
C|EH
Certified Ethical Hacker
Module 16
Hacking Wireless Networks

Module Objectives

Module Objectives

- Overview of Wireless Concepts
- Overview of Wireless Encryption Algorithms
- Understanding Wireless Threats
- Understanding Wireless Hacking Methodology
- Overview of Different Wireless Hacking Tools
- Understanding Bluetooth Hacking Techniques
- Overview of Wireless Hacking Countermeasures and Security Tools
- Overview of Wireless Penetration Testing

Module Flow

1. Wireless Concepts
2. Wireless Encryption
3. Wireless Threats
4. Wireless Hacking Methodology
5. Wireless Hacking Tools
6. Bluetooth Hacking
7. Countermeasures
8. Wireless Security Tools
9. Wireless Pen Testing

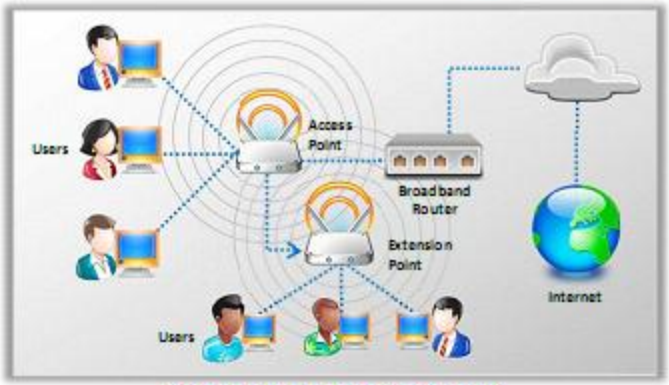
Wireless Terminologies

- **GSM**
  Universal system used for mobile transportation for wireless network worldwide
- **Bandwidth**
  Describes the amount of information that may be broadcasted over a connection
- **BSSID**
  The MAC address of an access point that has set up a Basic Service Set (BSS)
- **ISM band**
  A set of frequency for the international Industrial, Scientific, and Medical communities
- **Access Point**
  Used to connect wireless devices to a wireless/wired network
- **Hotspot**
  Places where wireless network is available for public use
- **Association**
  The process of connecting a wireless device to an access point
- **Service Set Identifier (SSID)**
  A 32 alphanumeric character unique identifier given to wireless local area network (WLAN)
- **Orthogonal Frequency-division Multiplexing (OFDM)**
  Method of encoding digital data on multiple carrier frequencies
- **Multiple input, multiple output orthogonal frequency-division multiplexing (MIMO-OFDM)**
  Air interface for 4G and 5G broadband wireless communications
- **Direct-sequence Spread Spectrum (DSSS)**
  Original data signal is multiplied with a pseudo random noise spreading code
- **Frequency-hopping Spread Spectrum (FHSS)**
  Method of transmitting radio signals by rapidly switching a carrier among many frequency channels

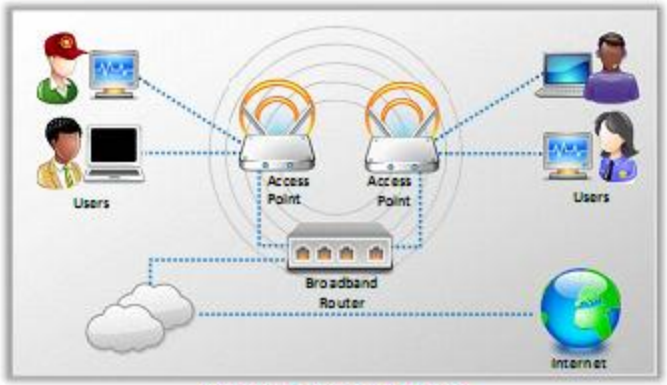
Wireless Networks

- Wireless Network (Wi-Fi) refers to wireless local area networks (WLAN) based on **IEEE 802.11 standard** where it allows the device to access the network from anywhere within range of an **access point**
- Devices such as a personal computer, video-game console, smartphone, etc. use Wi-Fi to connect to a **network resource** such as the Internet via a **wireless network access point**

