Q1 *Hackerman Visits the Voting Booth* **(21 points)**

Your sketchy friend Jared asks you to use your CS 161 skills to help him rig some sort of election. He hands you a business card with credentials for a Russian supercomputer.

Armed with massive computing power, you show up to the Caltopia polling center. It has a Wi-Fi network secured with standard WPA2-PSK.

Q1.1 (5 points) You observe a WPA 4-way handshake. Which values from the handshake are needed to perform a brute-force search for the Wi-Fi password? Select all that apply.

- ■ (A) ANonce
- ■ (B) SNonce
- ■ (C) The router's MAC address
- ■ (D) The client's MAC address
- ■ (E) The MICs
- □ (F) None of the above

Solution: In the WPA2 4-way handshake, the information dependency goes {SSID, password} → PSK + {ANonce, SNonce, Router MAC, Client MAC} → PTK → MIC, which is public and unencrypted. Given all of these except for the password, we can upload the information to our powerful computer and brute force to our heart's content.

Q1.2 (4 points) What can you do after successfully brute-forcing the Wi-Fi password? Select all that apply.

■ (G) Perform on-path network attacks against victims in the same Wi-Fi network

■ (H) Decrypt network traffic encrypted with the PTK of a user who joins the network after you

■ (I) Decrypt network traffic encrypted with the GTK

☐ (J) Decrypt TLS network traffic

☐ (K) None of the above

☐ (L) ——

Solution: Need to word these choices carefully, other attacks could be used once you're on-path to do things like MITM attacks. I think these are unambiguous now though

You are on the local network, so any on-path attack is fair game.

Additionally, the unencrypted information sent during the 4-way handshake combined with the network's password allow you to compute a user's PTK and the group GTK, which lets you decrypt any traffic encrypted with WPA2 keys.

TLS is end-to-end secure, so being an on-path attacker in the local network won't help you decrypt TLS traffic.

Q1.3 (3 points) Which defenses would stop your attack? Select all that apply.

☐ (A) Changing the Wi-Fi password every day

■ (B) Using WPA2-Enterprise

☐ (C) A modern NIDS system

☐ (D) None of the above

☐ (E) ——

☐ (F) ——

Solution: Changing the password each day is a poor solution to a low-entropy password.

A NIDS system operates on higher layers than required to detect or stop these attacks.

A high-entropy password resists brute-forcing, and without network access, the other attacks aren't possible.

Enterprise WPA2 doesn't let any user without credentials obtain keys, and each user has their own key.

You arrive at the New Blackwell City polling center. It also has a Wi-Fi network secured with standard WPA2-PSK.

You walk up to a poll worker, claim that you're a fellow poll worker, and ask for the Wi-Fi password. They write the password on a post-it note and give it to you.

Q1.4 (3 points) Which security principle is most closely related to your experience at this polling place?

◯ (G) Consider Shannon's maxim
● (J) Consider human factors
◯ (H) Least privilege
◯ (K) Defense in depth
◯ (I) Security is economics
◯ (L) Time of check to time of use

Solution: Polling places are temporary employers which employ many people. An overworked, underpaid employee who already has the WiFi password written down and doesn't have mastery of low-level network attacks is unlikely to be a good defense against a convincing imposter.

At the Campanile City polling center, you see a DHCP Discover message broadcast to everyone.

Assume your computer has IP address , and the network's router and DHCP server have IP address . Assume that there are no other machines on the network. Assume there are no reserved or private IP addresses.

You want to return a malicious DHCP Offer that would make you a MITM. What values of the assigned IP address and the gateway IP address could you use in your response?

Q1.5 (3 points) Assigned IP address:

Enter your answer in the text box on Exam Tool.

◯ (A) —— ◯ (B) —— ◯ (C) —— ◯ (D) —— ◯ (E) —— ◯ (F) ——

Solution: Any IP address not already in use works here. Since there are no other machines on the network, any IP except and is correct.

Q1.6 (3 points) Gateway IP address:

Enter your answer in the text box on Exam Tool.

Solution: You should make your own computer the gateway, so that the victim sends any outgoing messages to you first. The only correct answer is (your IP address).

