Announcement

- Quizzes
  - Option 1: Week 12 – 15, one each week
  - Option 2: After lectures end (Dec.5), and before the final (Dec.14)
  - Option 3: A combination of both 1 and 2
- Lecture schedule
- Project #2 to be released Thursday
  - To be released at Nov.2 11:59am
  - Due Nov.16 11:59pm
- Computing Research Association survey
  - Will open an assignment at Canvas
  - Submit a screenshot that you have finished the survey (Extra 1%)

Today’s Plan

- Network Attackers
  - Man-in-the-middle attacker
  - On-path attacker
  - Off-path attacker
- Important Concepts
  - **ARP: Translate IP addresses to MAC addresses**
  - DHCP: Get configurations when first connecting to a network
  - WPA: Communicate securely in a wireless local network
  - TCP: Reliably send packets
  - UDP: Not-reliably send packets
  - TLS: Secure TCP, securely send packets
  - DNS: Lookup IP address from domain names

Network Attackers

Types of Network Attackers

- Threat model: There are 3 types of attackers we'll consider

	Can modify or delete packets	Can read packets
Man-in-the-middle	✓	✓
On-path attacker		✓
Off-path attacker		

Spoofing

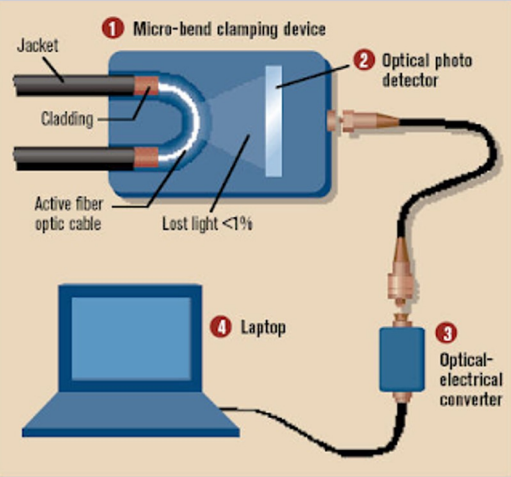
- **Spoofing**: Lying about the identity of the sender
  - Example: Mallory sends a message and says the message is from Alice
  - The attacker can lie about the *source address* in the packet header

- All types of attackers can spoof packets
  - However, some spoofing attacks may be harder if the attacker can’t read or modify packets

Real-World On-Path Attackers

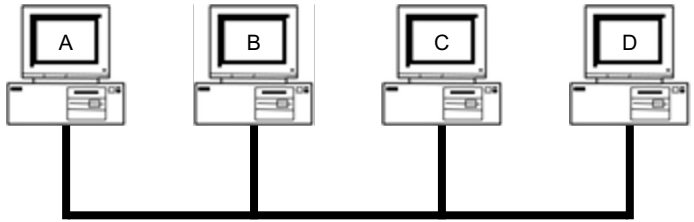
ITIS 6200 / 8200

- How might a real-life attacker read packets?
- Layer 1 attack: Use a special device to read bits being transmitted across space



Real-World On-Path Attackers

- Layer 2 attack: Read packets sent across the local area network (LAN)
- Recall: A LAN is a network of connected machines
  - Any machine on the LAN can send packets to any other machine on the LAN
- Some LANs use **broadcast technologies**
  - Every packet gets sent to every machine on the LAN
  - Each machine agrees to ignore packets where the destination is a different machine
- A machine can break the agreement and read packets meant for other machines
  - This is called **promiscuous mode**
  - May require root access on the machine