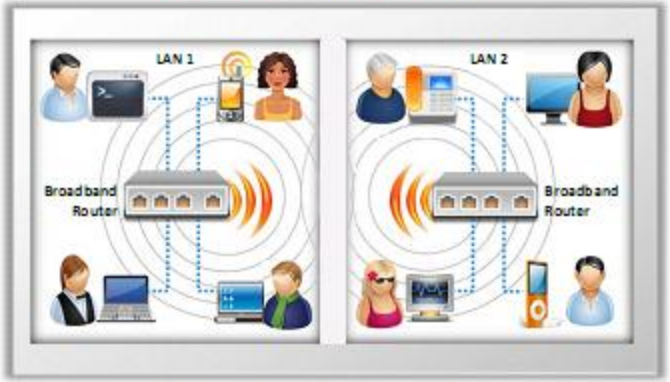
Types of Wireless Networks



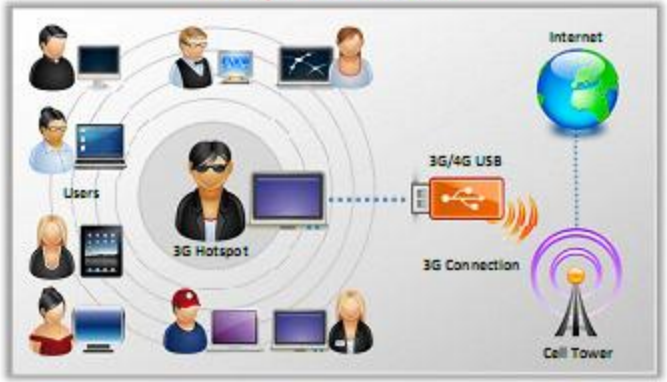
Extension to a Wired Network



Multiple Access Points



LAN-to-LAN Wireless Network



3G/4G Hotspot

Wireless Standards

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

Service Set Identifier (SSID)

- SSID is a human-readable text string with a maximum length of 32 bytes
- SSID is a token to identify a 802.11 (Wi-Fi) network; by default it is the part of the frame header sent over a wireless local area network (WLAN)
- 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
- If SSID of the network is changed, reconfiguration of the SSID on every host is required, as every user of the network configures the SSID into their system
- 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"
- The SSID remains secret only on the closed networks with no activity that is inconvenient to the legitimate users

