CS161 Summer 2026 — Introduction to Computer Security — Discussion 9

Q1 *Tor* **(3 points)**

Alice uses a Tor circuit of three relays (Relay 1, Relay 2, Relay 3) to send a message to Bob. She has established shared keys K1, K2, and K3 with the relays respectively. The last relay in the chain (Relay 3) is the exit node.

Q1.1 (1 point) In what order does Alice encrypt her message, and what exactly does Relay 1 learn after it decrypts the outermost layer?

Q1.2 (1 point) The exit node acts as a MITM. What can it see or tamper with, and how can Alice protect the contents of her message from it?

Q1.3 (1 point) True or False: If exactly one of the three relays is honest, Alice's anonymity is still preserved.

○ True ○ False

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

Q2 *Denial-of-Serivce* **(3 points)**

Mallory wants to make a popular web server unavailable to its legitimate users. She controls a single machine, but can also rent a botnet of thousands of compromised hosts.

Q2.1 (1 point) Mallory first floods the server with garbage packets from her own IP address. Why is this easy to defend against, and how do IP spoofing and a DDoS each improve the attack?

Q2.2 (1 point) Explain the asymmetry that makes a SYN flood effective, and how SYN cookies remove that asymmetry.

Q2.3 (1 point) In an amplified DoS attack, why do attackers prefer amplification servers that use UDP rather than TCP?

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