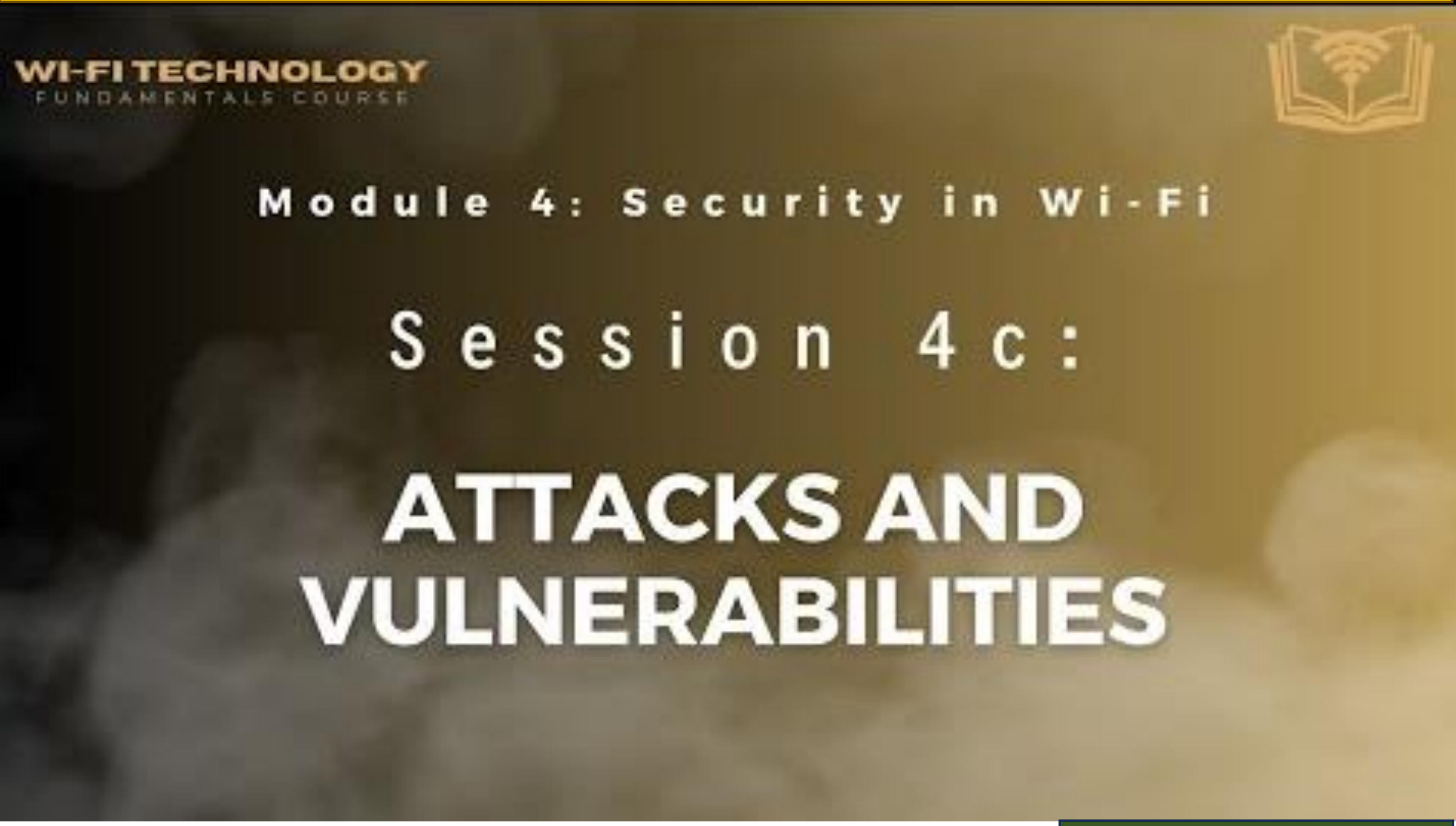


WI-FI TECHNOLOGY
FUNDAMENTALS COURSE

Module 4: Security in Wi-Fi

Session 4c:

ATTACKS AND VULNERABILITIES

What are Wireless Network Attacks?

Wireless network attacks are deliberate and malicious actions aimed at exploiting vulnerabilities in wireless communications systems to gain unauthorised access, intercept sensitive data, disrupt network operations, or compromise the security of devices and users connected to the network. These attacks target weaknesses in the protocols, configurations, or encryption mechanisms of wireless networks, taking advantage of their inherent nature of broadcasting signals over the airways.