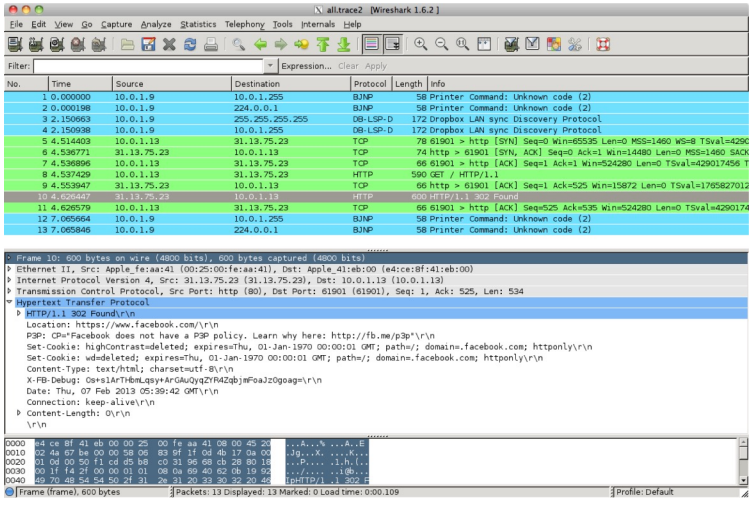


Real-World On-Path Attackers

ITIS 6200 / 8200

- **`tcpdump`**: A program for reading packets on the local network
  - Uses promiscuous mode to read other machines' packets in broadcast technologies
- Wireshark: A graphical user interface (GUI) for analyzing **`tcpdump`** packets

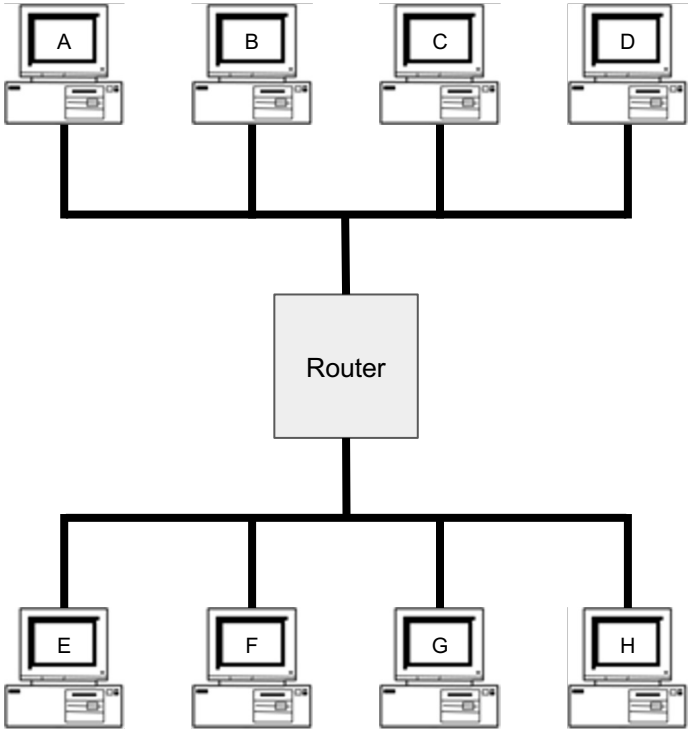
```
demo 2 % tcpdump -r all.trace2
reading from file all.trace2, link-type EN10MB (Ethernet)
21:39:37.772367 IP 10.0.1.9.60627 > 10.0.1.255.canon-bjnp2: UDP, length 16
21:39:37.772565 IP 10.0.1.9.62137 > all-systems.mcast.net.canon-bjnp2: UDP, length 16
21:39:39.923030 IP 10.0.1.9.17500 > broadcasthost.17500: UDP, length 130
21:39:39.923305 IP 10.0.1.9.17500 > 10.0.1.255.17500: UDP, length 130
21:39:42.286770 IP 10.0.1.13.61901 > star-01-02-pao1.facebook.com.http: Flags [S], seq 2
523449627, win 65535, options [mss 1460,nop,wscale 3,nop,nop,TS val 429017455 ecr 0,sack
OK,eol], length 0
21:39:42.309138 IP star-01-02-pao1.facebook.com.http > 10.0.1.13.61901: Flags [S.], seq
3585654832, ack 2523449628, win 14480, options [mss 1460,sackOK,TS val 1765826995 ecr 42
9017455,nop,wscale 9], length 0
21:39:42.309263 IP 10.0.1.13.61901 > star-01-02-pao1.facebook.com.http: Flags [.], ack 1
, win 65535, options [nop,nop,TS val 429017456 ecr 1765826995], length 0
21:39:42.309796 IP 10.0.1.13.61901 > star-01-02-pao1.facebook.com.http: Flags [P.], seq
1:525, ack 1, win 65535, options [nop,nop,TS val 429017456 ecr 1765826995], length 524
21:39:42.326314 IP star-01-02-pao1.facebook.com.http > 10.0.1.13.61901: Flags [.], ack 5
25, win 31, options [nop,nop,TS val 1765827012 ecr 429017456], length 0
21:39:42.398814 IP star-01-02-pao1.facebook.com.http > 10.0.1.13.61901: Flags [P.], seq
1:535, ack 525, win 31, options [nop,nop,TS val 1765827083 ecr 429017456], length 534
21:39:42.398946 IP 10.0.1.13.61901 > star-01-02-pao1.facebook.com.http: Flags [.], ack 5
35, win 65535, options [nop,nop,TS val 429017457 ecr 1765827083], length 0
21:39:44.838031 IP 10.0.1.9.54277 > 10.0.1.255.canon-bjnp2: UDP, length 16
21:39:44.838213 IP 10.0.1.9.62896 > all-systems.mcast.net.canon-bjnp2: UDP, length 16
```



