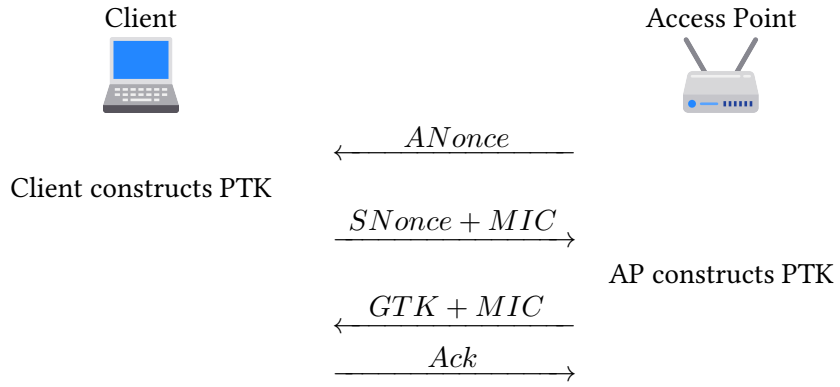
Q1 *WPA2 Personal* **(10 points)**

Consider the 4-way handshake used for the client to establish a connection to a Wi-Fi network, before receiving its network configuration.



Given a pre-shared key PSK, both client and access point compute the pairwise transient key as PTK = F(PSK, ANonce, SNonce, AP MAC, Client MAC).

Q1.1 If the pre-shared key is not high entropy, an attacker who doesn't know the key but records this 4-way handshake can bruteforce the key in an offline attack.

● True ○ False

Solution: True. Note that the key (PTK) is a function of PSK, ANonce, SNonce, AP MAC, and Client MAC.

ANonce and SNonce are sent in plaintext over the network, so the attacker who has recorded the handshake knows these values.

AP MAC and Client MAC are also sent in plaintext over the network (in the Source and Destination fields of the packets), so the attacker who has recorded the handshake also knows these values.

Thus the attacker only has to brute-force potential values of the pre-shared key (PSK), and if the PSK is not high-entropy, a brute-force attack is possible.

Note that the function F to generate the PTK is publicly known (recall Kerckhoff's principle: the attacker knows the system).

Q1.2 Even if the pre-shared key is high entropy and not known to the attacker, the attacker can still deploy a rogue access point that the client will trust as that network.

○ True ● False

Solution: The attacker would not be able to deploy a rogue access point (impersonating a legitimate access point) without knowing the pre-shared key (PSK).

In the handshake, the MICs (message integrity codes) use a key that is derived from the PTK. Recall that the PTK is derived from the PSK. Therefore, an attacker who doesn't know the PSK won't be able to derive the PTK and generate a valid MIC. The client will notice that the MICs are invalid and detect that they have not been talking to a legitimate access point.

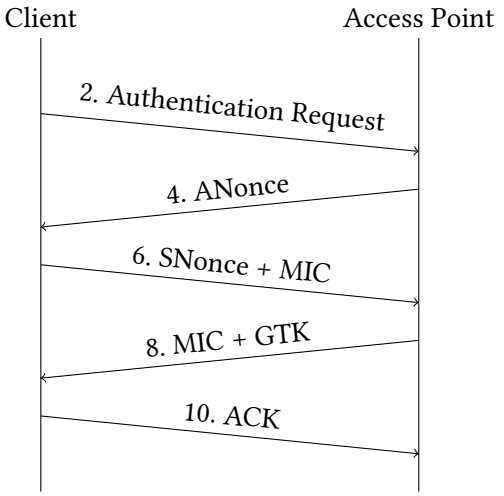
Q1.3 If an adversary records the traffic for the whole session and only later is able to discover the value of the pre-shared key, the adversary can decrypt all data sent in both directions, since the protocol doesn't provide forward secrecy.

● True ○ False

Solution: True. Messages sent over the network are encrypted with the PTK, which is a function of PSK, ANonce, SNonce, AP MAC, and Client MAC. As described in part (a), an adversary who records traffic knows all these values except PSK. An attacker who later discovers PSK will be able to derive the PTK and use the PTK to decrypt all the previously recorded messages.

Q2 *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.

Q2.1 (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

Solution: Because the MIC is the value of the PTK, it is trivial to decrypt subsequent communications. However, replay attacks are not possible since the ANonce is chosen by the AP, so the attacker can't trick the AP into completing a new handshake.

Additionally, because all the information needed to brute-force the PSK is sent in the clear (ANonce, SNonce, and MICs), brute-force attacks are possible by the rogue AP. However, there is no way of learning the PSK given the PTK with any method other than brute-force.

Q2.2 (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

Solution: Because the PSK isn't actually incorporated into this handshake, it is trivial for an attacker to derive the PTK to decrypt subsequent messages, and it is easy for them to form a new handshake with the AP.

Q2.3 (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

Solution: Assuming that an on-path attacker doesn't know the PSK, they can't brute-force the PTK since it's encrypted using the PSK and thus can't decrypt subsequent communications without learning the PSK. However, there are no nonces involved in the handshake, so it is possible to replay $\mathsf{H}(\mathsf{PSK})$ to trick the AP into completing a new handshake.

Because the PSK is hashed, it is not possible to learn the PSK as the attacker without brute force. However, if brute force is allowed, it is easy to guess a value of PSK and check if its hash equals the sent $\mathsf{H}(\mathsf{PSK})$.

Q2.4 (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

Solution: Unlike the previous question, Diffie-Hellman defends against replay attacks since the AP would choose a new private Diffie-Hellman component for each handshake. However, a rogue AP learns the value of K, and is thus able to learn the value of the PSK by decrypting $\mathsf{Enc}(K, \mathsf{PSK})$ using K.