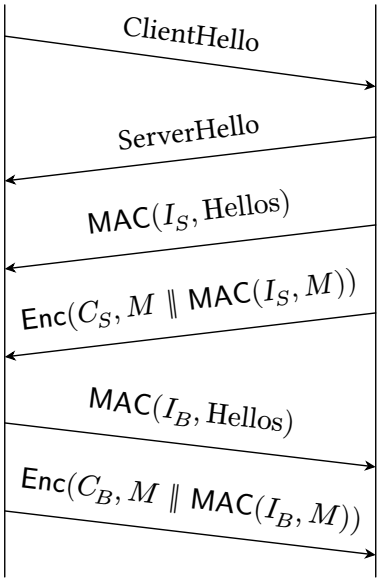
CS161 Fall 2026 — Introduction to Computer Security — Exam Prep 6

Q1 *Networking: TLSplit* 🔨 **(12 points)**



Consider the modified TLS handshake shown in the diagram:

1. **ClientHello**: Client sends $g^a \bmod p$ (ephemeral Diffie-Hellman value) and R_B (random nonce).
2. **ServerHello**: Server sends $g^b \bmod p$ (ephemeral Diffie-Hellman value) and R_S (random nonce).
3. The Client and Server derive the symmetric keys (I_S, I_B, M_S, M_B) using the premaster secret $g^{ab} \bmod p$ and the random nonces R_B, and R_S.
4. The Server sends the MAC on both Hello messages.
5. The Server MACs and encrypts a message and sends it to the Client.
6. The Client sends the MACs on the Hello messages.
7. The Client MACs and encrypts a message and sends it to the Server.

Note: The version of this question featured in the exam contained answer choices that referred to variables from an older version of the question. This was clarified, and has been corrected for this version of the exam.

Q1.1 (1 point) True or False: This scheme ensures forward secrecy.

○ True ○ False

Q1.2 (1 point) True or False: This scheme guarantees that the client is talking to the legitimate server.

○ True ○ False

Suppose the Client and Server start a connection in the presence of Mallory. Mallory is a man-in-the-middle attacker who wants to send messages to the client after the TLS handshake is completed.

Q1.3 (1 point) After the ClientHello has been recieved, Mallory replaces the ServerHello. What values should Mallory send to the client?

○ $g^a \bmod p$ and R_m ○ $g^b \bmod p$ and R_m

○ $g^m \bmod p$ and R_m ○ R_m

This content is protected and may not be shared, uploaded, or distributed.

Q1.4 (2 points) After Q1.3, what values will the **Client** use to derive the symmetric keys in Step 3?

- ☐ a
- ☐ m
- ☐ b
- ☐ $g^a \bmod p$
- ☐ $g^m \bmod p$
- ☐ $g^b \bmod p$
- ☐ R_B
- ☐ R_m
- ☐ R_S

Q1.5 (2 points) After Q1.3, what values will the **Server** use to derive the symmetric keys in Step 3?

- ☐ a
- ☐ m
- ☐ b
- ☐ $g^a \bmod p$
- ☐ $g^m \bmod p$
- ☐ $g^b \bmod p$
- ☐ R_B
- ☐ R_m
- ☐ R_S

Q1.6 (2 points) After Q1.3, what values will **Mallory** use to derive the same symmetric keys as the Client in Step 3?

- ☐ a
- ☐ m
- ☐ b
- ☐ $g^a \bmod p$
- ☐ $g^m \bmod p$
- ☐ $g^b \bmod p$
- ☐ R_B
- ☐ R_m
- ☐ R_S

Q1.7 (1 point) After Step 4 of the TLS handshake is complete, what can Mallory do? Select all that apply.

- ☐ Pretend to be the Server and send the message in Step 5 to the Client.
- ☐ Pretend to be the Client and send the message in Step 7 to the Server.
- ◯ None of the above

For Q1.8 and Q1.9, consider the standard TLS handshake from lecture (these subparts are **independent** from the modified scheme above).

Q1.8 (1 point) The Client and Server complete a standard TLS handshake. If an attacker compromises all routers between the Client and the Server, can they decrypt messages?

