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?

Solution: Alice encrypts innermost with K3, then K2, then the outermost layer with K1 (so the packet is peeled K1 -> K2 -> K3).

Relay 1 decrypts with K1 and learns only: (1) the message is from Alice, and (2) it should forward to Relay 2 next. Everything beyond is encrypted with K2, so Relay 1 learns nothing about Bob or the message contents.

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?

Solution: The exit node sees the final message and the recipient (Bob), but not the original sender (Alice).

If Alice uses plain HTTP, the exit node can read and modify the traffic. If she uses HTTPS (TLS end-to-end with Bob), the exit node cannot read or tamper with the payload, it only relays the encrypted bytes.

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

● True ○ False

Solution: True.

As long as at least one node is honest, the full circuit cannot collude to link Alice and Bob; if that honest node is the entry or exit, it also mitigates timing attacks.

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?

Solution: The victim can install a packet filter that drops all packets with "From: Mallory," stopping the flood.

IP spoofing forges the source field so it keeps changing but networks can still filter traffic whose source addresses look suspicious/ever-changing.

A DDoS sends genuine traffic from many botnet hosts: no spoofing is needed, it provides huge bandwidth, and attack traffic is hard to distinguish from legitimate traffic.

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

Solution: In the TCP handshake the server allocates state (memory) right after receiving a SYN, while Mallory sends SYNs cheaply and ignores the SYN-ACKs so small effort forces large resource use.

With SYN cookies the server stores no state on a SYN. It encodes the needed state (cryptographically) into the initial sequence number sent in the SYN-ACK, and only allocates state once the client echoes it back in the ACK. A spoofing attacker never sees the SYN-ACK, so it cannot complete the handshake.

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

Solution: Amplification requires spoofing the victim's address on a small request so the large response is sent to the victim.

With TCP, an off-path attacker must guess the sequence numbers in the handshake to spoof a connection, which is hard. UDP has no handshake or sequence numbers, so spoofing the source is easy.