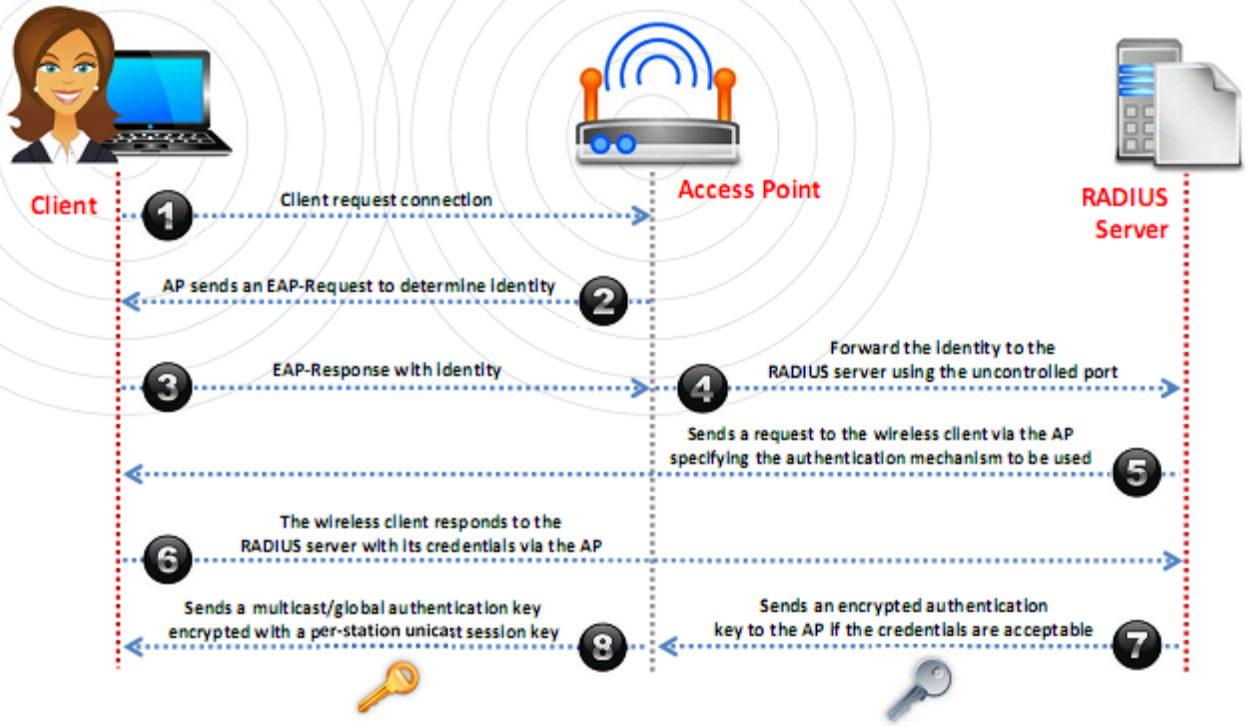
Wi-Fi Authentication Modes

Any wireless device can be **authenticated** with the access points, allowing the device to transmit data only when its WEP key **matches** with the **WEP key** of access point

The station and access point use the **same WEP key** to provide authentication which means that this key should be **enabled** and configured manually on both the **access point** and the **client**

Wi-Fi Authentication Process Using a Centralized Authentication Server

- In this Wi-Fi authentication process, a **centralized authentication server** known as **Remote Authentication Dial in User Service (RADIUS)** sends authentication keys to both the **AP** and **clients** that want to authenticate with the AP
- This **key enables** the **AP** to **identify** a particular **wireless client**



Types of Wireless Antennas

Directional Antenna

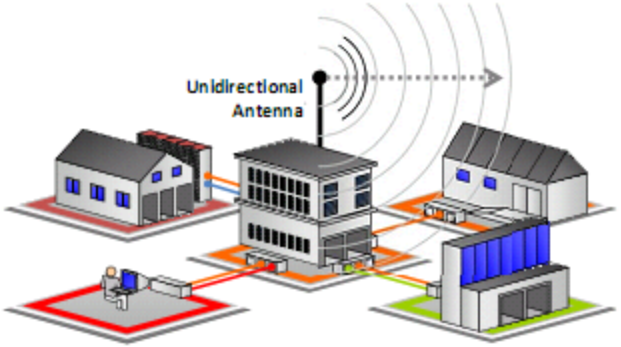
Used to broadcast and obtain radio waves from a single direction

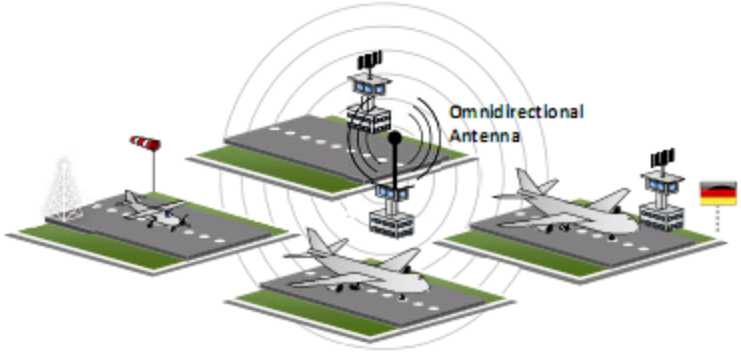
Omnidirectional Antenna

It provides 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

Reflector Antennas

Reflector antennas are used to concentrate EM energy which is radiated or received at a focal point

Module Flow

1. Wireless Concepts
2. Wireless Encryption
3. Wireless Threats
4. Wireless Hacking Methodology
5. Wireless Hacking Tools
6. Bluetooth Hacking
7. Countermeasures
8. Wireless Security Tools
9. Wireless Pen Testing

Types of Wireless Encryption

802.11i

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

WEP

WEP is an encryption algorithm for IEEE 802.11 wireless networks

LEAP

It is a proprietary version of EAP developed by Cisco

WPA

It is an advanced wireless encryption protocol using TKIP and MIC to provide stronger encryption and authentication

TKIP

A security protocol used in WPA as a replacement for WEP

WPA2

It is an upgrade to WPA using AES and CCMP for wireless data encryption

AES

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

CCMP

It is an encryption protocol used in WPA2 for stronger encryption and authentication