- ◯ Yes, because the compromised routers can inspect and forward packets.
- ◯ Yes, because the attacker can inject traffic to downgrade encryption and then decrypt.
- ◯ No, because TLS is end-to-end secure.
- ◯ No, because the underlying TCP session provides confidentiality.

This content is protected and may not be shared, uploaded, or distributed.

Q1.9 (1 point) Suppose the Client and Server change the length of the random nonce from 256 to 128 bits in the TLS handshake.

With this modification, what happens to the probability that a packet recorded from one connection can be replayed in another connection?

- ◯ The probability increases, and the resulting probability of success is non-negligible.
- ◯ The probability increases, and the resulting probability of success is negligible.
- ◯ The probability decreases, and the resulting probability of success is non-negligible.
- ◯ The probability decreases, and the resulting probability of success is negligible.

This content is protected and may not be shared, uploaded, or distributed.

Q2 *Network Security: Caffè Strada* ☕ **(11 points)**

Consider a local area network (LAN) at a coffee shop.

- Alice is a legitimate user trying to connect to the internet and communicate with Bob.
- Mallory is a malicious attacker on the same LAN.
- The network uses standard ARP for address resolution and DHCP for configuration.

Q2.1 (1 point) Mallory is on the same local network as Alice. She wants to intercept Alice's traffic destined for the Internet by providing false information about the Gateway Router.

If Mallory uses **ARP spoofing**, what information must she substitute in her malicious replies?

◯ Substitute the IP address normally provided by the gateway with Mallory's IP address

◯ Substitute the MAC address normally provided by the gateway with Mallory's MAC address

Q2.2 (1 point) Mallory is on the same local network as Alice. She wants to intercept Alice's traffic destined for the Internet by providing false information about the Gateway Router.

If Mallory uses **DHCP spoofing**, what information must she substitute in her malicious replies?

◯ Substitute the IP address normally provided by the gateway with Mallory's IP address

◯ Substitute the MAC address normally provided by the gateway with Mallory's MAC address

Q2.3 (2 points) Alice restarts her computer and rejoins the network. She broadcasts a `Client Discover` message to get a network configuration via DHCP.

Mallory sends a malicious `DHCP Offer` to Alice. Which fields in this offer would Mallory alter to position herself as a Man-in-the-Middle? Select all that apply.

☐ Gateway Router IP

☐ Alice's public key

◯ None of the above

☐ Alice's IP Address

☐ WiFi WPA2 pre-shared key

Q2.4 (1 point) The coffee shop owner wants to improve security. Which of the following defenses would effectively mitigate these vulnerabilities? Select all that apply.

☐ Implementing WPA2-PSK will prevent Mallory from spoofing ARP packets even if she knows the WiFi password.

☐ DHCP attacks are trivial to fix by having the router sign all DHCP offers with a hardcoded certificate.

This content is protected and may not be shared, uploaded, or distributed.

EvanBot and CodaBot are working on a project at a coffee shop. Mallory is connected to the same local network (LAN) and wants to intercept their traffic.

Mallory is an on-path attacker who can guarantee that her packets arrive before any legitimate packets, 100% of the time.

Q2.5 (2 points) EvanBot connects to the network for the first time and broadcasts a DHCP `Client Discover` message.

To trick EvanBot into accepting her configuration, how many packets is Mallory required to send that contain a falsified Source IP or Source MAC address (i.e., pretending to be the legitimate server in Source IP address or Source MAC address of the packet header)?

- ◯ 0
- ◯ 1
- ◯ 2
- ◯ More than 2

Q2.6 (2 points) CodaBot is already connected to the network. He wants to send a packet to the real Gateway Router (IP `10.1.6.1`), but his ARP cache is empty.

CodaBot broadcasts: "Who has IP `10.1.6.1`?".

How many packets does Mallory need to send to poison CodaBot's ARP cache and force him to send his traffic to her instead of the real router?

- ◯ 0
- ◯ 1
- ◯ 2
- ◯ More than 2

Q2.7 (2 points) What kind of attackers can execute a DHCP spoofing attack? Select all that apply.

- ☐ Man-in-the-middle
- ☐ On-path
- ☐ Off-path
- ◯ None of the above

This content is protected and may not be shared, uploaded, or distributed.