Q1 *I (T)C(P) You (su20-final-q7)* **(26 points)**

EvanBot builds a new course feature that sends announcements to students over TCP. To receive announcements, a student initiates a TCP connection with the server. The server sends the announcements and terminates the connection.

Q1.1 (3 points) Assuming that no adversaries are present, which of the following does communication over a TCP connection guarantee? Select all that apply.

- ☐ (A) That both the server and client can detect if a particular announcement needs to be resent
- ☐ (B) That different announcements are delivered in the same order they were sent in
- ☐ (C) That announcements are delivered using the most efficient path through the internet
- ☐ (D) None of the above
- ☐ (E) ——
- ☐ (F) ——

Q1.2 (3 points) When only an on-path adversary is present, which of the following does communication over a TCP connection guarantee? Select all that apply.

- ☐ (G) That both the server and client can detect if a particular announcement needs to be resent
- ☐ (H) That different announcements are delivered in the same order they were sent in
- ☐ (I) That announcements are delivered using the most efficient path through the internet
- ☐ (J) None of the above
- ☐ (K) ——
- ☐ (L) ——

Q1.3 (3 points) Suppose that EvanBot instead sends announcements over UDP. Assuming that no adversaries are present, which of the following might happen? Select all that apply.

☐ (A) Students might not receive some announcements

☐ (B) Students might receive the announcements more quickly

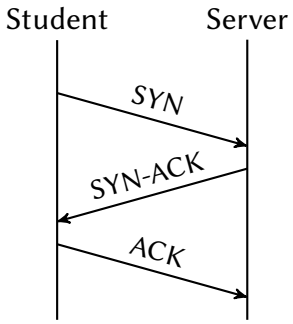
☐ (C) The server might not detect some errors which it would have had it been using TCP

☐ (D) None of the above

☐ (E) ——

☐ (F) ——

EvanBot realizes that the server is sending messages to the student, but the student only responds with ACKs and never sends any messages after the initial handshake. They design a *Half TCP* protocol which provides TCP's properties for communications from the server to the student, but not for communications from the student to the server. This is accomplished using a modified version of the standard three step handshake pictured below.



Q1.4 (5 points) Some sequence numbers are no longer necessary in *Half TCP*. Which fields **do not** need to be transmitted? Select all that apply.

☐ (G) The sequence number in the SYN packet

☐ (H) The sequence number in the SYN-ACK packet

☐ (I) The ACK number in the SYN-ACK packet

☐ (J) The sequence number in the ACK packet

☐ (K) The ACK number in the ACK packet

☐ (L) None of the above

Q1.5 (3 points) Which of these are consequences of moving from TCP to *Half TCP* for this application? Select all that apply.

☐ (A) The student will no longer receive announcements in the correct order

☐ (B) The server will not have to keep track of as much state

☐ (C) The student will not have to keep track of as much state

☐ (D) None of the above

☐ (E) ——

☐ (F) ——

The 161 staff likes security and decides to use TLS over *Half TCP*. Assume that the staff server has a valid certificate for their public key.

For each different adversary below, select all attacks which become ***easier*** when running TLS over *Half TCP* compared to normal TCP.

Q1.6 (3 points) Off-path adversary

☐ (G) RST Injection Attack

☐ (H) Interfere with a TLS handshake to learn the master key

☐ (I) Replay an encrypted command from a previous TLS connection

☐ (J) None of the above

☐ (K) ——

☐ (L) ——

Q1.7 (3 points) On-path adversary

☐ (A) RST Injection Attack

☐ (B) Interfere with a TLS handshake to learn the master key

☐ (C) Replay an encrypted command from a previous TLS connection

☐ (D) None of the above

☐ (E) ——

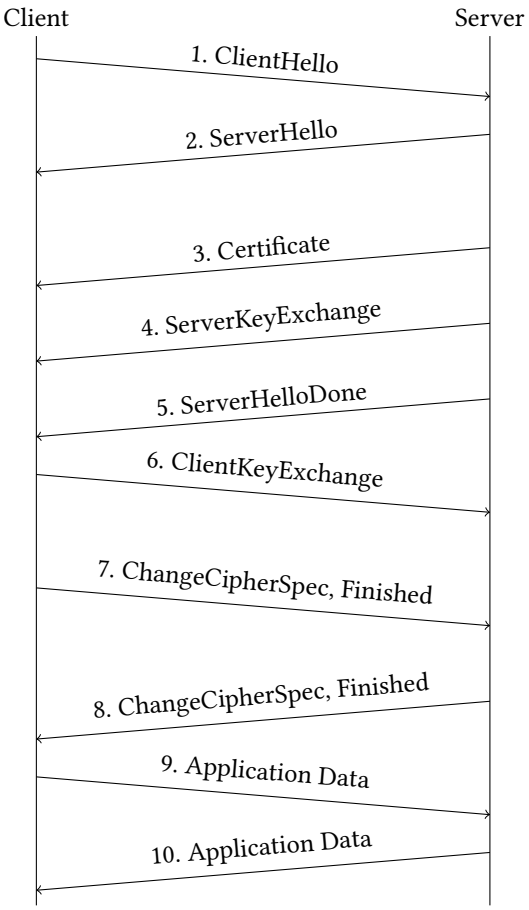
☐ (F) ——

Q1.8 (3 points) Man-in-the-middle adversary

- ☐ (G) RST Injection Attack
- ☐ (H) Interfere with a TLS handshake to learn the master key
- ☐ (I) Replay an encrypted command from a previous TLS connection
- ☐ (J) None of the above
- ☐ (K) ——
- ☐ (L) ——

