Popa & Weaver	CS 161	
Spring 2019	Computer Security	Discussion 6

# Network Security I

### Question 1 Back to L4 Basics

## (15 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?

#### Question 2 Attack On TCP

#### (35 min)

Suppose that a client connects to a server, and then performs the following TCP hand-shake and initial data transfer:

Client (port $P_C$ )	Server (port $P_S$ )
SYN	1. Client sends initial SYN with sequence number $A$ (usually random).
SYN-ACK	2. Server sends SYN-ACK with sequence number $B$ (also usually random) and ACK $A + 1$ .
ACK	3. Client sends ACK with sequence number $A + 1$ and
DATA A	ACK $B + 1$ . 4. Client sends DATA A of length $L_A$ with sequence num-
DATA B	ber $A + 1$ and ACK $B + 1$ . 5. Server sends DATA B of length $L_B$ with sequence number $B + 1$ and ACK $A + 1 + L_A$ .
DATA C	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 send- ing data.

(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. Can David successfully impersonate the client and establish a new connection with the server?

Assume that the server trusts the client's IP address as an identifier of the client.