Popa & Kao
Spring 2023

CS 161
Computer Security

Exam Prep 10

Q1 *Hackerman Visits the Voting Booth (FA20 Final Q11)* (21 points)

Your sketchy friend 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) None of the above

□ (K) ——

□ (L) ——

> **Solution:**
>
> 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.

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

□ (A) Changing the Wi-Fi password every day □ (D) ——

■ (B) Using WPA2-Enterprise □ (E) ——

□ (C) None of the above □ (F) ——

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

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 `10.10.10.142`, and the network's router and DHCP server have IP address `10.10.10.5`. 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:

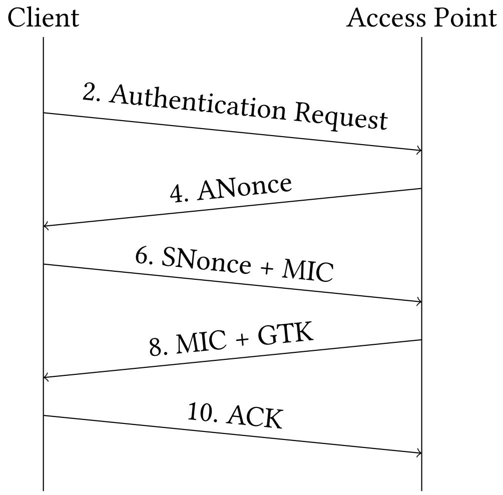
Solution: Any IP address not already in use works here. Since there are no other machines on the network, any IP except `10.10.10.142` and `10.10.10.5` is correct.

Q1.6 (3 points) Gateway IP address:

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 `10.10.10.142` (your IP address).

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.

This content is protected and may not be shared, uploaded, or distributed.

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 $\mathsf{Enc}(\mathsf{PSK}, \mathsf{PSK})$ to trick the AP into completing a new handshake.

Because the PSK is encrypted with itself, the on-path attacker and rogue AP aren't able to learn its value without brute force. However, if brute force is allowed, it is easy to guess a value of PSK and attempt to decrypt the ciphertext to see if the decrypted value is equal to the guessed 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.