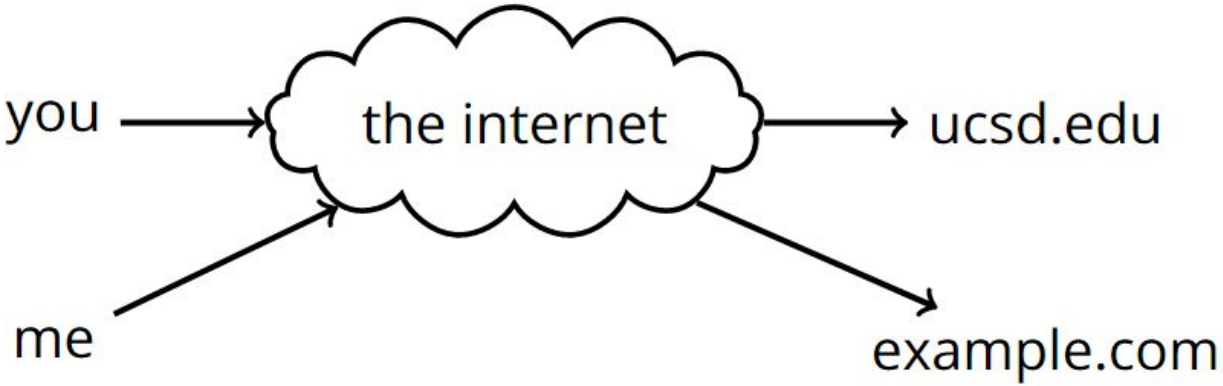
CSE 127 Discussion
Week 8 - Network Attacks