WPA2 Enterprise

It integrates EAP standards with WPA2 encryption

EAP

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

RADIUS

It is a centralized authentication and authorization management system

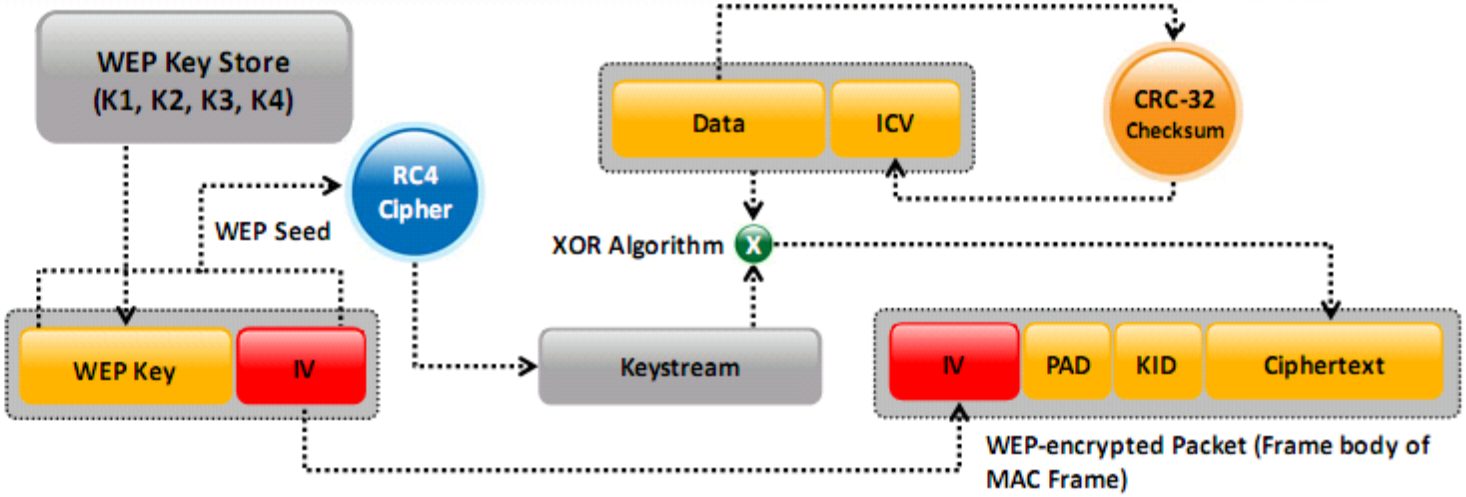
PEAP

It is a protocol, which encapsulates the EAP within an encrypted and authenticated Transport Layer Security (TLS) tunnel

WEP (Wired Equivalent Privacy) Encryption

- WEP is a security protocol defined by the 802.11b standard; it was designed to provide a wireless LAN with a level of **security and privacy** comparable to a wired LAN
- WEP **uses a 24-bit initialization vector (IV)** to form stream cipher RC4 for confidentiality and the CRC-32 checksum for integrity of wireless transmission
- It has significant vulnerabilities and design flaws and **can be easily cracked**