Examples of Wireless Network Attacks:

- Wireless Eavesdropping (Passive Attacks):

Wireless eavesdropping is a type of wireless network attack where the attacker passively monitors wireless traffic to intercept sensitive data. This can be done using a variety of tools, such as wireless sniffers.

- Wireless Jamming:

Wireless jamming is a type of wireless network attack where the attacker disrupts or disables wireless communications by flooding the airwaves with interference signals. This can be done using a variety of tools, such as wireless jammers.

- Rogue Access Points:

A rogue access point is a wireless access point that is set up without the authorization of the network administrator. Rogue access points can be used to lure users into connecting to them and then intercept their traffic or launch other attacks.

- WEP/WPA Cracking:

WEP and WPA are encryption protocols that are used to protect wireless traffic. However, both of these protocols have vulnerabilities that can be exploited by attackers to crack the passwords and gain access to the wireless network.

- Evil Twin Attacks:

An evil twin attack is a type of wireless network attack where the attacker creates a fake wireless access point that has the same name as a legitimate access point on the network. When a user connects to the evil twin access point, the attacker can intercept their traffic or launch other attacks.

- Deauthentication/Disassociation Attacks:

A deauthentication/disassociation attack is a type of wireless network attack where the attacker sends deauthentication or disassociation frames to clients connected to an access point. This causes the clients to disconnect from the access point.

- Man-in-the-Middle Attacks:

A man-in-the-middle attack is a type of wireless network attack where the attacker intercepts communication between two parties and impersonates one of them. This can be done to steal sensitive data or to launch other attacks.

- Replay attacks:

A replay attack is a type of wireless network attack where the attacker captures and replays legitimate packets. This can be done to gain access to the network or to launch other attacks.

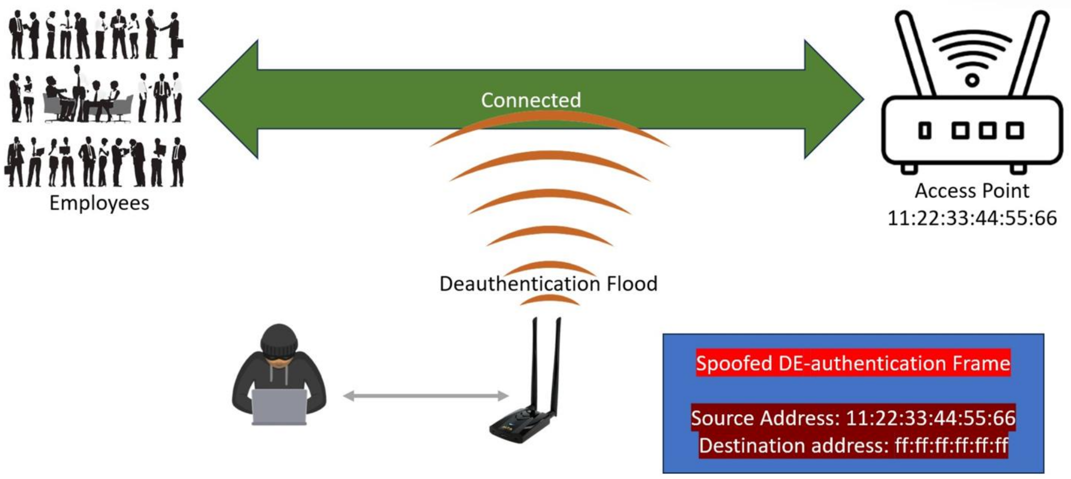
Denial-of-Service Attack on a Wireless Network

An attacker with minimal knowledge can disrupt a wireless network using a simple script and an Alpha adapter with monitor mode capability. By sending deauthentication frames disguised as coming from the access point, the attacker can disconnect all connected clients and prevent them from reconnecting. This effectively denies service to all users on the network.

How does it work?

1. The attacker creates a script to generate deauthentication frames. These frames appear to come from the access point.
2. The attacker uses an Alpha adapter with monitor mode capability to send the deauthentication frames to the network.
3. When a client receives a deauthentication frame, it believes it is being disconnected by the access point and attempts to reconnect.
4. The attacker continuously sends deauthentication frames, preventing clients from reconnecting and effectively denying them service.