Address Resolution Protocol (ARP)

Review: Layer 2 and Layer 3

- Local area network (LAN): A set of machines connected in a local network
  - The MAC identifies devices on layer 2
- Internet protocol (IP): Many LANs connected together with routers
  - The IP identifies devices on layer 3

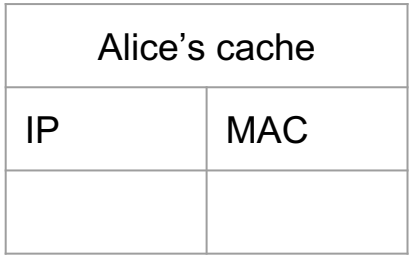


Address Resolution Protocol (ARP)

- **ARP**: Translates layer 3 IP addresses to layer 2 MAC addresses
  - Example: Alice wants to send a message to Bob on the local network, but Alice only knows Bob's IP address (**1.2.3.4**). To use layer 2 protocols, she must learn Bob's MAC address.
- Steps of the protocol
  a. Alice checks her cache to see if she already knows Bob's MAC address.
  b. If Bob's MAC address is not in the cache, Alice **broadcasts** to everyone on the LAN: "What is the MAC address of **1.2.3.4**?"
  c. Bob responds by sending a message only to Alice: "My IP is **1.2.3.4** and my MAC address is **ca:fe:f0:0d:be:ef**." Everyone else does nothing.
  d. Alice caches Bob's MAC address.

Address Resolution Protocol (ARP)

Alice knows Bob's IP address (`1.2.3.4`) but wants to learn Bob's MAC address.



Alice

Bob

Charlie

Dave

Router

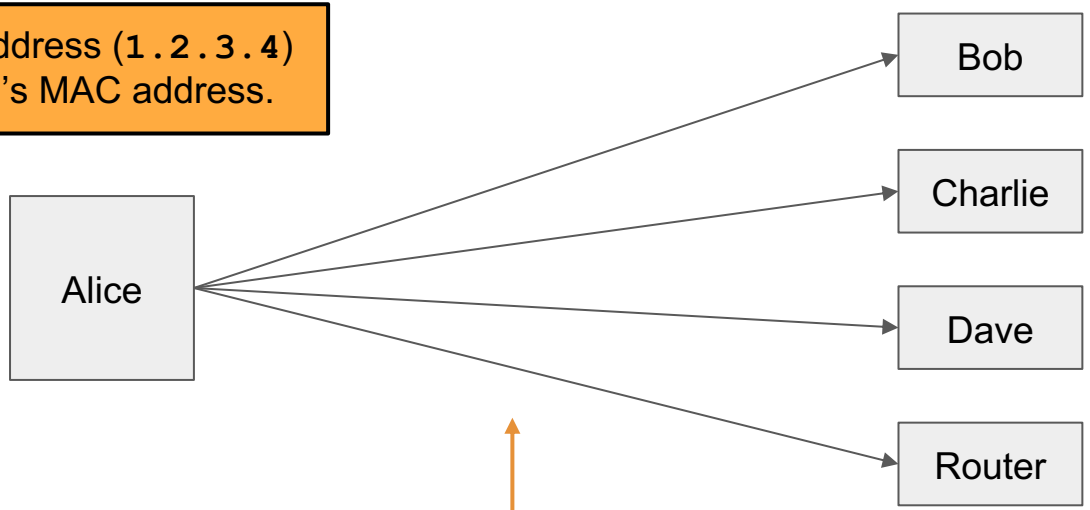
1. Alice checks her cache to see if she already knows the MAC address corresponding to `1.2.3.4`.