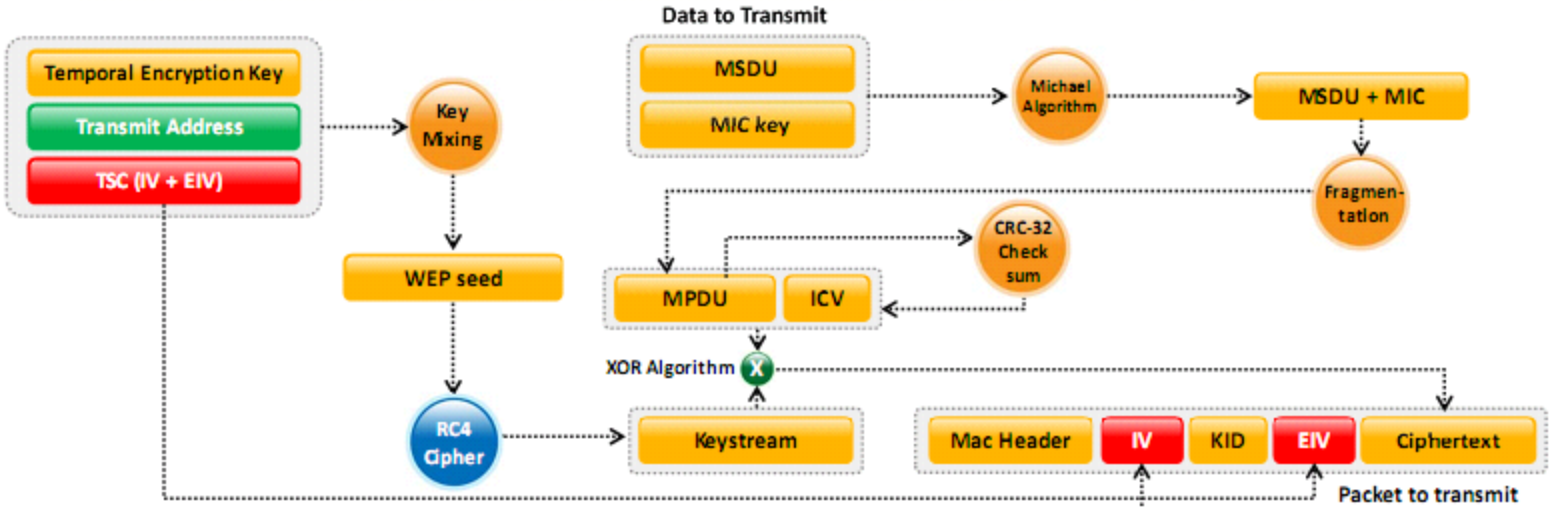
How WEP Works



WPA (Wi-Fi Protected Access) Encryption

- WPA is a security protocol defined by 802.11i standards; it uses a Temporal Key Integrity Protocol (TKIP) that utilizes **the RC4 stream cipher encryption** with 128-bit keys and 64-bit MIC integrity check to provide stronger encryption and authentication
- WPA uses TKIP to eliminate the weaknesses of WEP by including **per-packet mixing functions**, **message integrity checks**, **extended initialization vectors**, and **re-keying mechanisms**

How WPA Works



WPA2 (Wi-Fi Protected Access 2) Encryption

- WPA2 is an **upgrade to WPA**, it includes mandatory support for Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (**CCMP**), **an AES-based encryption mode** with strong security

Modes of Operation

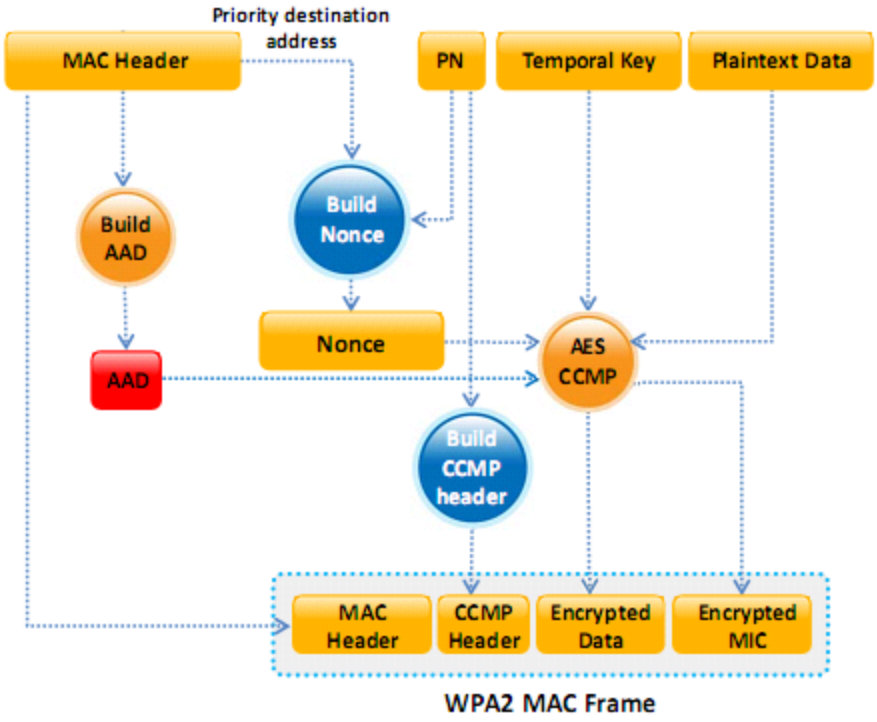
WPA2-Personal

- It uses a set-up password (**Pre-shared Key**, PSK) to protect unauthorized network access
- In PSK mode, each wireless network device encrypts the network traffic using a 128-bit key that is derived from 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, etc.
- Users are assigned **login credentials** by a centralized server which they must present when connecting to the network