Q2 *Coffee-Shop Attacks* **(17 points)**

Dr. Yang comes to MoonBucks and tries to connect to the network in the coffee shop. Dr. Yang and `http://www.piazza.com` are communicating through TCP. Mallory is an on-path attacker.

Q2.1 (5 points) Which of the following protocols are used when Dr. Yang first connects to the Wi-Fi network and visits `http://www.piazza.com`? Assume any caches are empty. Select all that apply.

☐ (A) CSRF

■ (C) DNS (or DNSSEC)

■ (E) DHCP

■ (B) IP

■ (D) HTTP

☐ (F) None of the above

Solution:

A: False. CSRF is not a protocol, but a web attack.

B: True. IP is used to send messages across the internet and is used by TCP, which is used by TLS, which is used by HTTPS.

C: True. DNS is used to look up the IP address of `www.piazza.com`.

D: True. HTTP is the application protocol being used.

E: True. DHCP is used to receive the initial network configuration for the client.

Q2.2 (3 points) Suppose Mallory spoofs a packet with a valid, upcoming sequence number to inject the malicious message into the connection. Would this affect other messages in the connection?

● (G) Yes, because the malicious message replaces some legitimate message

○ (H) Yes, because future messages will arrive out of order

○ (I) No, because on-path attackers cannot inject packets into a TCP connection

○ (J) No, because TCP connections are encrypted

○ (K) ——

○ (L) ——

Solution: When the server receives the original TCP packet whose sequence number was used by Mallory, the server will ignore it, thinking that it has already received its data and that it was retransmitted.

Q2.3 (3 points) To establish a TCP connection, Dr. Yang first sends a SYN packet with Seq $= 980$ to the server and receives a SYN-ACK packet with Seq $= 603$; Ack $= 981$. What packet should Dr. Yang include in the next packet to complete the TCP handshake?

◯ (A) SYN-ACK packet with Seq $= 981$; Ack $= 604$

◯ (B) SYN-ACK packet with Seq $= 604$; Ack $= 981$

● (C) ACK packet with Seq $= 981$; Ack $= 604$

◯ (D) ACK packet with Seq $= 604$; Ack $= 981$

◯ (E) Nothing to send, because the TCP handshake is already finished.

◯ (F) ——

Solution: This is the third step of the 3-way handshake, when the client sends an ACK packet to acknowledge the server's SYN-ACK packet.

Q2.4 (3 points) Immediately after the TCP handshake, Mallory injects a valid RST packet to the server. Next, Mallory spoofs a SYN packet from Dr. Yang to the server with headers Seq $= X$. The server responds with a SYN-ACK packet with Seq $= Y$; Ack $= X + 1$. What is the destination of this packet?

● (G) Dr. Yang

◯ (H) The server

◯ (I) Mallory

◯ (J) None of the above

◯ (K) ——

◯ (L) ——

Solution: The server uses the source as the destination for the SYN-ACK packet. Because Mallory spoofed the packet from the client, the response is sent to the client.

Q2.5 (3 points) Which of the following network attackers would be able to perform the same attacks as Mallory?

Clarification during exam: By "perform the same attacks," we mean "reliably perform the same attacks."

● (A) A MITM attacker between Dr. Yang and the server

○ (B) An off-path attacker

○ (C) All of the above

○ (D) None of the above

○ (E) ——

○ (F) ——

Solution: A MITM attacker has all the capabilities of an on-path attacker, so it would be able to perform Mallory's attacks. An off-path attacker would be unable to guess the sequence numbers and would be unable to perform Mallory's attacks.

Q3 *Pancake Query Protocol* **(19 points)**

EvanBot is already prepared for the winter break but realizes that there are no more pancakes and needs to order more! To speed up the ordering process, EvanBot crafts a custom Pancake Query Protocol (PQP) and needs to ensure that it is secure.

PQP runs directly over IP, and a PQP packet contains the following information:

- A packet type
- The pancake query data (either a request for an order, or the order itself)

For now, assume that the only packet type supported by PQP is the ORDER type. For example, EvanBot might send the following PQP packet:

- EvanBot $\longrightarrow$ Restaurant: {Type: ORDER; Data: "I want 1 stack of blueberry pancakes!"}

For all parts, assume that EvanBot knows the IP address of the restaurant. All subparts of this question are independent.

Q3.1 (5 points) Which of the following statements are true about PQP? Select all that apply.

