Nick Weaver
Fall 2018

CS 161
Computer Security

Discussion 8

Week of October 15, 2018

Question 1 ***DHCP*** **(5 min)**

Nick gets home after a tiring day of lecturing CS 161. He opens up his laptop and goes on Twitter. From a networking and web perspective, what are the steps involved in loading the Twitter homepage?

Nick's computer needs to connect to the wifi. What messages are exchanged in the 4 part handshake in order to achieve this?

Nick's computer sends: _____.

This message is *broadcasted / unicasted*. Choose one and explain:

A DHCP server replies with a DHCP Offer. What does this message contain? What can a malicious attacker do at this step? Keep in mind that an attacker on the same subnet can hear the discovery message.

Nick's computer sends: _____.

This message is *broadcasted / unicasted*. Choose one and explain:

The server then responds with: _____.

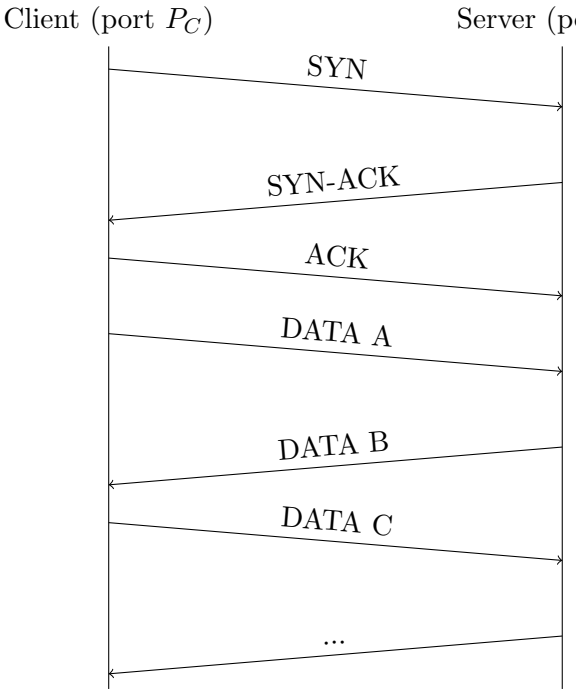
Question 2 ***Back to L4 Basics*** **(10 min)**

The transmission control protocol (TCP) and user datagram protocol (UDP) are two of the primary protocols of the Internet protocol suite.

(a) How do TCP and UDP relate to IP (Internet protocol)? Which of these protocols are encapsulated within (or layered atop) one another? Could all three be used simultaneously?

(b) What are the differences between TCP and UDP? Which is considered "best effort"? What does that mean?

(c) Which is easier to spoof, and why?



1. Client sends initial SYN with sequence number A (usually random).
2. Server sends SYN-ACK with sequence number B (also usually random) and ACK $A + 1$.

3. Client sends ACK with sequence number $A + 1$ and ACK $B + 1$.
4. Client sends DATA A of length L_A with sequence number $A + 1$ and ACK $B + 1$.
5. Server sends DATA B of length L_B with sequence number $B + 1$ and ACK $A + 1 + L_A$.

6. Client sends DATA C of length L_C with sequence number $A + 1 + L_A$ and ACK $B + 1 + L_B$.
7. Data exchange continues until both sides are done sending data.

Figure 1: TCP handshake and initial data transfer

Question 3 ***Attack On TCP*** **(35 min)**

(a) Assume that the next transmission in this connection will be DATA D from the server to the client. What will this packet look like?

Sequence number:	_____	ACK:	_____
Source port:	_____	Destination port:	_____
Length:	L_D	Flags:	None

(b) You should be familiar with the concept and capabilities of a *man-in-the-middle* as an attacker who **CAN observe** and **CAN intercept** traffic. There are two other types of relevant attackers in this scenario:

1. *On-path* attacker: **CAN observe** traffic but **CANNOT intercept** it.
2. *Off-path* attacker: **CANNOT observe** traffic and **CANNOT intercept** it.

Carol is an *on-path* attacker. Can Carol do anything malicious to the connection? If so, what can she do?

(c) David is an *off-path* attacker. Can David do anything malicious to the connection? If so, what can he do?

(d) The client starts getting responses from the server that don't make any sense. Inferring that David is attempting to hijack the connection, the client then immediately sends the server a **RST** packet, which terminates the ongoing connection. Is the client now safe?