How WPA2 Works



WPA2 MAC Frame

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	CBC-MAC

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

WEP Issues

1. The IV is a 24-bit field, which is too small and is sent in the cleartext portion of a message
2. Identical key streams are produced with the reuse of the same IV for data protection, as the IV short key streams are repeated within short time
3. Lack of centralized key management makes it difficult to change the WEP keys with any regularity
4. When there is IV Collision, it becomes possible to reconstruct the RC4 keystream based on the IV and the decrypted payload of the packet
5. IV is a part of the RC4 encryption key, which leads to an analytical attack that recovers the key after intercepting and analyzing a relatively small amount of traffic
6. Use of RC4 was designed to be a one-time cipher and not intended for multiple message use
7. No defined method for encryption key distribution
8. 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
9. Associate and disassociate messages are not authenticated
10. 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
11. WEP is based on a password, prone to password cracking attacks
12. 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)

1. In the RC4 algorithm, the **Key Scheduling Algorithm (KSA)** creates an IV based on the base key
2. The IV value is **too short and not protected** from reuse and no protection again message replay
3. A flaw in the WEP implementation of RC4 allows **"weak" IVs** to be generated
4. The way the keystream is constructed from the IV makes it susceptible to **weak key attacks** (FMS attack)
5. Those weak IVs **reveal information** about the key bytes they were derived from
6. No effective detection of **message tampering** (message integrity)
7. An attacker will collect enough weak IVs to reveal bytes of the **base key**
8. It directly uses the **master key** and has no built-in provision to update the keys

Module Flow

1. Wireless Concepts
2. Wireless Encryption
3. Wireless Threats
4. Wireless Hacking Methodology
5. Wireless Hacking Tools
6. Bluetooth Hacking
7. Countermeasures
8. Wireless Security Tools
9. Wireless Pen Testing

Wireless Threats

Access Control Attacks

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

- War Driving
- Rogue Access Points
- MAC Spoofing
- AP Misconfiguration
- Ad Hoc Associations
- Promiscuous Client
- Client Mis-association
- Unauthorized Association

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)

- Data Frame Injection
- WEP Injection
- Bit-Flipping Attacks
- Extensible AP Replay
- Data Replay
- Initialization Vector Replay Attacks
- RADIUS Replay
- Wireless Network Viruses

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

- Eavesdropping
- Traffic Analysis
- Cracking WEP Key
- Evil Twin AP
- Honeypot Access Point
- Session Hijacking
- Masquerading
- Man-in-the-Middle Attack

Wireless Threats (Cont'd)

Availability Attacks

Availability attacks aim at **obstructing the delivery of wireless services to legitimate users**, either by crippling those resources or by denying them access to WLAN resources

