Lecture 1 Activity: Analyzing HTTPS

(Fast Learner)

Case Study: Analyzing How HTTPS Works Across OSI Layers

Scenario: You're a cybersecurity intern at a fintech company. A junior developer asks you to explain how HTTPS works when a user visits https://www.bank.com. Your task is to explain what happens at each layer of the OSI model and answer related questions to ensure understanding.

How HTTPS Works (Layer-by-Layer)

1. Application Layer (Layer 7):
   - HTTPS (which is HTTP over SSL/TLS) is initiated.
   - The browser requests the secure page using HTTPS.
   - The server sends back its SSL/TLS certificate.
2. Transport Layer (Layer 4):
   - TLS handshake begins.
   - Uses TCP to establish a reliable connection.
   - Encryption keys are exchanged securely.
3. Network Layer (Layer 3):
   - IP addresses (source and destination) are used to route data packets.
   - Routers forward the encrypted packets to the destination server.
4. DATA Link Layer (Layer 2):
   - Frames are created, and MAC addresses are used to deliver frames on local networks.
   - Switches operate at this layer to move frames.

Questions and Answers

Question 1: Which protocol is responsible for encrypting HTTP traffic in HTTPS?

A. FTP
B. TCP
C. TLS/SSL
D. IP

Answer: C. TLS/SSL

Question 2: Fill in the Blank

At the Transport Layer, HTTPS uses the _____ protocol to ensure reliable data delivery.

Answer: TCP

Question 3: Short Answer

What is the main function of the Network Layer when a client connects to an HTTPS website?

Answer:

To route encrypted data packets across networks using IP addresses from source to destination.

Question 4: Scenario-Based

If a switch is used to forward HTTPS packets within a local area network, at which OSI layer is it operating?

Answer:

Data Link Layer (Layer 2) – Uses MAC addresses to forward frames.

Question 5: True or False
TLS encryption is applied at the Network Layer to protect data between the client and server.
Answer:
False – TLS encryption is applied at the Application/Transport Layer, not at the Network Layer.
Question 6: Matching Exercise
Match the OSI layer with what HTTPS does at that level:

OSI Layer	HTTPS Role
Application	A. TLS handshake, certificate validation
Transport	B. TCP connection, secure session setup
Network	C. Routing encrypted packets using IP addresses
Data Link	D. Forwarding frames with MAC addresses on local networks

Answers:

- Application → A
- Transport → B
- Network → C
- Data Link → D

Question 7: Protocol Identification
Name one protocol used at the Application layer when establishing an HTTPS connection.
Answer:
HTTP (over TLS)
Question 8: Short Answer
Why is TCP used instead of UDP in HTTPS connections?
Answer:
Because TCP provides reliability, sequencing, and error correction, which are essential for secure web communication.

Question 9: Analysis
During the TLS handshake, a digital certificate is used. Which layer is this process associated with?
Answer:
Application Layer – where the certificate is exchanged and validated as part of the HTTPS request.

Lecture 1 Activity: Designing a Protocol Stack
(Fast Learner)
Case Study: Designing a Protocol Stack for Online Banking
Scenario: You're a network architect for a bank. Your team is launching a new online banking platform. Customers will log in, transfer funds, and view transactions from browsers and mobile apps. You must design a protocol stack that ensures security, reliability, and data integrity.
Chosen Protocol Stack for Online Banking

OSI Layer	Protocol(s)	Reasoning
Application	HTTPS (HTTP over TLS), DNS	Secure web communication and domain resolution
Presentation	TLS/SSL	Data encryption and certificate-based authentication
Session	TLS Handshake	Establishes secure sessions between clients and servers
Transport	TCP	Reliable delivery of transaction data
Network	IP (IPv4/IPv6)	Routing packets across networks
Data Link	Ethernet / Wi-Fi (IEEE 802.3/802.11)	Local network data transmission
Physical	Fiber, Ethernet cables, Wi-Fi	Transmitting bits over physical media

Questions and Answers

Question 1: Multiple Choice

Which protocol ensures encrypted communication in the online banking application?

A.FTP

B.HTTP

C.TLS

D. UDP

Answer: C. TLS

Question 2: True or False

TCP is chosen at the Transport layer because it offers faster performance than UDP, even if some packets are lost.

Answer:

False – TCP is chosen for reliability, not speed. It ensures no data loss, which is critical for banking.

Question 3: Fill in the Blank

The protocol _____ is responsible for translating the bank's domain name (e.g., bank.com) into an IP address.

Answer:

DNS

Question 4: Short Answer

Why is HTTPS used instead of HTTP in an online banking system?

Answer:

Because HTTPS uses TLS to encrypt data, preventing eavesdropping, tampering, or impersonation.

