CMSC 426
Principles of Computer Security

Introduction to Networks

Last Class We Covered

- Offensive security
  - What it is
  - Attacker Lifecycle
  - Common tools
- Demo
- Effective Windows Hardening

Any Questions from Last Time?

Today's Topics

- Intro to TCP/IP model

- Link layer
- Internet layer
- Transport layer
- Application layer

Internet Protocol Suite

TCP/IP

- TCP = Transmission Control Protocol
- IP = Internet Protocol

- Communication protocols used to connect devices on a network, such as the Internet
  - Protocols specify how data should be packaged, transmitted, routed, received, etc.
  - Protocols are split into four layers

TCP/IP Layers

- From “lowest” (closer to physical transmission of data) to “highest” (closer to the user application) the layers are...

- Link layer
- Internet layer (or network)
- Transport layer
- Application layer

- Each of these layers is present on both sides of communication

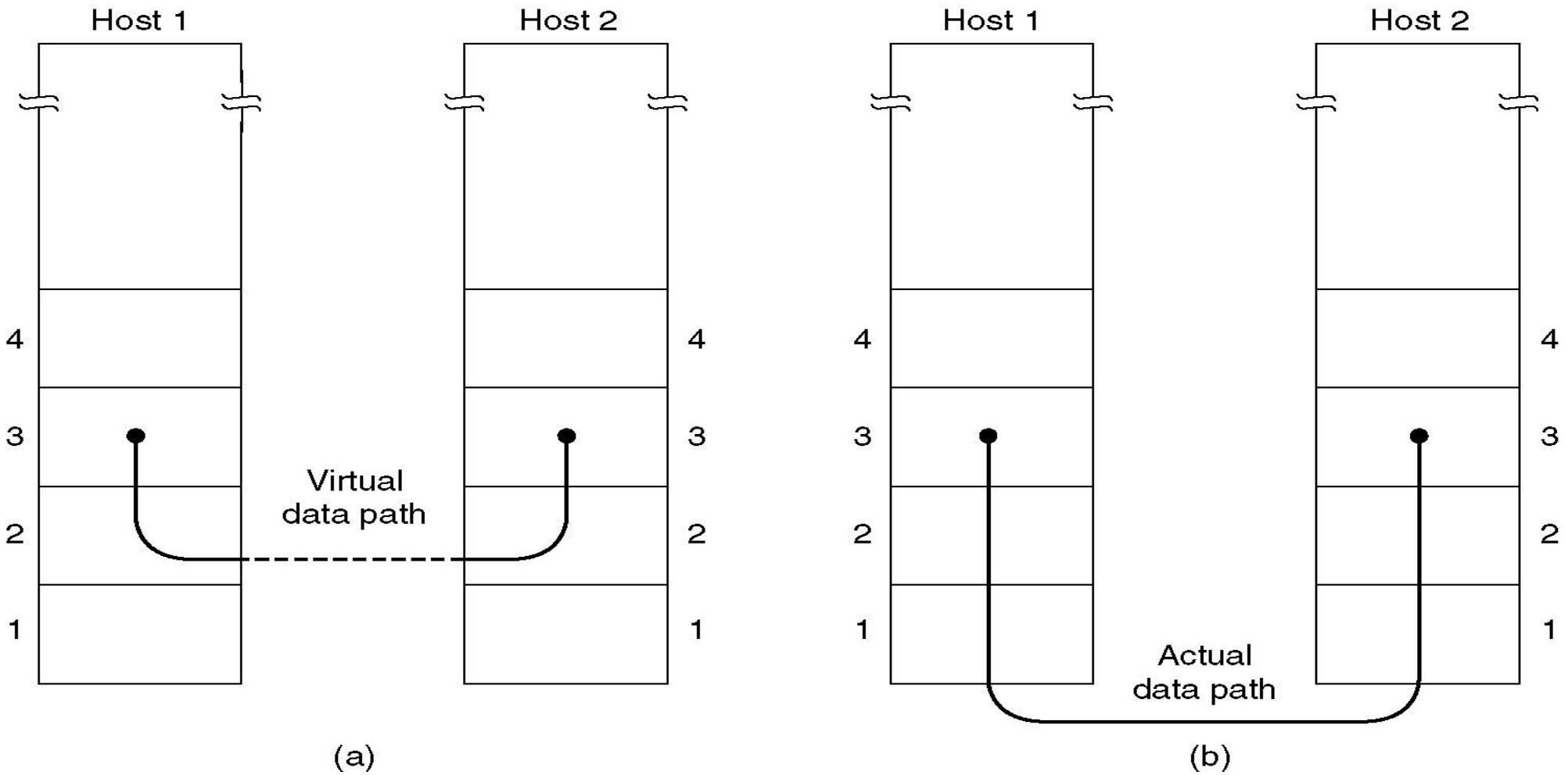


Image from Computer Networks (Tanenbaum)

