Weaver
Fall 2019

CS 161
Computer Security

Discussion 8

Network Security I

Question 1 ***Web Security Wrap-Up: UI-Based Attacks and Privacy***

(a) **Phishing**

A phishing attacker tries to gain sensitive user information by tricking users into going to a fake version of a website they trust. The attacker might convince the user to go to what *appears* to be their bank and to enter their username and password.

i. What are some ways that attackers try to fool users about the site they are going to? How do they convince people to click on links to sites?

ii. What are some defenses you should employ against phishing?

(b) **Clickjacking**

Smartphone users are used to notifications popping up over their browsers as texts and calls arrive. How can attackers use this to their advantage?

(c) **Web Tracking**

What kind of information do sites gain about you when you visit them? How could a business learn about many of the sites you visit and construct a detailed profile of you based on your web habits?

Question 2 *Introduction to Networking*

(a) **Protocol Layers** At which network layer does each of the following operate (physical, link, network, transport, or application)?

- Ethernet
- SMTP (email)
- SYN packet
- UDP
- Fiber optics
- FTP
- DNS request
- BitTorrent
- IP address
- 127.0.0.1
- 802.11n WiFi

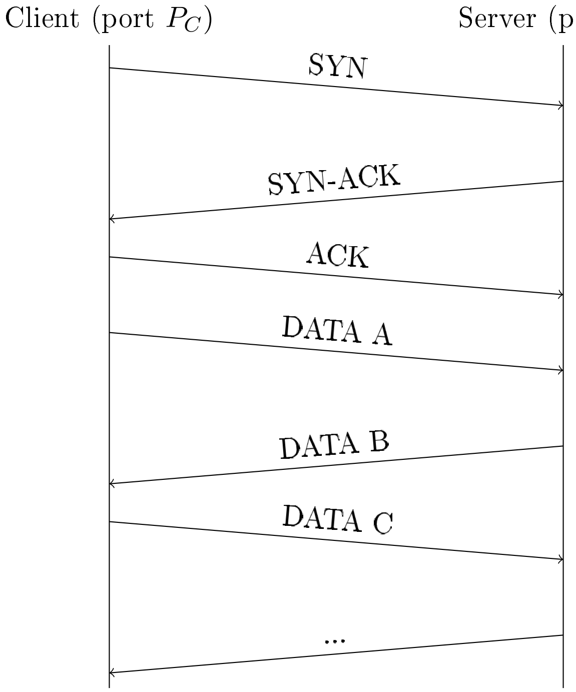
(b) **TCP and UDP** The transmission control protocol (TCP) and user datagram protocol (UDP) are two of the primary protocols of the Internet protocol suite.

i. 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?

ii. What are the differences between TCP and UDP? Which is considered "best effort"? What does that mean?

Question 3 *Attack on TCP*

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: ACK

(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?