Since her cache is empty, she must make a request to find out.

Address Resolution Protocol (ARP)

Alice knows Bob's IP address (`1.2.3.4`) but wants to learn Bob's MAC address.

Alice's cache	
IP	MAC

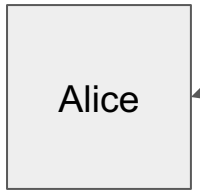


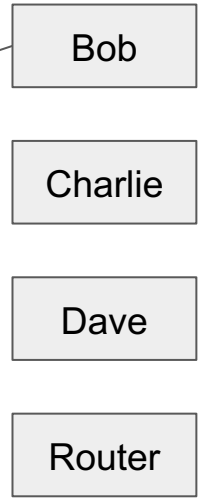
2. Alice asks everyone else on the local network: "What is the MAC address of `1.2.3.4`?"

Address Resolution Protocol (ARP)

Alice knows Bob's IP address (`1.2.3.4`) but wants to learn Bob's MAC address.

Alice's cache	
IP	MAC



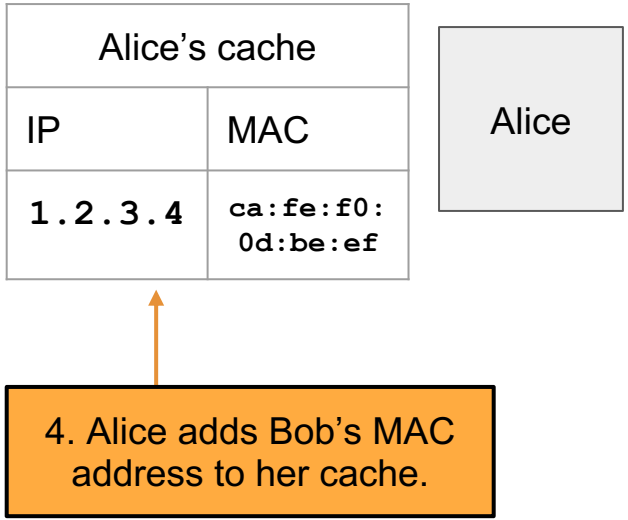


3. Bob responds: "My IP is `1.2.3.4` and my MAC address is `ca:fe:f0:0d:be:ef`."

Everybody else ignores the request.

Address Resolution Protocol (ARP)

Alice knows Bob's IP address (`1.2.3.4`) but wants to learn Bob's MAC address.



Bob

Charlie

Dave

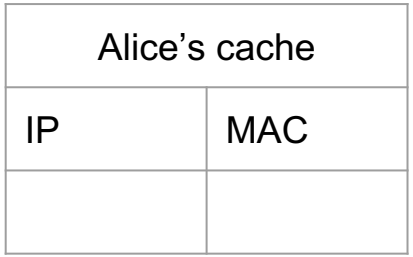
Router

Address Resolution Protocol (ARP)

- If Bob is outside of the LAN, Alice knows this
  - Bob’s IP is not on the same “subnet” as Alice
- But Alice knows the IP address of the “Gateway router”
  - Recall: The router’s job is to make sure that the packet will be forwarded towards Bob (Layer 3)
- So instead Alice generates an ARP request for the gateway router
  - Layer 2 MAC address of the frame is set to the router
  - Layer 3 IP address of the packet remains set as Bob's
  - The router will forward the packet to some other LAN to get it closer to Bob

Attacks on ARP

Alice knows Bob's IP address (**1.2.3.4**) but wants to learn Bob's MAC address.



