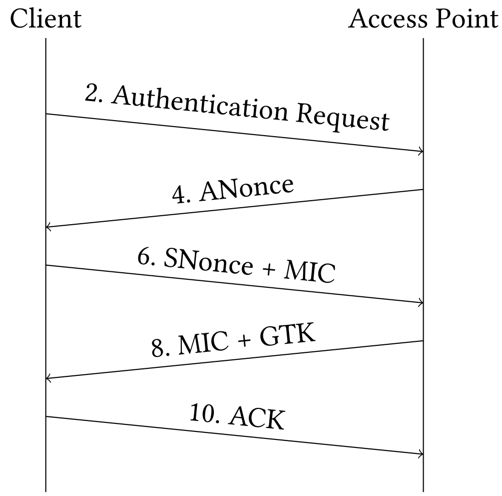
Q1 *I am Inevitable (SP22 Final Q10)* **(20 points)**

Recall the WPA 4-way handshake from lecture:



1. Client and AP derive the PSK from SSID and password.

3. AP randomly chooses ANonce.

5. Client randomly chooses SNonce and derives PTK.

7. AP derives PTK and verifies the MIC.

9. Client verifies the MIC.

For each method of client-AP authentication, select all things that the given adversary would be able to do. Assume that:

- The attacker does not know the WPA-PSK password but that they know that client's and AP's MAC addresses.
- For rogue AP attacks, there exists a client that knows the password that attempts to connect to the rogue AP attacker.
- The AMAC is the Access Point's MAC address and the SMAC is the Client's MAC address.

Q1.1 (5 points) The client and AP perform the WPA 4-way handshake with the following modifications:

- $\mathsf{PTK} = F(\mathsf{ANonce}, \mathsf{SNonce}, \mathsf{AMAC}, \mathsf{SMAC}, \mathsf{PSK})$, where F is a secure key derivation function
- $\mathsf{MIC} = \mathsf{PTK}$

☐ An on-path attacker that observes a successful handshake can decrypt subsequent WPA messages without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can trick the AP into completing a new handshake without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can learn the PSK without brute force.

☐ A rogue AP attacker can learn the PSK without brute force.

☐ A rogue AP attacker can only learn the PSK if they use brute force.

☐ None of the above

Q1.2 (5 points) The client and AP perform the WPA 4-way handshake with the following modifications:

- $\mathsf{PTK} = F(\mathsf{ANonce}, \mathsf{SNonce}, \mathsf{AMAC}, \mathsf{SMAC})$, where F is a secure key derivation function
- $\mathsf{MIC} = \mathsf{HMAC}(\mathsf{PTK}, \text{Dialogue})$

☐ An on-path attacker that observes a successful handshake can decrypt subsequent WPA messages without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can trick the AP into completing a new handshake without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can learn the PSK without brute force.

☐ A rogue AP attacker can learn the PSK without brute force.

☐ A rogue AP attacker can only learn the PSK if they use brute force.

☐ None of the above

Q1.3 (5 points) The client and AP perform the WPA 4-way handshake with the following modifications:

- Authentication: Client sends $\mathsf{H}(\mathsf{PSK})$ to AP, where H is a secure cryptographic hash.
- Verification: AP compares $\mathsf{H}(\mathsf{PSK})$ and to the value it received.
- AP sends: $\mathsf{Enc}(\mathsf{PSK}, \mathsf{PTK})$ to client, where Enc is an IND-CPA secure encryption algorithm.

☐ An on-path attacker that observes a successful handshake can decrypt subsequent WPA messages without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can trick the AP into completing a new handshake without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can learn the PSK without brute force.

☐ A rogue AP attacker can learn the PSK without brute force.

☐ A rogue AP attacker can only learn the PSK if they use brute force.

☐ None of the above

Q1.4 (5 points) The client and AP perform the WPA 4-way handshake with the following modifications:

- Authentication: Client conducts a Diffie-Hellman exchange with the AP to derive a shared key K.
- Client sends: $\mathsf{Enc}(K, \mathsf{PSK})$ to the AP.
- Verification: Check if $\mathsf{Dec}(K, \text{Ciphertext})$ equals the PSK
- Upon verification, AP sends: $\mathsf{Enc}(\mathsf{K}, \mathsf{PTK})$, where PTK is a random value, and sends it to the client.
- Assume that Enc is an IND-CPA secure encryption algorithm.

☐ An on-path attacker that observes a successful handshake can decrypt subsequent WPA messages without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can trick the AP into completing a new handshake without learning the value of the PSK.

☐ An on-path attacker that observes a successful handshake can learn the PSK without brute force.

☐ A rogue AP attacker can learn the PSK without brute force.

☐ A rogue AP attacker can only learn the PSK if they use offline brute force.

☐ None of the above

Q2 *Coffee-Shop Attacks (SU21 Final Q4)* (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.

- ☐ CSRF
- ☐ HTTP
- ☐ None of the above
- ☐ IP
- ☐ DHCP

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?

- ○ Yes, because the malicious message replaces some legitimate message
- ○ Yes, because future messages will arrive out of order
- ○ No, because on-path attackers cannot inject packets into a TCP connection
- ○ No, because TCP connections are encrypted

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?

- ○ SYN-ACK packet with Seq $= 981$; Ack $= 604$
- ○ SYN-ACK packet with Seq $= 604$; Ack $= 981$
- ○ ACK packet with Seq $= 981$; Ack $= 604$
- ○ ACK packet with Seq $= 604$; Ack $= 981$
- ○ Nothing to send, because the TCP handshake is already finished.

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?

- ○ Dr. Yang
- ○ Mallory
- ○ The server
- ○ None of the above

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

- ○ A MITM attacker between Dr. Yang and the server
- ○ All of the above
- ○ An off-path attacker
- ○ None of the above