Link Layer

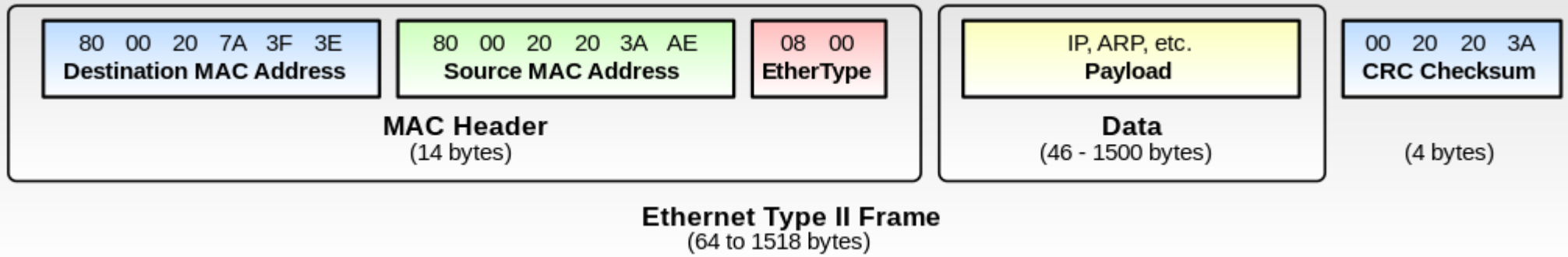
Link Layer's Purpose

- How data is generated and physically transmitted over the network by connected devices
  - Interface between physical hardware and the internet layer

- Ensures reliable delivery
- Controls point-to-point access
- Handles error detection and correction

Link Layer: Framing and MAC addresses

- ***Framing*** encapsulates the data sent from the internet layer within a link-layer frame before transmission over the link
  - Contains additional header fields with important information



- MAC addresses (Media Access Control) are unique identifiers assigned to network interfaces
  - Similar to a person's SSN (permanent and very difficult to change)

Internet Layer

Internet Layer's Purpose

- Concerned with getting packets from one end to another
  - Packet format is defined by the IP (Internet Protocol)
  - Packet routing and congestion are major issues

- Provides only unreliable service and best effort delivery
  - Makes no guarantee about correct or eventual arrival of packets
  - Burden of reliability is placed on the hosts instead (not the network)

Internet Layer: Routing Data

- Routing algorithms attempt to find the most efficient path between a source and a destination
  - ***Completely*** out of scope for this course

- Routing tables contain information about the topology of the network immediately around (directly connected and remote)
  - Used by the routing algorithm as a sort of “cache” of information, to allow it to more quickly compute the route to be taken

IP Addresses

- Unique identifier for a host on a TCP/IP network
- 32-bit address
  - Composed of four 8-bit “octets” separated by dots
  - *e.g.*, 192.168.84.2
- IP addresses have 2 parts: network address and host address
- Routers don’t know exact host location, just which network it’s on
  - Network address used by router to get packets to the correct network
  - Once packet is delivered to correct network, it can be delivered to the host using the host address

Internet Layer: Subnet Mask

- Used to determine which half of the IP address is the network address and which half is the host address
- The IP address is bitwise-ANDed with the subnet mask to get the network address
- The rest of the IP address is the host address

- Example of a typical subnet mask:
  - `255.255.255.0`

Internet Layer: Subnet Mask Example

```
192.168.84.2   → 11000000.10101000.01010100.00000010
255.255.255.0 → 11111111.11111111.11111111.00000000

11000000.10101000.01010100.00000010 AND
11111111.11111111.11111111.00000000 =
11000000.10101000.01010100.0000000
```

- Converting back to decimal gives 192.168.84.0 as network address and .2 as the host address

Internet Layer: CIDR Notation

- Shorthand notation used to express IP address and subnet mask
- Written as the IP address, a slash, and a number (less than 32)
- For example:
  - **`192.168.84.2/24`**

- The number after the slash is the number of 1 bits on the left of the subnet mask
  - So the value will never be higher than 32

Internet Layer: Default Gateway

- When a computer wants to communicate with another computer, it computes that computer's network address using its IP address and subnet mask
- If they are on the same local network, it can simply send packets to that computer
- Otherwise, packets are forwarded to the default gateway
  - Router used to send traffic to other networks
  - It is the router's responsibility to make sure packets end up in the right place

Internet Layer: IPv6

- We've been talking about the IPv4 protocol
- IPv4 addresses are 32 bits, so there's only ~4 billion of them
  - We're running out!
- IPv6 addresses have 128 bits