Alice

Bob

Charlie

Mallory

Router

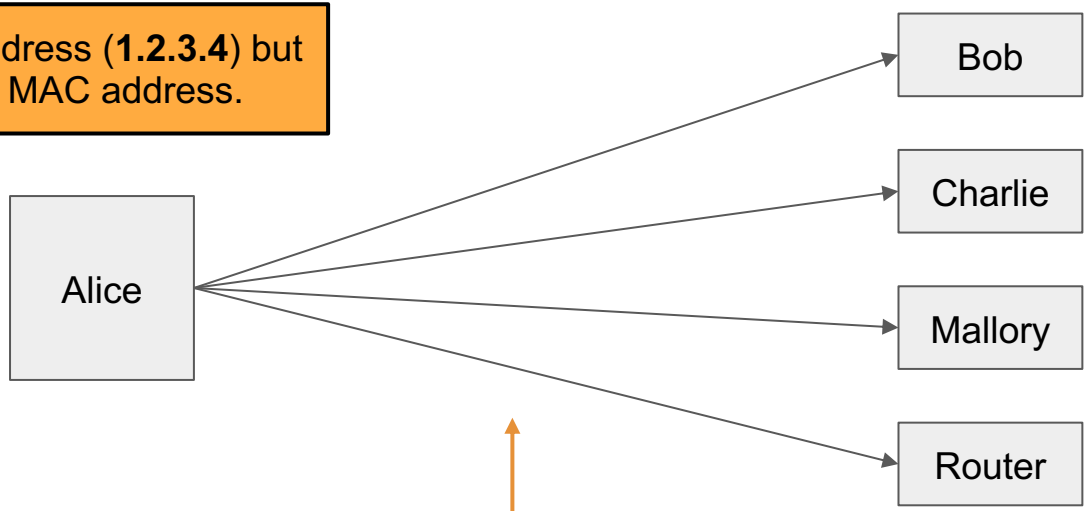
1. Alice checks her cache to see if she already knows the MAC address corresponding to **1.2.3.4**.

Since her cache is empty, she must make a request to find out.

Attacks on ARP

Alice knows Bob's IP address (**1.2.3.4**) but wants to learn Bob's MAC address.

Alice's cache	
IP	MAC

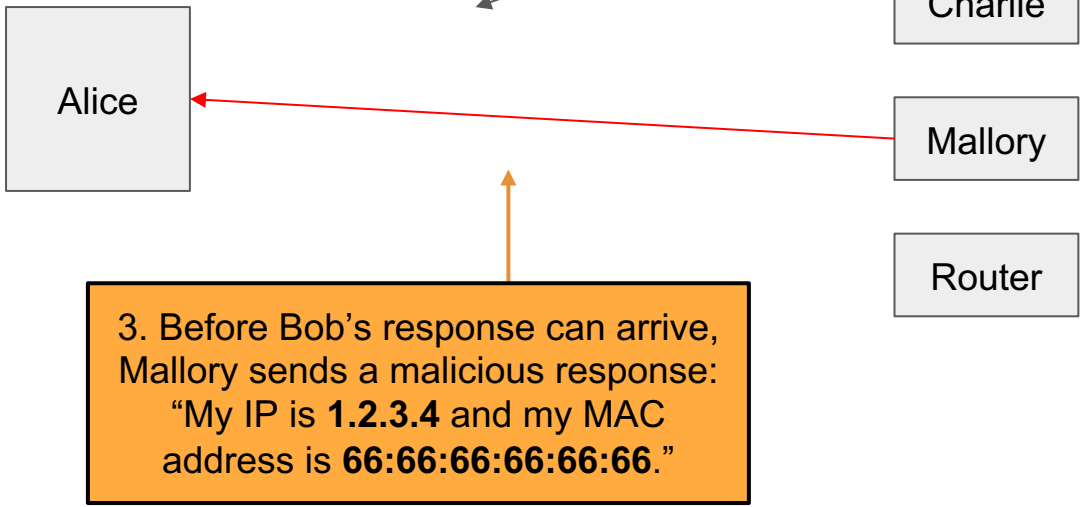


2. Alice asks everyone else on the local network: "What is the MAC address of **1.2.3.4**?"

Attacks on ARP

Alice knows Bob's IP address (`1.2.3.4`) but wants to learn Bob's MAC address.

