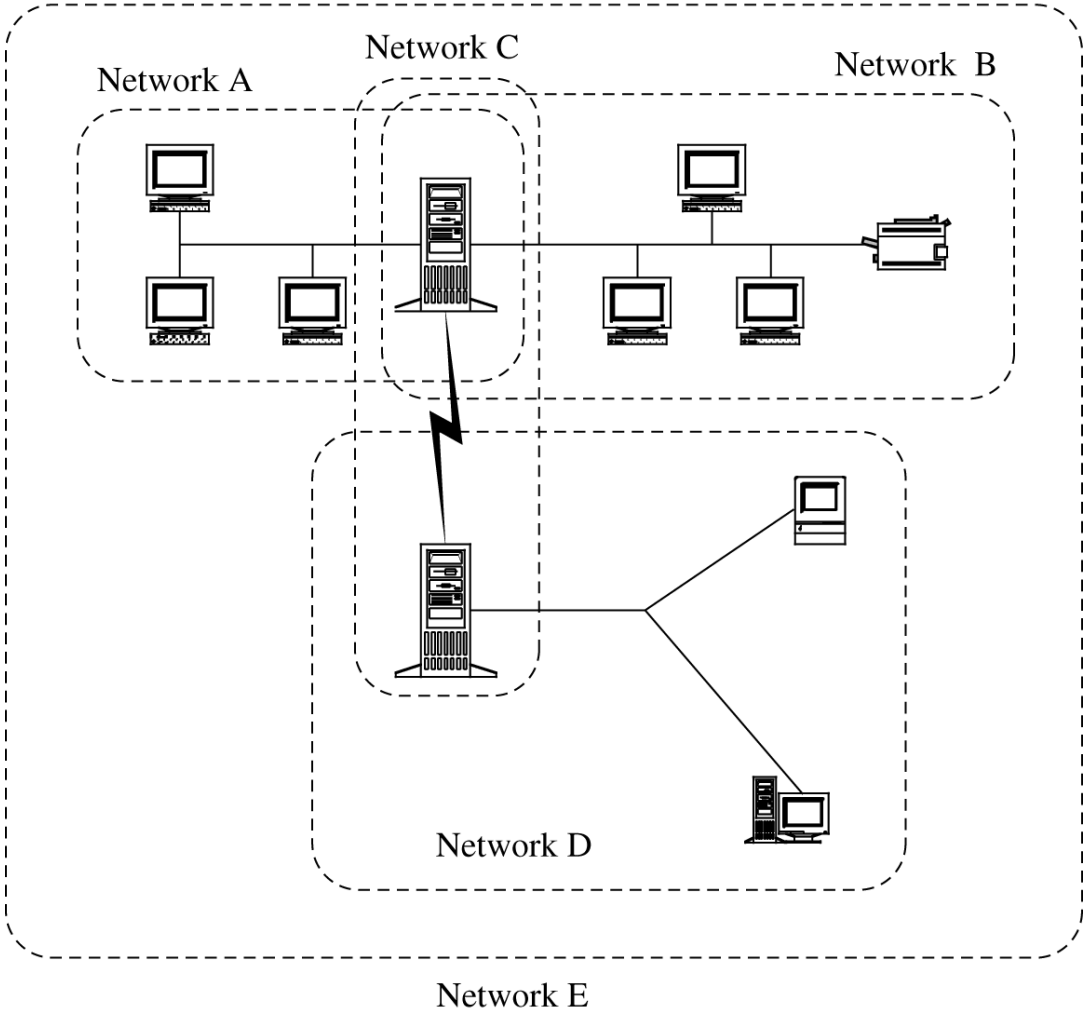
Types of Networks

- Local area network (LAN)
  - Small: Often not more than 100 users within 2 miles
  - Local controlled
  - Physically protected
  - Limited scope
- Wide area network (WAN)
  - One organization controls it
  - Covers a large distance
  - Physically exposed
- Internetworks
  - A connection of two or more separate networks
  - The most significant is the Internet
  - Enormous
  - Heterogeneous
  - Physically and logically exposed

Network Threats

Why is a network vulnerable?

- Anonymity
- Many points of attack (targets and origins)
- Sharing
- Complexity
- Unknown perimeter

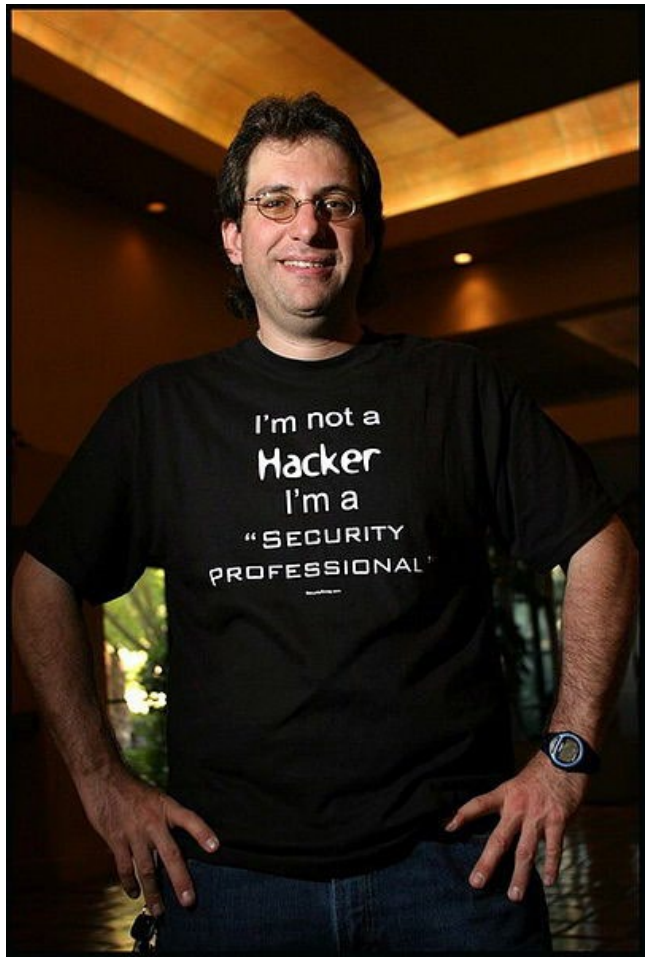


Why do people attack networks?

- Challenge
- Fame
- Money
  - State espionage
  - Industrial espionage
- Organized crime
  - Stolen credit card numbers
  - Identity theft
- Ideology
  - **Hacktivist** groups like Anonymous
  - **Cyberterrorism**
    - Used to be from groups like al Qaeda
    - Now more commonly from quasi-government-affiliated groups like Pakistani Cyber Army or Syrian Electronic Army

Kevin Mitnick

Once the most wanted computer criminal in the US



Mid-Semester Evaluation

Upcoming

Next time…

- Network security controls
- Firewalls
- Intrusion detection
- Network management
- Austin Rheyne presents

Reminders

- Read Sections 6.6 through 6.9
- Keep working on Project 2
  - Due this Friday