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

Authentication Attacks

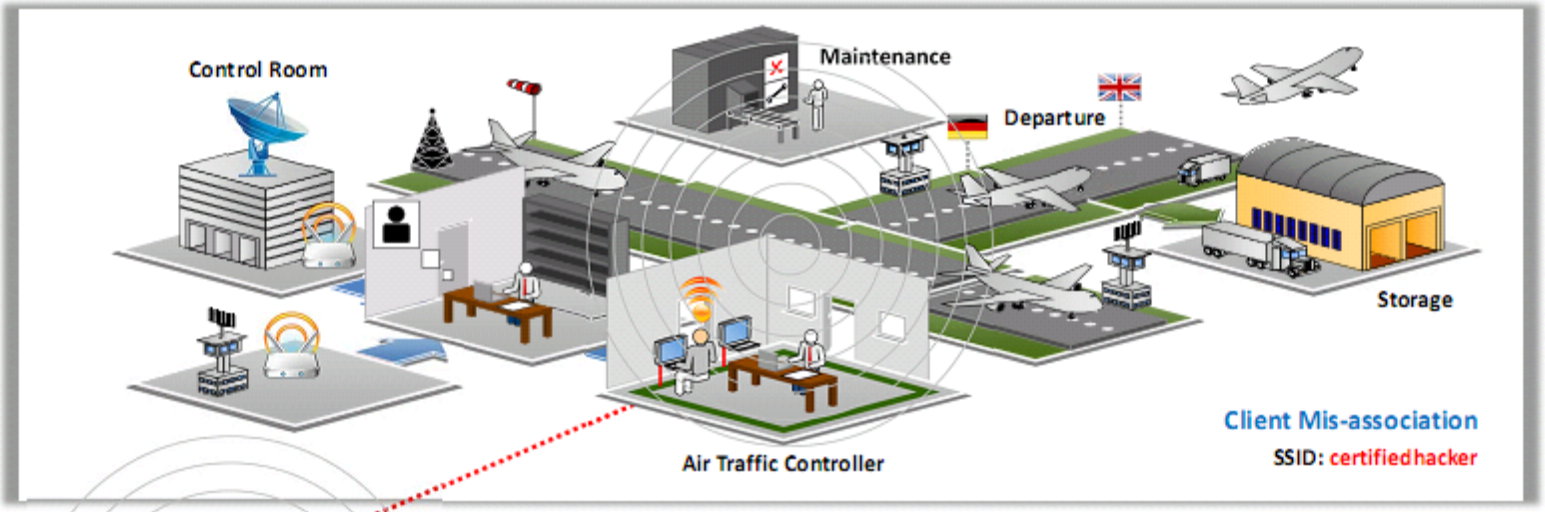
The objective of authentication attacks is to **steal the identity of Wi-Fi clients**, their personal information, login credentials, etc. to gain unauthorized access to network resources

- PSK Cracking
- Key Reinstallation Attack
- Identity Theft
- LEAP Cracking
- Shared Key Guessing
- VPN Login Cracking
- Password Speculation
- Domain Login Cracking
- Application Login Theft

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

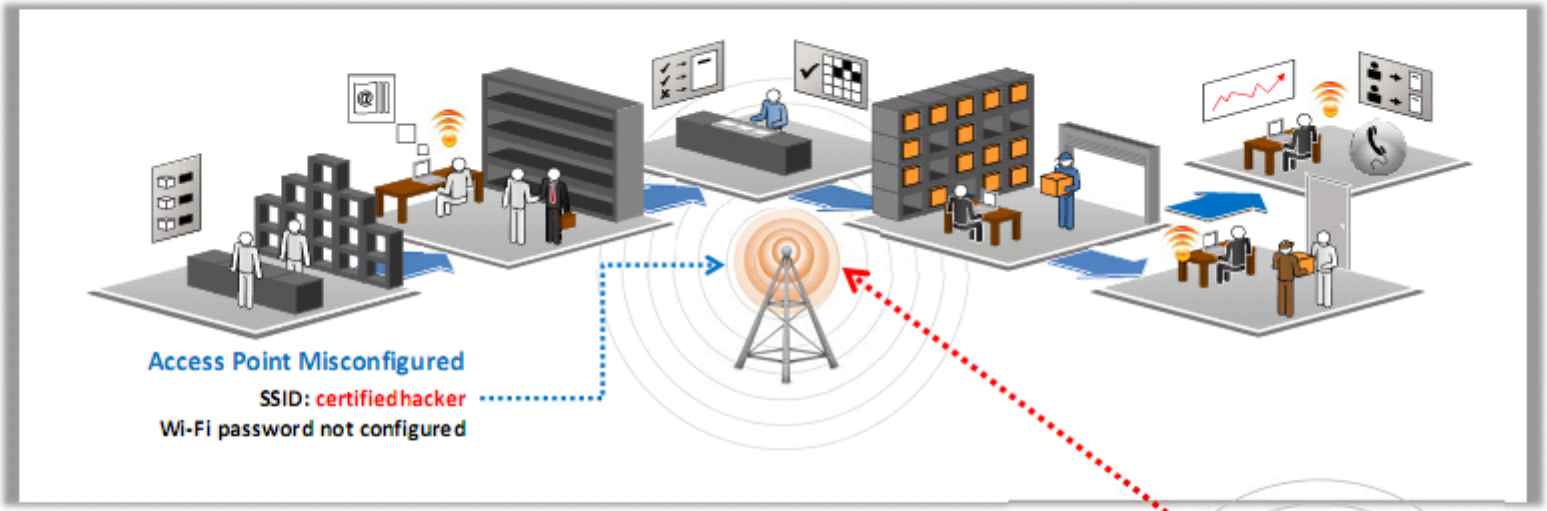
Client Mis-association



- Attacker sets up a rogue access point outside the corporate perimeter and lures the employees of the organization to connect with it