Q2 *Mutuality (SP21 Final Q9)* **(18 points)**

Recall the TLS handshake:



1. Client sends 256-bit random number R_b and supported ciphers

2. Server sends 256-bit random number R_s and chosen cipher

3. Server sends certificate

4. DH: Server sends $\{g, p, g^a \bmod p\}_{K_{\text{server}}^{-1}}$

5. Server signals end of handshake

6. DH: Client sends $g^b \bmod p$
   RSA: Client sends $\{PS\}_{K_{\text{server}}}$
   Client and server derive cipher keys C_b, C_s and integrity keys I_b, I_s from R_b, R_s, PS

7. Client sends MAC(dialog, I_b)

8. Server sends MAC(dialog, I_s)

9. Client data takes the form $\{M_1, \text{MAC}(M_1, I_b)\}_{C_b}$

10. Server data takes the form $\{M_2, \text{MAC}(M_2, I_s)\}_{C_s}$

In TLS, we verify the identity of the server, but not the client. How would we modify TLS to also verify the identity of the client?

Clarification during exam: All parts of this question refer to a modified TLS scheme designed to verify the identity of the client.

Q2.1 (3 points) Which of these additional values should the client send to the server?

- ◯ (A) A certificate with the client's public key, signed by the client's private key
- ◯ (B) A certificate with the client's public key, signed by the server's private key
- ◯ (C) A certificate with the client's private key, signed by a certificate authority's private key
- ◯ (D) A certificate with the client's public key, signed by a certificate authority's private key
- ◯ (E) —
- ◯ (F) —

Q2.2 (3 points) How should the client send the premaster secret in RSA TLS?

◯ (G) Encrypted with the server's public key, signed by the client's private key

◯ (H) Encrypted with the client's public key, signed by the server's private key

◯ (I) Encrypted with the server's public key, signed by a certificate authority's private key

◯ (J) Encrypted with the client's public key, signed by a certificate authority's private key

◯ (K) ——

◯ (L) ——

Q2.3 (3 points) EvanBot argues that the key exchange protocol in Diffie-Hellman TLS doesn't need to be changed to support client validation. Is EvanBot right?

◯ (A) Yes, because only the client knows the secret a, so the server can be sure it's talking to the legitimate client

◯ (B) Yes, because the server has already received and verified the client's certificate

◯ (C) No, the client must additionally sign their part of the Diffie-Hellman exchange with the client's private key

◯ (D) No, the client must additionally sign their part of the Diffie-Hellman exchange with the certificate authority's private key

◯ (E) ——

◯ (F) ——

Q2.4 (2 points) True or False: The server can be sure that they're talking to the client (and not an attacker impersonating the client) immediately after the client and server exchange certificates.

◯ (G) True ◯ (H) False ◯ (I) —— ◯ (J) —— ◯ (K) —— ◯ (L) ——

Q2.5 (3 points) At what step in the TLS handshake can both the client and server be sure that they have derived the same symmetric keys?

◯ (A) Immediately after the TCP handshake, before the TLS handshake starts

◯ (B) Immediately after the ClientHello and ServerHello are sent

◯ (C) Immediately after the client and server exchange certificates

◯ (D) Immediately after the client and server verify signatures

◯ (E) Immediately after the MACs are exchanged and verified

◯ (F) ——

Q2.6 (4 points) Which of these keys, if stolen individually, would allow the attacker to impersonate the client? Select all that apply.

- ☐ (G) Private key of a certificate authority
- ☐ (H) Private key of the client
- ☐ (I) Private key of the server
- ☐ (J) Public key of a certificate authority
- ☐ (K) None of the above
- ☐ (L) ——

Q3 *Networking: TLS Times Two* **(14 points)**

A client and server form a secure connection with Diffie-Hellman TLS. The client uses Diffie-Hellman secret c_1, and the server uses secret s_1. After the first connection ends, Mallory, a MITM attacker, compromises s_1.

Next, the same client and server form a second connection with Diffie-Hellman TLS. For this connection, the client uses Diffie-Hellman secret c_2, and the server uses secret s_2.

Mallory wants to impersonate the server in the second connection (i.e. Mallory wants to be able to send her own messages to the client in the second connection).
Clarification during exam: Assume that Mallory recorded all communication from the first TLS connection.

Q3.1 (3 points) During the second handshake, the server sends $g^{s_2} \bmod p$ to the client, along with a signature on this value.

Mallory intercepts this message and replaces it, sending the replaced message to the client. What should the replaced message be?

Your answer can contain any values that Mallory knows.

Q3.2 (3 points) What is the shared premaster secret that the client derives?

Q3.3 (3 points) After executing this attack, what can Mallory do in the second TLS connection? Select all that apply.

- ☐ Read messages sent by the client
- ☐ Send messages to the server
- ☐ Read messages sent by the server
- ☐ None of the above

Q3.4 (5 points) Suppose the server acts as a certificate authority for EvanBot. (In other words, the server can use their secret key to sign EvanBot's public keys.)

The client wants to form a TLS connection with EvanBot. Can Mallory use this attack to cause EvanBot to derive a shared secret that Mallory knows?

- ○ Yes
- ○ No

Briefly justify your answer.