Question 5: Matching Exercise

Match each OSI layer with the correct protocol or function in the online banking stack:

OSI Layer	Protocol / Function
Application	A. HTTPS
Transport	B. TCP
Session	C. TLS handshake
Network	D. IP routing

Answers:

- Application → A
- Transport → B
- Session → C
- Network → D

Question 6: Scenario-Based

If a user is experiencing dropped packets while transferring funds, which layer would you inspect to ensure reliability?

Answer:

Transport Layer – to verify TCP is operating correctly and handling retransmissions.

Question 7: Analysis

Why is TLS also associated with the Presentation layer in this model?

Answer:

TLS performs encryption and decryption, which is considered a Presentation layer function (data representation and security).

Question 8: Protocol Identification

What type of network protocols would typically be used at the Data Link layer in a banking office connected via Wi-Fi?

Answer:

IEEE 802.11 (Wi-Fi)

Question 9: Design Thinking

What could be added to the protocol stack to enhance protection against DNS spoofing in online banking?

Answer:

DNSSEC (DNS Security Extensions) – provides origin authentication and data integrity for DNS responses.

Summary

This case study helps learners:

- Understand how real-world applications like online banking use multiple protocols
- See how security, reliability, and performance influence protocol choice
- Practice identifying protocol responsibilities at each OSI layer

Lecture 1 Activity: Protocol Stack Use Case Mapping for WhatsApp

(Fast Learner)

Case Study: Protocol Stack Use Case Mapping for WhatsApp

Scenario: Real-World Application: WhatsApp

WhatsApp is a messaging application that supports text, voice, video, image sharing, and real-time calling functionalities over the internet.

Protocol Mapping to OSI Layers for WhatsApp

OSI Layer	Protocols / Technologies Used in WhatsApp
7. Application	HTTP/HTTPS, WebSocket, Signal Protocol (for E2E encryption), STUN/TURN (for NAT traversal in calls), SIP-like signaling for VoIP features

OSI Layer	Protocols / Technologies Used in WhatsApp
6. Presentation	TLS/SSL (used within HTTPS and secure WebSocket to encrypt/decrypt data), Compression (e.g., for media messages)
5. Session	TLS handshake management, WebSocket session management, and NAT traversal session control
4. Transport	TCP (for message delivery and control), UDP (for real-time voice/video calls)
3. Network	IP (Internet Protocol) for routing across the Internet
2. Data Link	Ethernet/Wi-Fi Protocols (like IEEE 802.11) for local network communication
1. Physical	Physical transmission via network adapters, fiber optics, 4G/5G radio waves, etc.

Student Q&A Section

Q1: What layer of the OSI model does the Signal Protocol work at in WhatsApp?

A1: The Signal Protocol operates at the Application Layer (Layer 7) and is used to provide end-to-end encryption for messages, voice, and video communications.

Q2: Which transport layer protocols are used by WhatsApp, and why?

A2: WhatsApp uses:

- TCP for reliable delivery of messages and media.
- UDP for real-time voice and video calls because it offers lower latency and is more tolerant of dropped packets.

Q3: How does WhatsApp ensure secure communication between users?

A3: WhatsApp uses TLS/SSL for secure transport over HTTP/HTTPS and Signal Protocol for end-to-end encryption of messages. This ensures that messages are encrypted on the sender's device and decrypted only on the recipient's device.

Q4: What role does the Network Layer play in WhatsApp's functionality?

A4: The Network Layer (Layer 3) is responsible for routing packets between users over the Internet. WhatsApp uses the IP protocol to assign addresses and direct data packets from one user's device to another.

Q5: What happens at the Data Link Layer when a WhatsApp message is sent?

A5: At the Data Link Layer (Layer 2), the message is encapsulated into frames and sent over the local network (e.g., Wi-Fi or mobile network) using protocols like IEEE 802.11 (Wi-Fi) or LTE standards.

Q6: How does WhatsApp handle NAT traversal in voice/video calls?

A6: WhatsApp uses STUN and TURN protocols to manage NAT traversal, allowing devices behind different routers to establish peer-to-peer connections or use relay servers when needed.

Q7: Why are both TCP and UDP necessary in WhatsApp?

A7: WhatsApp needs TCP for reliable message delivery (text, files) and UDP for faster, real-time communication (voice, video) where speed is prioritized over reliability.

Q8: Which layer handles data compression in WhatsApp?

A8: Data compression typically occurs at the Presentation Layer (Layer 6) to reduce the size of data, such as images or voice, before sending it over the network.

Q9: What role does the Physical Layer play in WhatsApp communication?

A9: The Physical Layer (Layer 1) handles the actual transmission of bits over the physical medium—this could include 4G/5G signals, Wi-Fi radio waves, or electrical signals over Ethernet cables.