☐ (A) An off-path attacker can learn EvanBot's order

■ (B) An off-path attacker can trick the restaurant into cooking unwanted pancakes for EvanBot

☐ (C) An on-path attacker can conduct a RST injection attack

■ (D) An on-path attacker can learn EvanBot's order

☐ (E) EvanBot can be sure that the restaurant received the order

☐ (F) None of the above

Solution: A: False. EvanBot will always send their order to the restaurant (i.e. not visible to the off-path attacker), since Bot knows the restaurant's IP address.

B: True. An off-path attacker can forge an IP packet as if it were coming from EvanBot and place an malicious order inside the forged PQP packet.

C: False. RST injection attacks don't exist without TCP, since a RST packet is a construct of TCP.

D: True. An on-path attacker can see the contents of the PQP packet and learn the order.

E: False. Raw IP does not provide reliability.

Q3.2 (3 points) EvanBot adds an ACK packet type to PQP packets. After a restaurant receives an order, the restaurant sends an ACK packet acknowledging the order. If EvanBot does not receive the ACK, EvanBot re-sends the order until an ACK is received.

EvanBot tries to order 1 stack of pancakes from the restaurant and eventually receives an ACK. Assume that **no** network attackers are present. How many orders could the restaurant receive?

◯ (G) Exactly 0, because IP is unreliable.

◯ (H) Either 0 or 1, because IP is unreliable.

◯ (I) 0 or more, because IP is unreliable.

◯ (J) Exactly 1, because the restaurant ACKs any order it receives.

● (K) 1 or more, because EvanBot might try more than once.

◯ (L) 2 or more, because the restaurant may send multiple ACKs.

Solution: EvanBot succeeds in receiving an ACK, sot he restaurant must have received at least one order. However, it is possible that the restaurant received more than one order: One possible sequence of events is that EvanBot tried sending their order multiple times without receiving an ACK. However, the restaurant received all of these orders, but all of the ACK packets they sent back were lost, because IP is unreliable. Eventually, one of the ACK packets got through to EvanBot.

Q3.3 (4 points) Consider the following modification to PQP: To order, the client generates a random order ID and sends it in the PQP ORDER packet along with the order. The server sends back the order ID in the PQP ACK packet.

Can an off-path attacker trick the restaurant into accepting a spoofed order appearing to come from EvanBot? Briefly justify your answer (1–2 sentences).

● (A) Yes

◯ (B) No

◯ (C) ——

◯ (D) ——

◯ (E) ——

◯ (F) ——

Solution: While including the random order ID makes this seem secure, notice that the restaurant takes action immediately when the order is received. An off-path attacker can thus forge an ORDER packet containing a malicious order and random order ID.

Q3.4 (4 points) Which of the following modifications to PQP, if made individually, would prevent an off-path attacker from tricking the restaurant into accepting spoofed orders? Select all that apply.

■ (G) The restaurant generates a random order ID and sends it back in the PQP ACK. The restaurant must receive a PQP ACK-ACK packet from EvanBot containing the order ID to confirm the order.

☐ (H) The restaurant sends a fixed time-to-live (TTL) to EvanBot in the PQP ACK. The restaurant must receive a final, empty PQP ACK packet from EvanBot within the TTL to confirm the order.

☐ (I) PQP runs over UDP instead of IP, and EvanBot chooses a random source port.

■ (J) PQP runs over TCP instead of IP.

☐ (K) None of the above

☐ (L) ——

Solution: Having the *restaurant* generate a random order ID, sending it back to the client, and then having the client send that order ID back to the server to confirm the order would work. This ensures that an off-path attacker must guess information that it cannot see, since it can't see the random order ID generated by the restaurant.

Q3.5 (3 points) EvanBot proposes an additional packet types for PQP: LISTORDERS. When a restaurant receives an LISTORDERS packet, it responds with a list of all orders that it has ever received from any customer. Name one security issue with this proposal and describe the steps an attacker should take to exploit this issue (1–2 sentence).

Solution: This creates a classic amplified DoS attack: An attacker can spoof an ORDER_LIST packet appearing to come from a victim IP address, and the restaurant will send a very large response to the victim. This is similar to DNSSEC response packets and the deprecated NTP MONLIST command.