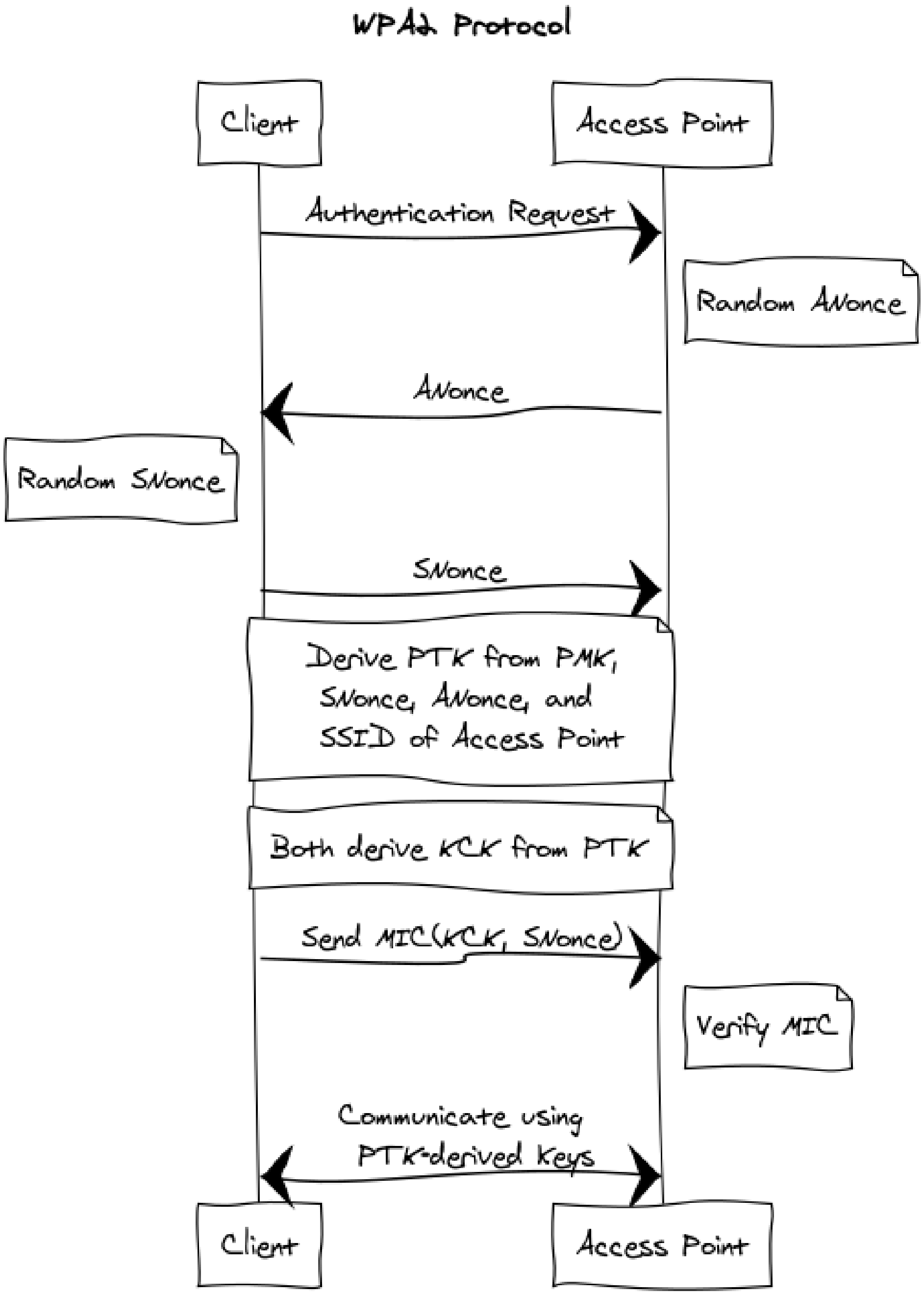
(d) The client starts getting responses from the server that don't make any sense. Inferring that David is attempting to hijack the connection, the client then immediately sends the server a **RST** packet, which terminates the ongoing connection. Can David successfully impersonate the client and establish a new connection with the server?

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

Question 4 *WPA2*

Let's review WPA2. You might find some of the definitions below helpful.

- PMK is the *premaster key*, also known as "the WiFi password".
- PTK is the *pairwise transient key*, which is used to derive symmetric keys.
- KCK is the *key confirmation key*, which helps the client and the access point confirm they've agreed on the same keys.



(a) Louis Reasoner proposes that we don't generate ANonce or SNonce, and instead derive the PTK directly from the SSID and PMK. What sort of attack does this fail to prevent?

(b) Alyssa P. Hacker wants to compromise a WPA2 WiFi network. In order to do so, she performs the handshake many times. She bruteforces possible PMK against the Access Point many times, until the access point eventually accepts it. If the password has 28 bits of entropy[1] and the attacker can make 10 guesses a second, how long will it take to bruteforce the password?

(c) Ben Bitdiddle has an alternate idea. Ben waits until Louis attempts to connect to the network. While this happens, he records all of the messages that Louis sends over the network. How can Ben use this to bruteforce possible PMKs? Why do we expect this to be faster than Alyssa's method?

[1] As per this XKCD comic, a password which looks like `Tr0ub4dor&3` has roughly 28 bits of entropy.