Jawale & Dutra
Summer 2019

CS 161 Computer Security

Discussion 7

Question 1 ***DNS Walkthrough*** **(15 min)**

Your computer sends a DNS request for "www.google.com"

(a) Assume the DNS resolver receives back the following reply:

```
com. NS a.gtld-servers.net
a.gtld-servers.net A 192.5.6.30
```

Describe what this reply means and where the DNS resolver would look next.

(b) If an off-path adversary wants to poison the DNS cache, what values does the adversary need to guess?

(c) What are some issues with using TLS to secure DNS?

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.

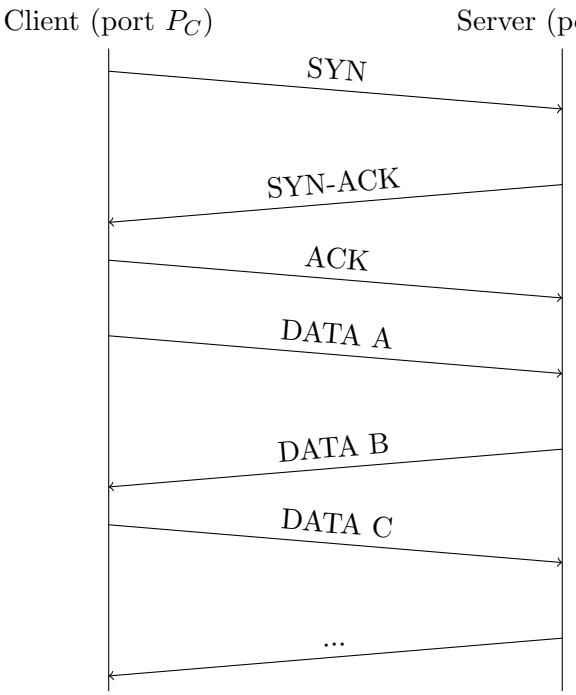
(a) How do TCP and UDP relate to IP (Internet protocol)? Which of these protocols are encapsulated within (or layered atop) one another? Could all three be used simultaneously?

(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?

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

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



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.

(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.