- Separated into 8 16-bit segments, written in hex
  - `2001:0db8:85a3:0000:0000:8a2e:0370:7334`
- Adoption of IPv6 has been slow

Internet Layer: ARP

- ARP stands for “Address Resolution Protocol”
- Used to discover the link layer MAC address associated with an IPv4 address
  - For IPv6, the protocol is called NDP (Neighbor Discovery)
  - Only works on machines in the same subnet

- MAC addresses are hex, and IP addresses are decimal
  - There is no correlation between MAC and IP address values
  - Instead, each host and router has an ARP table in its memory

Transport Layer

Transport Layer's Purpose

- Transports application-layer messages

- One common protocol is TCP
  - Guarantees delivery to the destination
  - Controls flow of data (match speed of sender/receiver)

  - When sending, segments incoming byte stream into discrete messages before sending to internet layer
  - When receiving, reassembles the received messages

Transport Layer: Three-Way Handshake

- Primarily used to create a socket connection for TCP
  - SYNchronize and ACKnowledge packets
- Client sends a SYN data packet to a server
  - Objective is to determine if the server is open for new connections
- Target server receives SYN packet
  - If it has open ports that can accept and initiate new connections, it respondsd and returns a confirmation receipt – SYN/ACK
- Client receives the SYN/ACK from the server and responds with an ACK packet

Information from https://www.techopedia.com/definition/10339/three-way-handshake

Transport Layer: UDP

- UDP (User Datagram Protocol)

- UDP is a connectionless, no-frills alternative to TCP
  - No reliability
  - No flow control
  - No congestion control

- Used when quick delivery is more important than accuracy
  - Streaming data falls under this, especially as “lost” data is of minimal importance, as it is constantly replaced by new incoming information

Application Layer

Application Layer's Purpose

- "Top" layer that is closest to the end user
- Contains all the higher-level protocols

- Simply standardizes communication
  - Relies heavily on the transport layer beneath it to establish connections and manage data exchange

Application Layer: DHCP

- Dynamic Host Configuration Protocol
- Network management protocol that dynamically assigns IP addresses to each device on a network
- Happens upon device first connecting to the network

Application Layer: DNS

- Domain Name System
- Essentially, allows a human-readable domain to be translated into its corresponding IP address
  - People are bad at remembering random numbers in a sequence
- Details are outside of the scope of this class

Application Layer: HTTP

- Hypertext Transfer Protocol
- Not the same as HTML (Hypertext Markup Language)
- Request-response protocol in a client-server model
  - Use different HTML message types to communicate
  - GET, POST, and HEAD

Application Layer: TLS/SSL

- TLS (Transport Layer Security)
- SSL (Secure Sockets Layer)
  - Deprecated, replaced by TLS

- Cryptographic protocols that provide communication security
- Use a handshake procedure to establish a secure connection

Application Layer: TLS Handshake

- Client connects to a TLS-enabled server
  - Requests a secure connection
  - Presents a list of supported cipher suites (ciphers and hash functions)
- Server picks a set it also supports and notifies the client
  - Server then provides identification in the form of a digital certificate
  - The certificate contains info about the server and its public key
- Client confirms the validity of the certificate before proceeding
- To generate session keys for the secure connection, client either:
  - Encrypts a random number with the server's public key and sends the result to the server; both parties then use the random number to generate a unique session key for subsequent encryption and decryption of data during the session
  - Uses Diffie-Hellman key exchange (secure even if server's private key is leaked later)

Information from https://en.wikipedia.org/wiki/Transport_Layer_Security

Application Layer: HTTPS

- Stands for “HTTP Secure”
- Use of HTTP where the communication is encrypted with TLS
- Allows authentication of the website being accessed, and protects the privacy and integrity of the exchanged data
  - Originally used mostly for payments, banking, and sensitive email
  - Much more widely used now

Application Layer: FTP

- File Transfer Protocol
  - FTPS = FTP Secure
  - SFTP = SSH FTP

- Default mode is clear-text (completely unsecured)

Application Layer: SMTP

- Simple Mail Transfer Protocol
- Standard for email transmission
- Other protocols:
  - POP3 (Post Office Protocol version 3)
    - Used to retrieve email
  - IMAP (Internet Message Access Protocol)
    - Also retrieves email, but syncs with the mail server

Announcements

- Lab 4 will be released this week
  - Total VM size will be large (~20 GBs) so prepare your machine
- Homework 4 will be released next week
- Remaining assignments will have their point values rolled into the final exam (HW5, Papers 4 and 5)
  - 40 additional points, for 190 total points on the final exam

Image Sources

- Ethernet frame
  - https://commons.wikimedia.org/wiki/File:Ethernet_Type_II_Frame_format.svg