Alice's cache	
IP	MAC



Attacks on ARP

Alice knows Bob's IP address (`1.2.3.4`) but wants to learn Bob's MAC address.

Alice's cache	
IP	MAC
1.2.3.4	**66:66:66:66:66:66**

Alice

Bob

Charlie

Mallory

Router

4. Alice adds Mallory's malicious address to her cache.

Attack: ARP Spoofing

- Alice has no way of verifying the ARP response
  - Spoofing: Any attacker on the network can claim to have the requested IP address
- Alice is only expecting one machine to respond, so she will accept the first response
  - **Race condition**: As long as the attacker responds faster, the requester will accept the attacker's response
- ARP spoofing requires Mallory to be in the same LAN as Alice
- ARP spoofing lets Mallory become a man-in-the-middle (MITM) attacker
  - Alice thinks that Bob's MAC address is **66:66:66:66:66:66** (Mallory's MAC address)
  - When Alice sends a message to Bob, she is actually sending the message to Mallory
  - Mallory can modify the message and then send the modified message to Bob

ARP Spoofing: Defenses

- Network switches
  - When Alice wants to send a message to Bob, she sends the message to a switch on the LAN
  - The switch maintains a cache of MAC to port (physical connection) mappings
  - If Bob's MAC address is in the cache, the switch sends the message directly to Bob
  - Otherwise, the switch broadcasts the message to all computers
- Enterprise-class switches have additional optional features
  - Security: An additional IP/MAC cache that responds first, preventing the attacker from seeing repeated requests
  - Security: Only authorized MAC addresses can connect to specific ports—access control
  - Isolation: Virtual local area networks (VLANs), which splits a single LAN into isolated parts
- Tools like **`arpwatch`** track ARP responses and make sure that there is no suspicious activity

Important Concepts

Network Protocols

Layer	Protocols
7. Application	Web Security
4.5. Secure transport	TLS
4. Transport	TCP, UDP
3. Internet	IP
2. Link	ARP
1. Physical	WPA

Extra Protocols	
Connect for the first time	DHCP
Convert hostname to IP address	DNS, DNSSEC

Important Protocols

- ARP: A protocol to translate local IP addresses to MAC addresses
  - Ask everyone on the network, “Who has the IP 1.2.3.4?”
- DHCP: A protocol for a new client to receive a network configuration
  - Ask everyone on the network, “What is the network configuration to use?”
- WPA: A protocol to encrypt Wi-Fi connections at layer 1
  - A protocol for securing Wi-Fi network communications with cryptography
- Transmission Control Protocol (TCP)
  - Reliably sending packets
- User Datagram Protocol (UDP)
  - Non-reliably sending packets

Transmission Control Protocol (TCP)

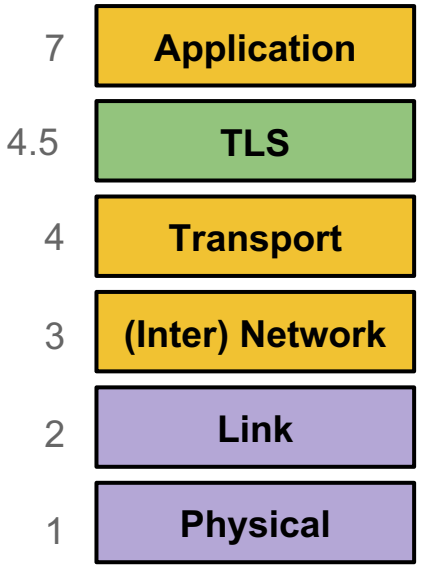
- Provides a byte stream abstraction
  - Bytes go in one end of the stream at the source and come out at the other end at the destination
  - TCP automatically breaks streams into **segments**, which are sent as layer 3 packets
- Provides ordering
  - Segments contain sequence numbers, so the destination can reassemble the stream in order
- Provides reliability
  - The destination sends **acknowledgements** (ACKs) for each sequence number received
  - If the source doesn't receive the ACK, the source sends the packet again
- Provides ports
  - Multiple services can share the same IP address by using different ports