Agenda

1) Network Recap
2) PA4: Network Attacks
3) Tools for PA4

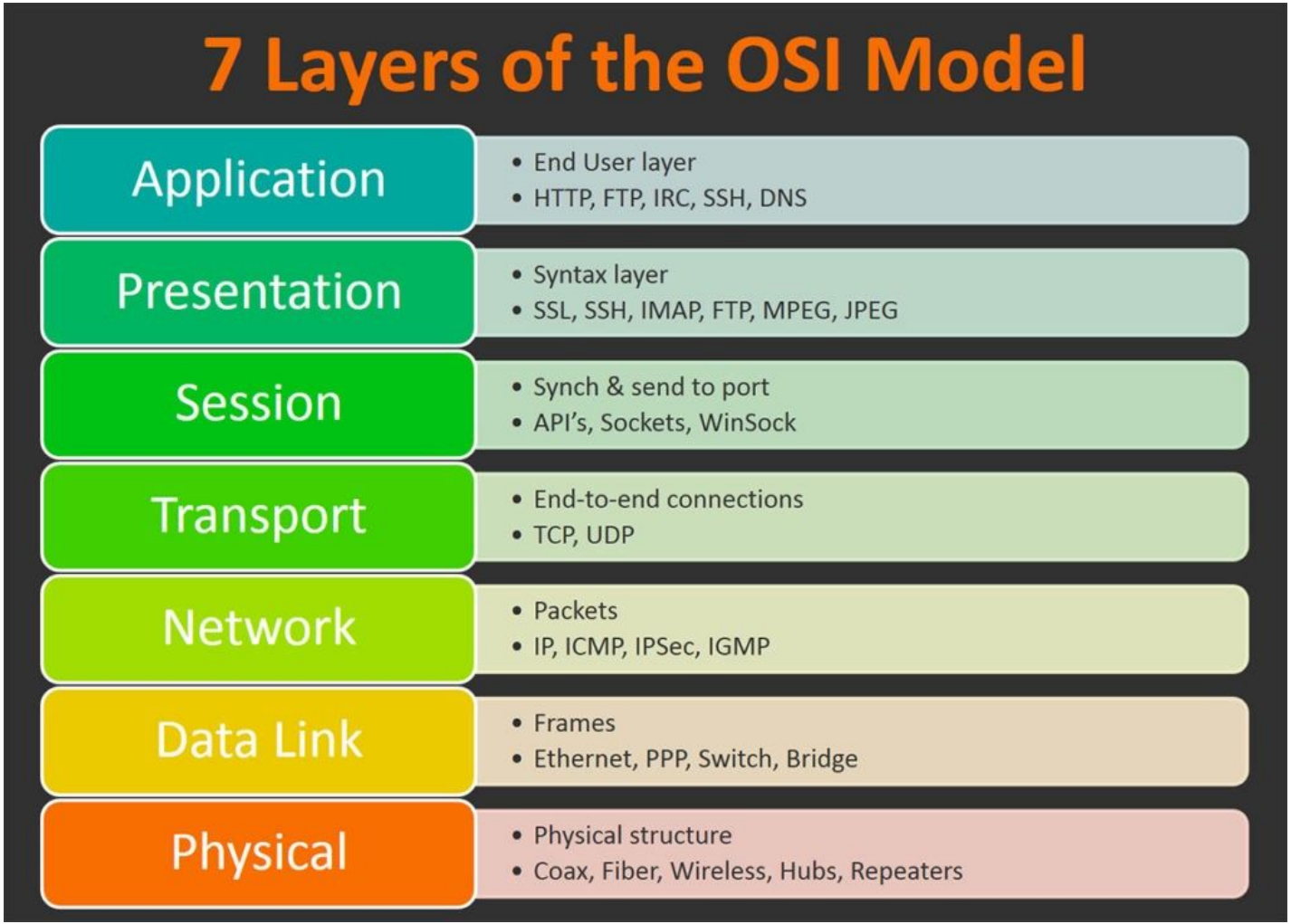
Networking Recap



Original Idea:

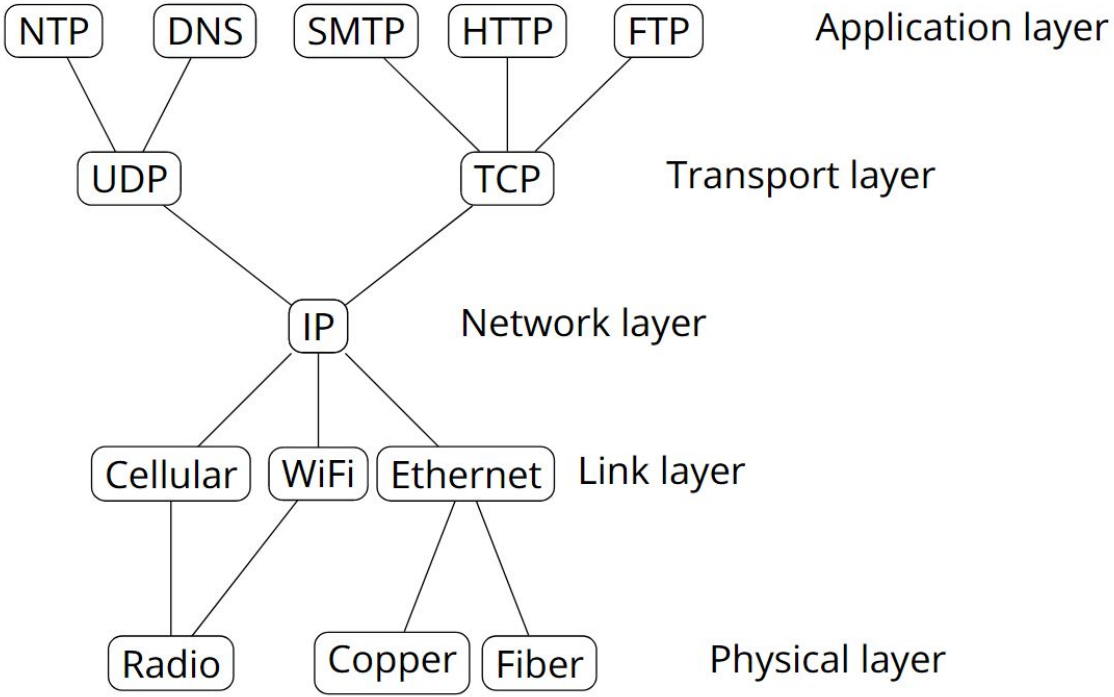
- Network is dumb
- Simple, robust service
- Shift complexity to endpoints
- Acts like postal system (packet-based) rather than traditional phone system (circuit-based)

7 Layers of the OSI Model



Basic Internet Archictecture “Hourglass”

Narrow waist = interoperability



Using the Internet: A Worked Example

You connect your laptop a cafe WiFi network and type ucsd.edu into your browser's URL bar. What happens?