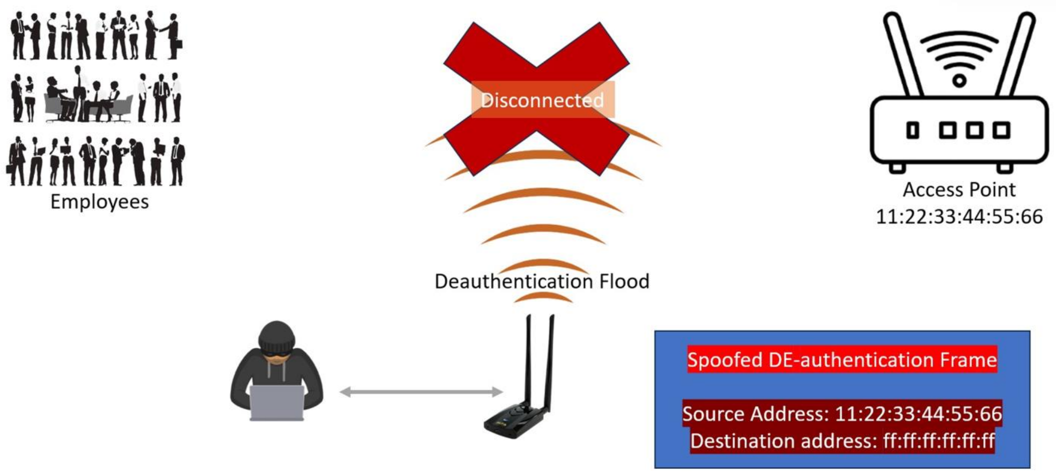
Denial of service attack



Spoofed DE-authentication Frame

Source Address: 11:22:33:44:55:66
Destination address: ff:ff:ff:ff:ff:ff

Denial of service attack



Spoofed DE-authentication Frame

Source Address: 11:22:33:44:55:66
Destination address: ff:ff:ff:ff:ff:ff

This attack can be particularly harmful because:

- It requires minimal knowledge and can be easily performed using readily available tools and scripts.
- It can disrupt network access for all connected clients, potentially causing significant downtime and inconvenience.
- It can be difficult to detect and prevent.

802.11w: Management Frame Protection

802.11w is a security protocol that encrypts management frames, offering enhanced protection for wireless networks.

- 802.11w significantly enhances wireless network security.
- While not a complete solution, it offers valuable protection against various attacks.
- Enabling 802.11w is recommended for improved network security.
- Other DoS attacks exist that aren't directly related to 802.11w.
- A layered security approach, including 802.11w, is crucial for comprehensive network protection.

Function:

- Encrypts management frames used for association, roaming, etc.
- Protects against eavesdropping and packet injection attacks.
- Enhances privacy by securing sensitive information within frames.

Mechanism:

- Generates additional keys during handshake:
  - PTK: encrypts unicast management frames.
  - GTK: encrypts broadcast/multicast management frames.

Benefits:

- Improved security: mitigates eavesdropping and injection attacks.
- Enhanced privacy: encrypts sensitive information for improved protection.
- Roaming protection: safeguards against deauthentication attacks during roaming.

Limitations:

- Device compatibility: not all devices support 802.11w.
- Performance impact: encryption processes may slightly affect network performance.
- DoS vulnerability: doesn't offer complete protection against all DoS attacks.

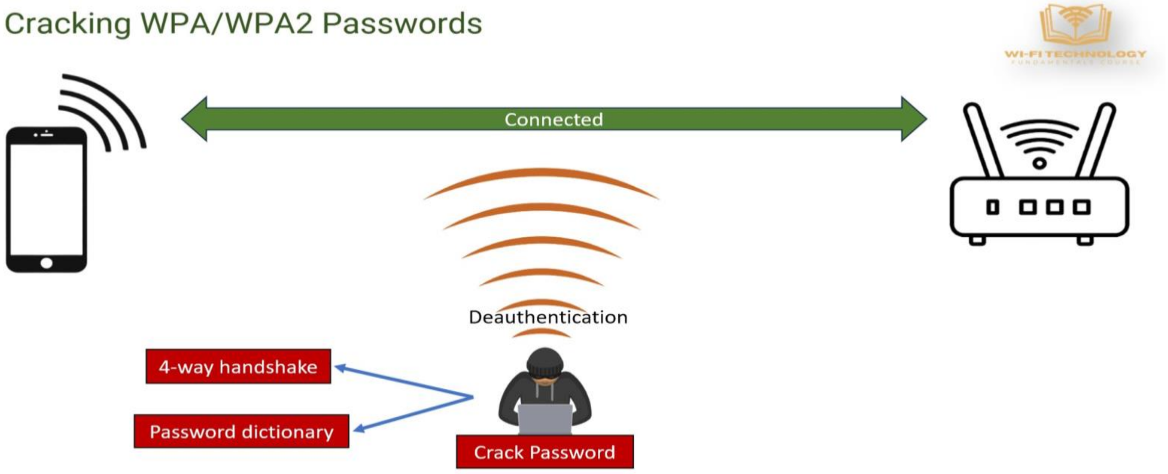
Demonstration:

