CS161 Fall 2025 — Introduction to Computer Security — Exam Prep 13

Q1 *Networking: A TORrible Mistake* **(7 points)**

Q1.1 (1 point) An $n > 1$-node Tor circuit provides anonymity (i.e. no node learns who both the user and server are) when at least _____ node(s) are honest. Assume that malicious nodes can collude, but they do not correlate traffic. Fill in the blank.

◯ 0 ◯ 1 ◯ n-1 ◯ n

For the next 3 subparts, a user is using Tor to send a message to a server. Assume that there is no collusion between any Tor nodes, and that the user choses exactly 3 nodes for their Tor circuit.

Q1.2 (1 point) Which values can a malicious **entry** node learn? Select all that apply.

☐ The IP address of the user ☐ The list of all nodes in the circuit

☐ The IP address of the server ☐ None of the above

Q1.3 (1 point) Which values can a malicious **exit** node learn? Select all that apply.

☐ The IP address of the user ☐ The list of all nodes in the circuit

☐ The IP address of the server ☐ None of the above

Q1.4 (1 point) Which values can an on-path attacker on the user's local network learn? Select all that apply.

☐ The IP address of the user ☐ The list of all nodes in the circuit

☐ The IP address of the server ☐ None of the above

When a new user first downloads Tor, they need to download a list of nodes from a trusted directory server.

A malicious, on-path attacker on the user's local network wishes to eavesdrop on the new user's Tor connection. Assume that the attacker controls 3 nodes out of 100 total Tor nodes, and can win any data race.

For the next three subparts, select the approximate probability that the attacker can learn the identity of the server.

Q1.5 (1 point) User connects to the directory via TLS, attacker is on-path.

◯ Exactly 0% ◯ Greater than 50%, less than 100%

◯ Greater than 0%, less than 50% ◯ Exactly 100%

Q1.6 (1 point) User connects to the directory via TCP, attacker is on-path.

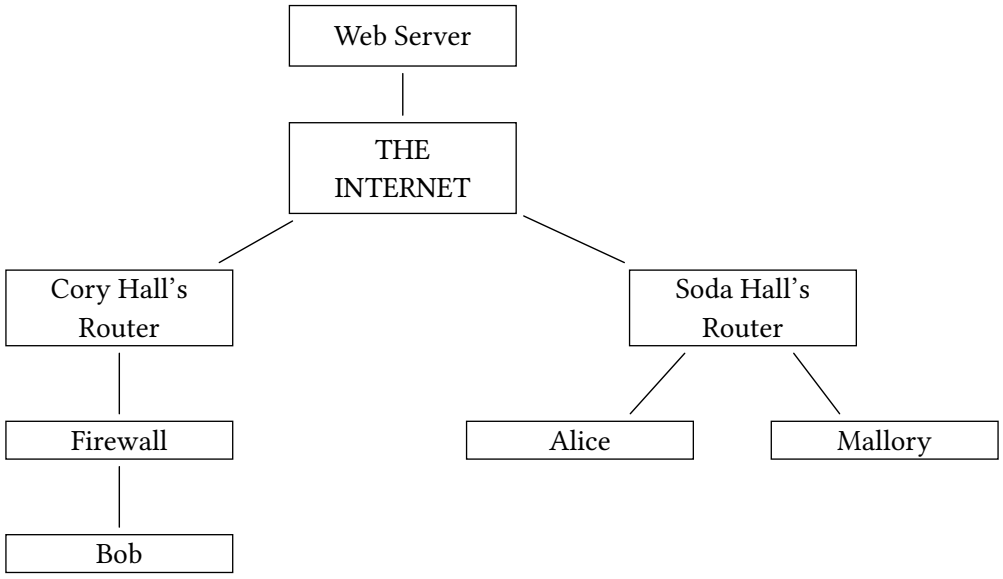
- ◯ Exactly 0%
- ◯ Greater than 0%, less than 50%
- ◯ Greater than 50%, less than 100%
- ◯ Exactly 100%

Q1.7 (1 point) User connects to the directory via TCP, attacker is off-path.

- ◯ Exactly 0%
- ◯ Greater than 0%, less than 50%
- ◯ Greater than 50%, less than 100%
- ◯ Exactly 100%

Q2 *Making New Friends* **(9 points)**

Consider two local broadcast networks, as shown in the diagram below.



Q2.1 (2 points) Alice broadcasts an ARP request for Mallory's MAC address.

Which of these entities, if malicious, can poison Alice's ARP cache? Select all that apply.

- ☐ Mallory
- ☐ Bob
- ☐ None of the above
- ☐ Soda Hall's router
- ☐ Cory Hall's router

Q2.2 (4 points) Mallory and Bob form a TLS connection. Then, Bob adds a rule to the firewall disallowing all inbound packets from Mallory.

EvanBot argues that TLS messages are encrypted, so the firewall cannot stop Mallory from sending more TLS messages to Bob. Is EvanBot correct? Justify your answer in 10 words or fewer.

- ◯ Yes
- ◯ No

Q2.3 (3 points) Bob adds a rule to the firewall disallowing all inbound packets from anybody in Soda Hall's local network.

Which of the following attacks can Mallory still perform on Bob? Assume that Mallory cannot spoof packets. Select all that apply.

- ☐ DoS
- ☐ TLS Hijacking
- ☐ XSS
- ☐ None of the above