Using the Internet: A Worked Example (1)

1. Your laptop uses DHCP (Dynamic Host Configuration Protocol) to bootstrap itself on the local network via WiFi over radio waves
   - New host has no IP address, doesn't know who to ask
   - Broadcasts DHCPDISCOVER to 255.255.255.255 with its MAC address
   - DHCP server responds with config:lease on host IP address, gateway IP address, DNS server information

Using the Internet: A Worked Example (2)

2. Your laptop makes an ARP request to learn the MAC address of the local router
    - Every connection outside the local network will be encapsulated in a link-layer frame with the local router's MAC address as the destination
    - Your laptop encapsulates each IP packet in a WiFi frame addressed to the local router
    - The router removes the WiFi frame and adds an Ethernet frame to forward them on its fiber connection to its upstream ISP, or to another part of the network
    - Each hop re-encodes the link-layer for its own network

Using the Internet: A Worked Example (3)

3. Your laptop does a DNS lookup on ucsd.edu
    - It learned the IP address of a DNS server from the router or had one already hard coded in (8.8.8.8)
    - The DNS request is tunneled through UDP packets which are themselves inside IP packets
    - The DNS server responds with either “ucsd.edu has IP address x.x.x.x” or “I don’t know, but the nameserver at y.y.y.y might”
        - Follows a hierarchy upward: your ISP, then the .edu nameserver, then UCSD’s nameserver.
        - Eventually, get final IP address 75.2.44.127

Using the Internet: A Worked Example (4)

4. Your laptop opens a TCP connection to IP address 75.2.44.127
    - Unlike UDP, has reliability
    - TCP is wrapped in IP which is wrapped in Ethernet
    - Each stop in the network checks its routing table against the destination IP address
    - e.g. sbcglobal.net-> att.net-> leve3.net -> cenic.net-> ucsd.edu

Using the Internet: A Worked Example (5)

5. Your laptop sends an HTTP GET request across the TCP connection
    - If you're using HTTPS, it performs a TLS handshake and encrypts the request before splitting it into TCP packets
    - Any future connections restart from step 3 with a new DNS request

PA4:
Network Attacks

PA4 Overview

- Scavenger hunt! You need to find Nadia's "password" in the form of a token
- You should be receiving a tar.gz file in your email
  - This will be the starting point
- The email you should received should be
  - Subject: [CSE 127] PA4 Flash Drive Dump
  - From: root@bungle.sysnet.ucsd.edu
- Please be cautious of spoilers, utilize OH and private Piazza posts
- START EARLY! You could be stuck for a while if you don't know what to do, and it can be hard to estimate how much further you still have to go

PA4 Logistics

- Deadline: Thursday, 3/3 6:00pm
- Submit to each of the Gradescope assignments:
  - Part A: Mystery
    - What to submit revealed in the middle of the PA
  - Part B: Token
    - Submit a single file named "token"
  - Part C: Writeup
    - Any file briefly describing what you did to achieve the end goal

General Tips

- At every point ask yourself:
  - “How can I find information that is hidden?”
    - Concealed, but still discoverable
- Some of the steps take time
- Try to find the commands as well as the options that give you exactly what you need

Tools for PA4

List of Tools You May Need

- nc - Allows you to make connections locally
- nmap - Scan ports/IPs (locally and externally)
- ssh - Connect to servers over shell
- tcpdump - View network traffic on machine
- wget - Download files from the internet
- **Check out all their "man" pages**

netcat

Julia Evans
wizardzines.com

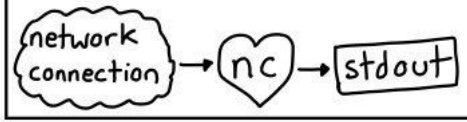
nc

like 'cat' for your network!

it lets you create TCP (or UDP) connections from the command line & send/receive data

nc -l PORT

start a server! this listens on PORT & prints everything received



nc IP PORT

be a client! opens a TCP/UDP connection to IP:PORT.

send files

want to send a 100 GB file to someone on the same wifi network? easy!

receiver:

```
nc -l 8080 > file
```

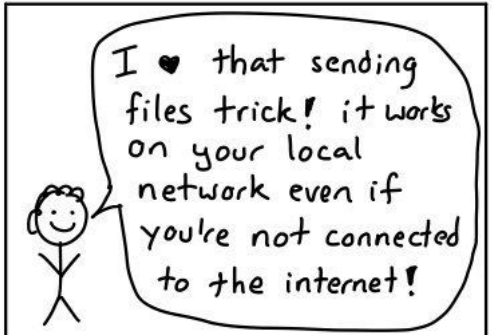
sender: (192.168.x.x)

```
cat file | nc YOUR_IP 8080
```

make HTTP requests by hand

```
printf 'GET / HTTP/1.1\nHost: example.com\r\n\r\n' | nc example.com 80
```

type in any weird HTTP request you want! 😈



tcpdump

- Used to display TCP/IP and other packets that are transported over a network the machine is in
- Reading the tcpdump of a machine can be very noisy
  - Use "tcpdump -D" to see what interfaces are available
  - Specify an interface with the "-i" option
- By default, tcpdump only looks at packet header information
  - If you wish to view the packet contents, you must use the "-X" or "-A" options

Good Luck!

Due Date: Thursday, March 3rd, 6:00PM