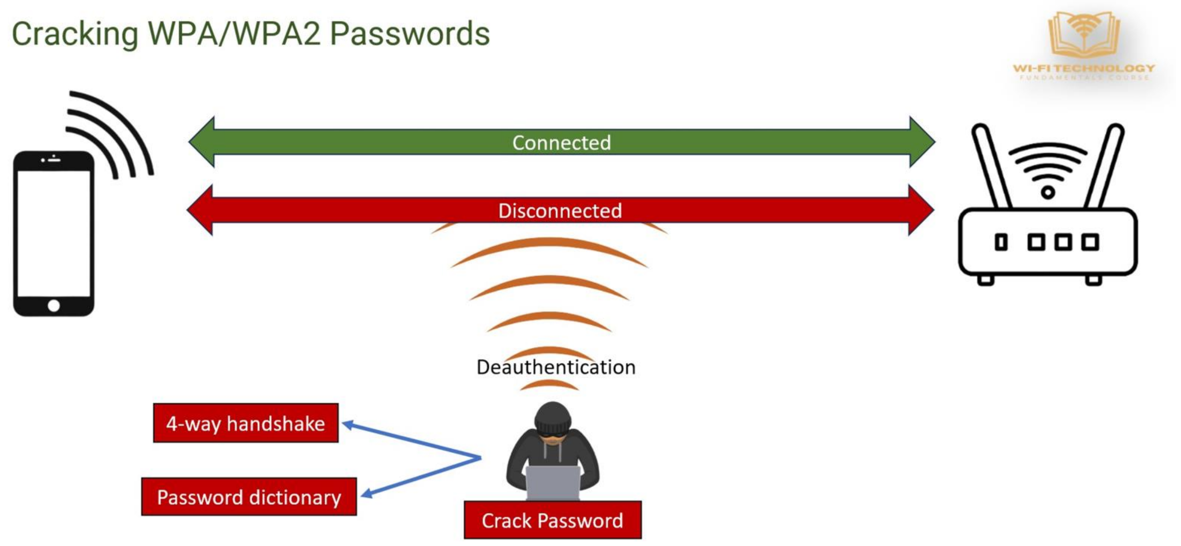
- Deauthentication attack:
  - Attacker sends deauthentication frames to disconnect clients.
  - With 802.11w, encrypted frames prevent this attack.
- Probe request flood:
  - Attacker sends numerous probe requests to overwhelm the access point.
  - 802.11w doesn't directly address this vulnerability, but performance impact is reduced.

