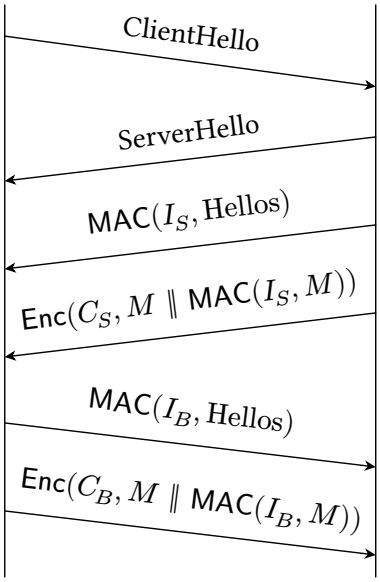
CS161 Fall 2026 — Introduction to Computer Security — Exam Prep 6

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

> **Solution:** True.
>
> Diffie-Hellman ensures that we have forward secrecy. The ephemeral values are never reused and never sent across the channel so even when the attacker is able to compromise the current channel (know all the secret values), the attacker can't derive the necessary keys of a previous session.

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

○ True ● False

> **Solution:** False.
>
> We are no longer sending a certificate, thus losing authenticity in this scheme. Mallory could simply race the server's messages as shown in the next few subparts.

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.

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

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

Solution: Matching the form of the Client/Server Hellos, Mallory will want to send their own ephemeral DH key and their own chosen random nonce.

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

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

Solution: Client will recieve Mallory's message instead of the server's. So the Client will derive Premaster Secret $PS = g^{am} \bmod p$ from $g^m \bmod p$ and the client's own ephemeral value a. The random nonces that the Client will know is R_a and R_m.

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

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

Solution: Server will recieve Client's message as normal since Mallory can't race this message. The Server will derive Premaster Secret $PS = g^{as} \bmod p$ from $g^a \bmod p$ and the server's own ephemeral value s. The random nonces that the Client will know is R_a and R_s.

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

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

Solution: Mallory can eavesdrop on both the Client/Server Hellos. But since Mallory wants to share a key with the Client, Mallory will raced the server's message to force the Client into deriving symmetric keys of Mallory's choosing.

Mallory will use the same nonce as the Client: R_a and R_m. To derive the same Premaster Secret $PS = g^{am} \bmod p$, Mallory will use $g^a \bmod p$ and their own ephemeral value 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

Solution: Since Mallory couldn't race the first ClientHello, Mallory won't be a true MITM. She can only share the same set of symmetric keys with the Client and not the Server. So Mallory must and can only successfully race messages from Server to Client.

Also notice how no matter if Mallory spoofs the message in step 7 or not, the connection would fail at Step 6 since the server will not be able to verify the MAC correctly due to the different symmetric keys that the Client ended up deriving.

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.

Solution: After the handshake, the message security relies on TLS, which is secure, as attacker does not know the keys being used to encrypt.

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.

Solution: The probability of a collision is $\frac{1}{2^{128}}$, which is larger than $\frac{1}{2^{256}}$ but is still 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

Solution: The router/gateway is the system that relays the user's traffic to the Internet. ARP resolves IP addresses to MAC addresses. To spoof the gateway via ARP, Mallory claims that the Gateway's IP maps to **her** 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

Solution: The router/gateway is the system that relays the user's traffic to the Internet. DHCP provides network configuration, including the IP of the default gateway. To spoof the gateway via DHCP, Mallory sends a configuration claiming that the gateway is at **her** IP 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

Solution: By spoofing the Gateway Router, Mallory ensures that when Alice sends messages to the internet, she sends them to Mallory first.

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

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.

Solution: DHCP spoofing is hard to fix because when a user first connects, they don't know who to trust (no root of trust), so they generally have to accept the first valid-looking offer. Signing doesn't help because the user doesn't know what public key to use to verify signatures. WPA2-PSK doesn't help either, because if Mallory knows the Wifi password, Mallory can compute the cryptographic keys needed to eavesdrop on all Wifi packets and send spoofed Wifi packets.

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

Solution: 0 packets with falsified Source IP/MAC address.

Because DHCP clients typically accept the first valid offer they receive, regardless who it is from, and Mallory is guaranteed to be faster, she does not need to forge the packet headers to look like the legitimate server. She can simply reply as herself (a rogue server) with her own IP/MAC address, and EvanBot will accept the offer because it arrived first.

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

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

Solution: 1 packet.

Mallory only needs to send one malicious ARP response: "My IP is `10.1.6.1` and my MAC address is `[Mallory's MAC address]`". Because of the race condition vulnerability in ARP, CodaBot will accept this single response if it arrives before the real router's response.

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

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

Solution: To successfully spoof a DHCP response, the attacker must be able to see the client's `DHCP Discover` or `Request` broadcast to know when to respond (and often to learn transaction IDs, so they can include the transaction ID in their response).

- On-path attackers can see packets and inject spoofed packets, so they can perform this attack.
- Man-in-the-middle attackers can see, modify, and drop packets, so they can also perform this attack (and are often the result of it).
- Off-path attackers are defined as unable to see packets, so they cannot execute this attack because they cannot see the initial request. Also, DHCP packets are not forwarded outside the local area network, so an off-path attacker (on a different LAN) cannot get a malicious DHCP packet to the victim.

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