User Datagram Protocol (UDP)

- Provides a **datagram** abstraction
  - A message, sent in a single layer 3 packet (though layer 3 could fragment the packet)
  - Max size limited by max size of packet
  - Applications break their data into datagrams, which are sent and received as a single unit
    - Contrast with TCP, where the application can use a bytestream abstraction
- No reliability or ordering guarantees, but adds ports
  - It still has *best effort* delivery
- Much faster than TCP, since there is no 3-way handshake
  - Usually used by low-latency, high-speed applications where errors are okay (e.g. video streaming, games)

TLS (Transport Layer Security)

- **TLS** (**Transport Layer Security**): A protocol for creating a secure communication channel over the Internet
  - Replaces **SSL** (**Secure Sockets Layer**), which is an older version of the protocol
- TLS is built on top of TCP
  - **Relies upon**: Byte stream abstraction between the client and the server
  - **Provides**: Byte stream abstraction between the client and the server
    - The abstraction appears the same to the end client, but TLS provides confidentiality and integrity!
- Can be used by the application layer (e.g. HTTPS)

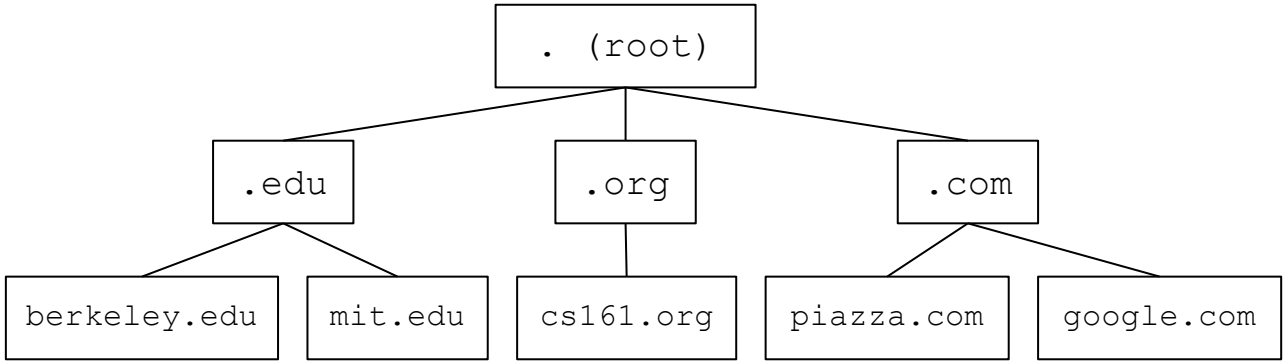


TLS (Transport Layer Security)

- Goals of TLS
  - **Confidentiality**: Ensure that attackers cannot read your traffic
  - **Integrity**: Ensure that attackers cannot tamper with your traffic
    - Prevent **replay attacks**
      - The attacker records encrypted traffic and then replays it to the server
      - Example: Replaying a packet that sends “Pay $10 to Mallory”
  - **Authenticity**: Make sure you’re talking to the legitimate server
    - Defend against an attacker impersonating the server

DNS

- DNS (Domain Name System): An Internet protocol for translating human-readable domain names to IP addresses
  - DNS name servers on the Internet provide answers to DNS queries
  - Name servers are arranged in a domain hierarchy tree
  - Lookups proceed down the domain tree: name servers will direct you down the tree until you receive an answer



DNS Security

- Cache poisoning attack: Send a malicious record to the resolver, which caches the record
  - Causes packets to be sent to the wrong place (e.g. to the attacker, who becomes a MITM)
- Risk: Malicious name servers
  - Defense: Bailiwick checking: Resolver only accepts records in the name server's zone
- Risk: Network attackers
  - MITM attackers can poison the cache without detection
- DNSSEC: An extension of the DNS protocol that ensures integrity on the results