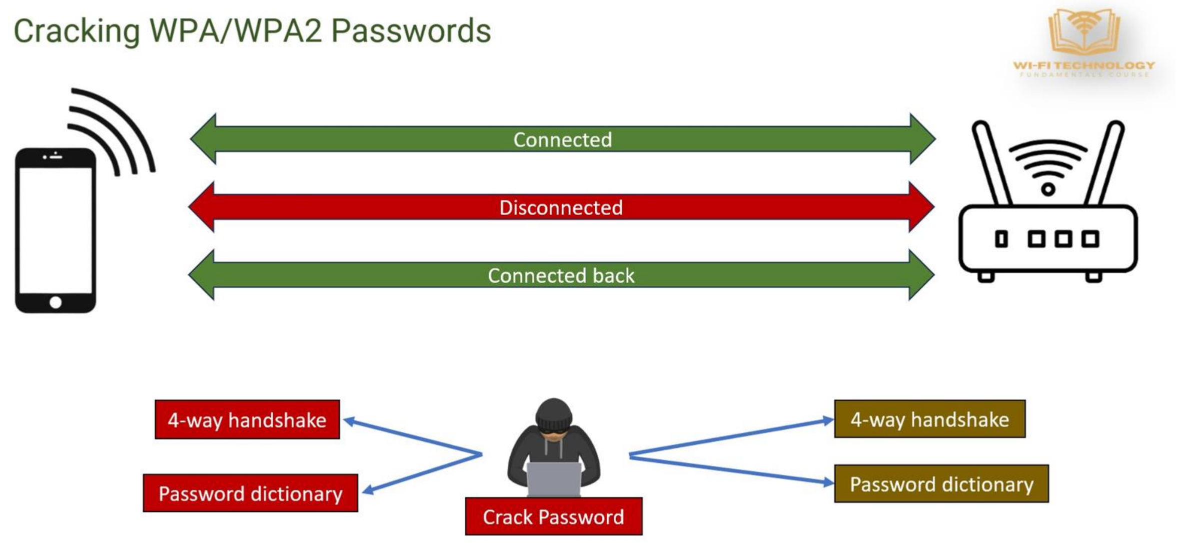
Cracking WPA/WPA2 Password

Here we can know how attackers can crack WPA/WPA2 passwords using a dictionary attack.

- Attackers need both a password dictionary and a four-way handshake to crack the password.
  - Password dictionary: Contains millions of potential passwords.
  - Four-way handshake captured: Obtained when a client connects to the access point.
- The process involves generating keys and comparing MICs to verify the password.
- Attackers can use tools to automate the process and try millions of passwords.
- We have two ways to capture the four-way handshake:
  - Waiting for a client to disconnect and reconnect.
  - Disconnecting the client and access point manually.
- Cracking WPA/WPA2 passwords is illegal and unethical.







How Attackers Crack Passwords:

- Evil twin attacks exploit human trust and lack of awareness.
- Strong passwords and secure access points are crucial for defense.

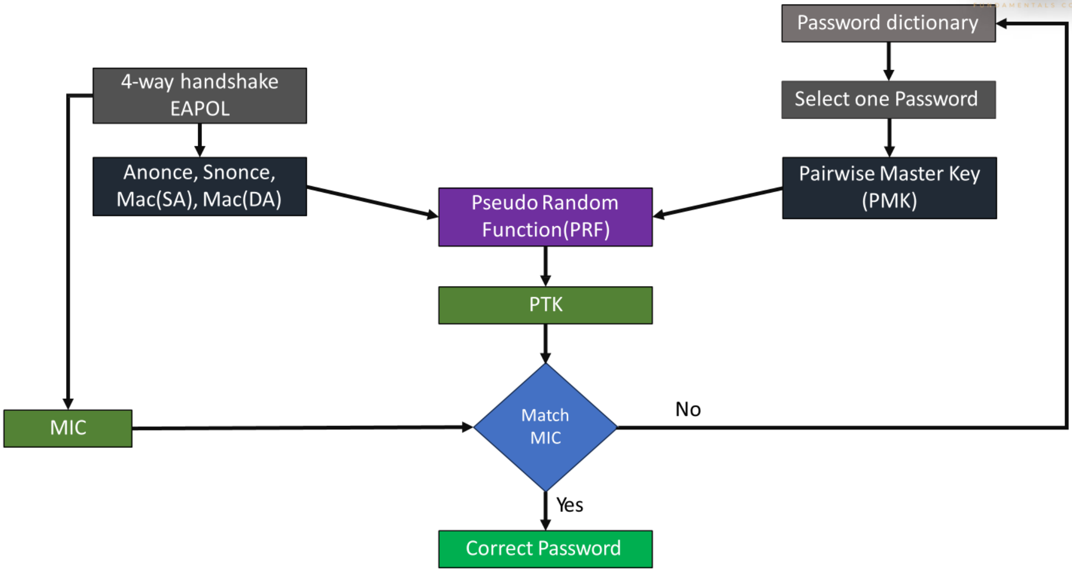
Attacker Tools and Techniques:

- Password dictionaries: Contain millions of potential passwords.
- Four-way handshake capture: Obtained when a client connects to the access point.
- Tools: Aircrack-ng, Hashcat, Reaver.

