CS161 Fall 2025 — Introduction to Computer Security — Exam Prep 10

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.

- ☐ That both the server and the client can detect if a particular announcement needs to be resent
- ☐ That different announcements are delivered in the same order they were sent in
- ☐ That announcements are delivered using the most efficient path through the internet
- ○ None of the above

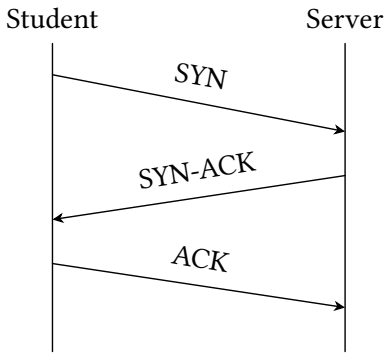
Q1.2 (3 points) When only an on-path adversary is present, which of the following does communication over a TCP connection guarantee? Select all that apply.

- ☐ That both the server and the client can detect if a particular announcement needs to be resent
- ☐ That different announcements are delivered in the same order they were sent in
- ☐ That announcements are delivered using the most efficient path through the internet
- ○ None of the above

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.

- ☐ That both the server and the client can detect if a particular announcement needs to be resent
- ☐ That different announcements are delivered in the same order they were sent in
- ☐ That announcements are delivered using the most efficient path through the internet
- ○ None of the above

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.

- ☐ The sequence number in the SYN packet
- ☐ The sequence number in the SYN-ACK packet
- ☐ The ACK number in the SYN-ACK packet
- ☐ The sequence number in the ACK packet
- ☐ The ACK number in the ACK packet
- ○ 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.

- ☐ The student will no longer receive announcements in the correct order.
- ☐ The server will not have to keep track of as much state
- ☐ The student will not have to keep track of as much state
- ○ None of the above

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

- ☐ RST Injection Attack
- ☐ Interfere with a TLS handshake to learn the master key
- ☐ Replay an encrypted command from a previous TLS connection
- ◯ None of the above

Q1.7 (3 points) On-path adversary

- ☐ RST Injection Attack
- ☐ Interfere with a TLS handshake to learn the master key
- ☐ Replay an encrypted command from a previous TLS connection
- ◯ None of the above

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

- ☐ RST Injection Attack
- ☐ Interfere with a TLS handshake to learn the master key
- ☐ Replay an encrypted command from a previous TLS connection
- ◯ None of the above

Q2 *Mutuality (SP21 Final Q9)* **(0 points)**

(Question 2 continued…)