CS 161 Fall 2024 — Introduction to Computer Security — Exam Prep 9

Q1 *Networking: New Phone Who This* (6 points)

EvanBot joins a new **broadcast** local network with many users. CodaBot is on the local network, but EvanBot doesn't know CodaBot's phone number. EvanBot wants to learn CodaBot's phone number, using the following protocol:

1. EvanBot broadcasts a request asking what CodaBot's phone number is.
2. CodaBot sends a response to EvanBot with their phone number.
3. EvanBot caches the phone number.

Q1.1 (1 point) Which networking protocol is this most similar to?

- ○ ARP
- ○ WPA2
- ○ BGP
- ○ TCP

Q1.2 (2 points) Eve is an on-path attacker in the local network. Select all attacks that Eve can carry out.

- ☐ Perform an online brute-force attack to learn CodaBot's phone number, by sending back every possible phone number to EvanBot.
- ☐ Learn CodaBot's phone number by reading message(s) Eve was not supposed to read.
- ☐ Learn CodaBot's phone number without reading message(s) Eve was not supposed to read.
- ☐ Convince EvanBot that CodaBot's phone number is some malicious value chosen by Eve.
- ☐ None of the above

In the next three subparts, consider this modification to the protocol: Instead of sending just the phone number, CodaBot sends their public key, and a signature on their phone number.

When EvanBot receives this data, EvanBot uses the public key to verify the signature on the phone number.

Eve wants to trick EvanBot into thinking CodaBot's phone number is a malicious value chosen by Eve. What values does Eve include in the packet she sends to EvanBot?

Q1.3 (1 point) For the public key, Eve sends:

- ○ Eve's public key
- ○ EvanBot's public key
- ○ CodaBot's public key
- ○ The router's public key

Q1.4 (1 point) For the signature over the phone number, Eve signs using:

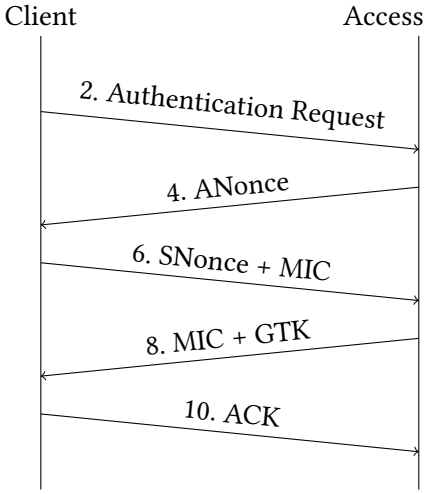
- ○ Eve's private key
- ○ EvanBot's private key
- ○ CodaBot's private key
- ○ The router's private key

Q1.5 (1 point) How often will this attack succeed?

- ○ 100% of the time
- ○ Only when CodaBot's packet arrives first
- ○ Only when Eve's packet arrives first
- ○ Never

Recall the WPA 4-way handshake from lecture:

Q2 *I am Inevitable (SP22 Final Q10)* **(20 points)**



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

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

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

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