Cracking Process:

1. Select a password from the dictionary.
2. Generate PMK (Pairwise Master Key) from the selected password.
3. Generate PTK (Pairwise Transient Key) from PMK and information captured in the four-way handshake.
4. Derive MIC (Message Integrity Check) from PTK.
5. Compare the derived MIC with the MIC from the four-way handshake.
6. If the MICs match, the password is correct.
7. Repeat steps 1-6 with other passwords until the correct password is found.

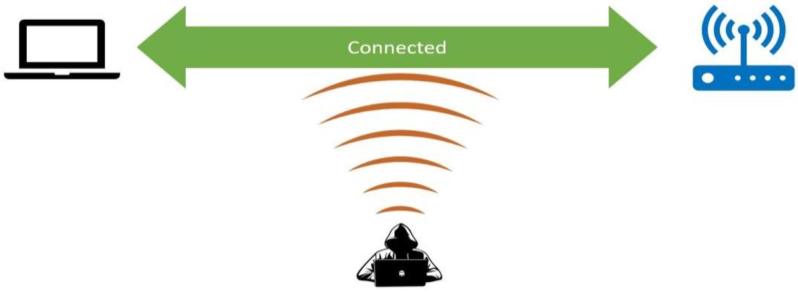
How attackers crack the password



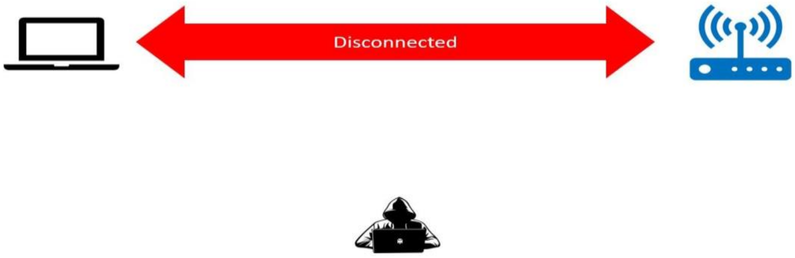
Evil Twin Attack:

1. Attacker sets up a fake access point with the same SSID as the legitimate one.
2. The attacker lures the user to connect by broadcasting a beacon and creating a captive portal. The user, thinking it's the legitimate network, enters their password.
3. The attacker checks if the entered password matches the captured four-way handshake. If successful, the attacker grants internet access, allowing them to intercept and manipulate the user's data.

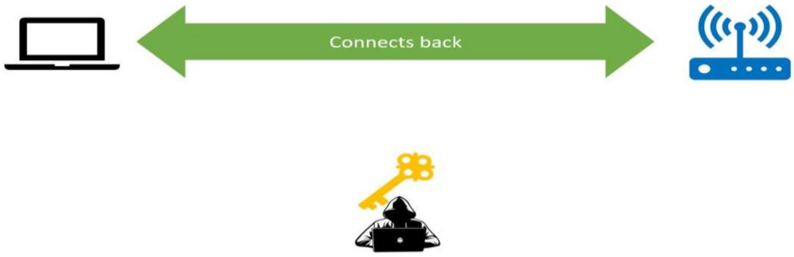
Evil Twin Attack



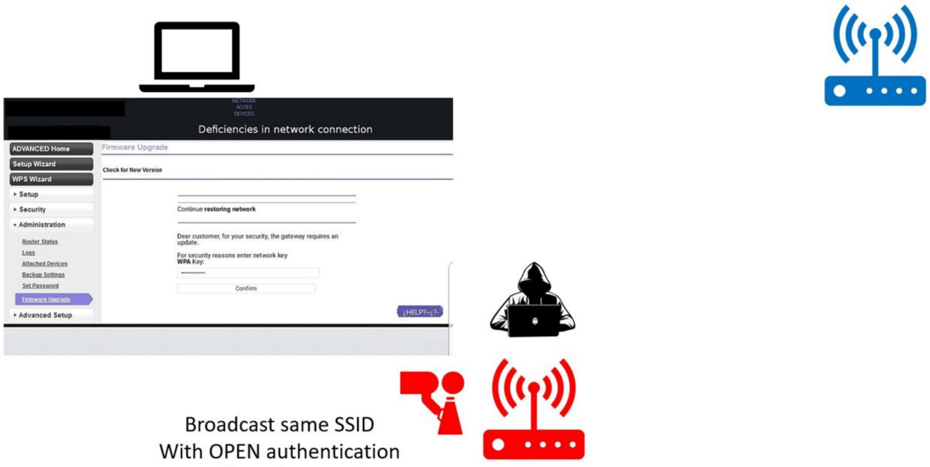
Evil Twin Attack



Evil Twin Attack



Evil Twin Attack



[redacted]

Deficiencies in network connection

Firmware Upgrade

Check for New Version

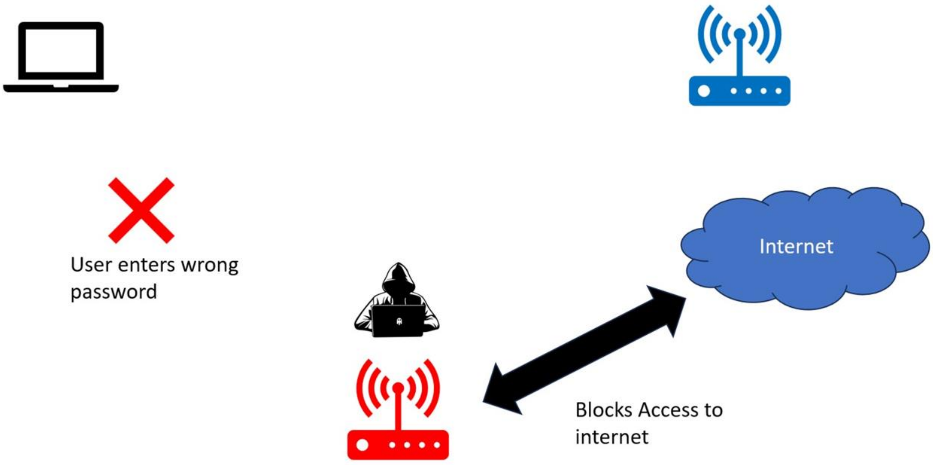
Continue **restoring network**

Dear customer, for your security, the gateway requires an update.

For security reasons enter network key
WPA Key:
•••••••••••••

Broadcast same SSID
With OPEN authentication
and captive portal

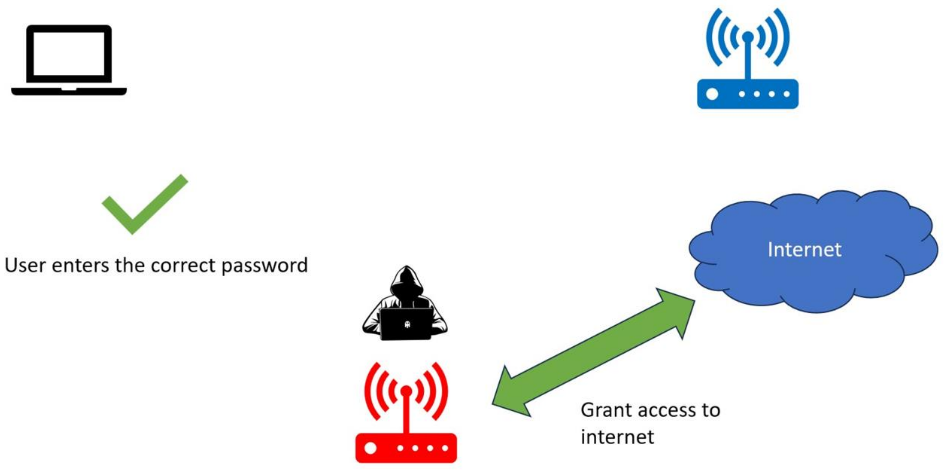
Evil Twin Attack



User enters wrong password

Blocks Access to internet

Evil Twin Attack



User enters the correct password

Internet

Grant access to internet

Preventing Wireless Network Attacks:

1. Use strong passwords: Avoid dictionary words, use uppercase and lowercase letters, numbers, and special characters.

2. Change default router credentials: Don't use "admin" or "password" for username and password.

3. Enable WPA3: The latest Wi-Fi security standard offering improved protection.

4. Enable 11w: Prevents denial-of-service attacks by securing management frames.

5. Use a RADIUS server for authentication: Provides centralised user management and different PMKs for each client.

6. Implement TLS: Ensures secure communication between clients and the network.

7. Use an IDS system: Detects and alerts about suspicious activity on the network.

8. Use MAC filtering: Allows access only to authorised devices by their MAC addresses.