- Once associated, attackers may bypass the enterprise security policies

Misconfigured Access Point Attack



SSID Broadcast

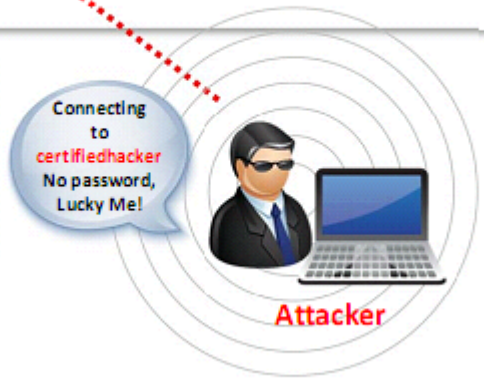
Access points are configured to broadcast SSIDs to authorized users

Weak Password

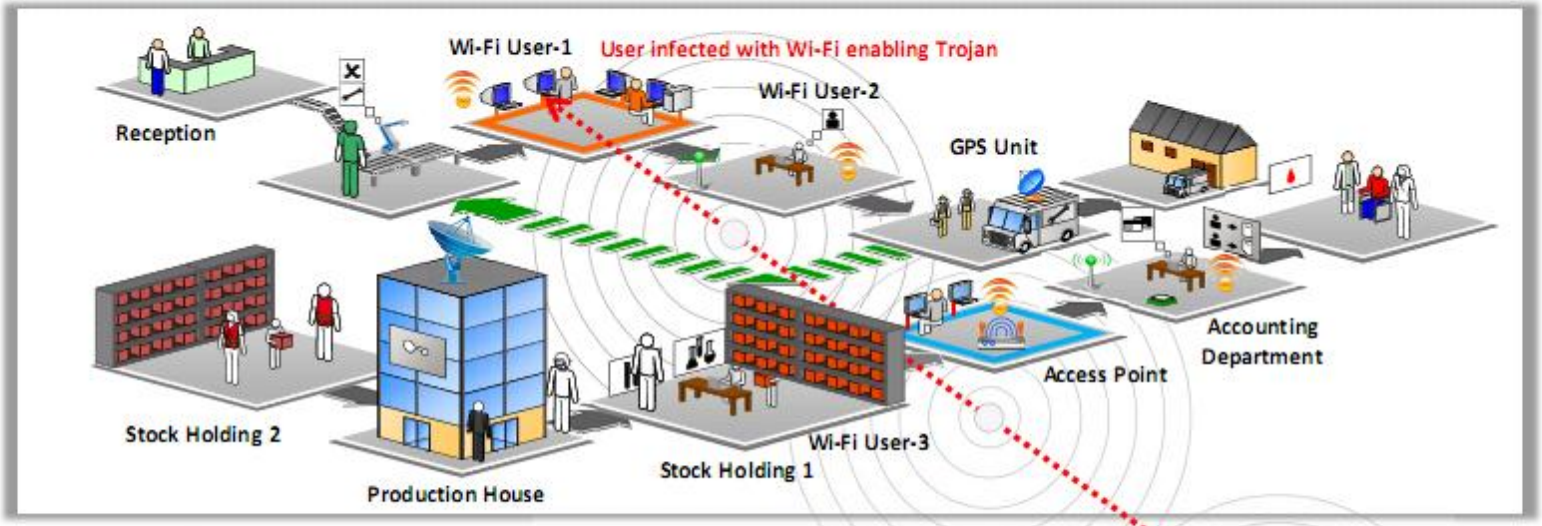
To verify authorized users, network administrators incorrectly use the SSIDs as passwords

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



Unauthorized Association



01

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

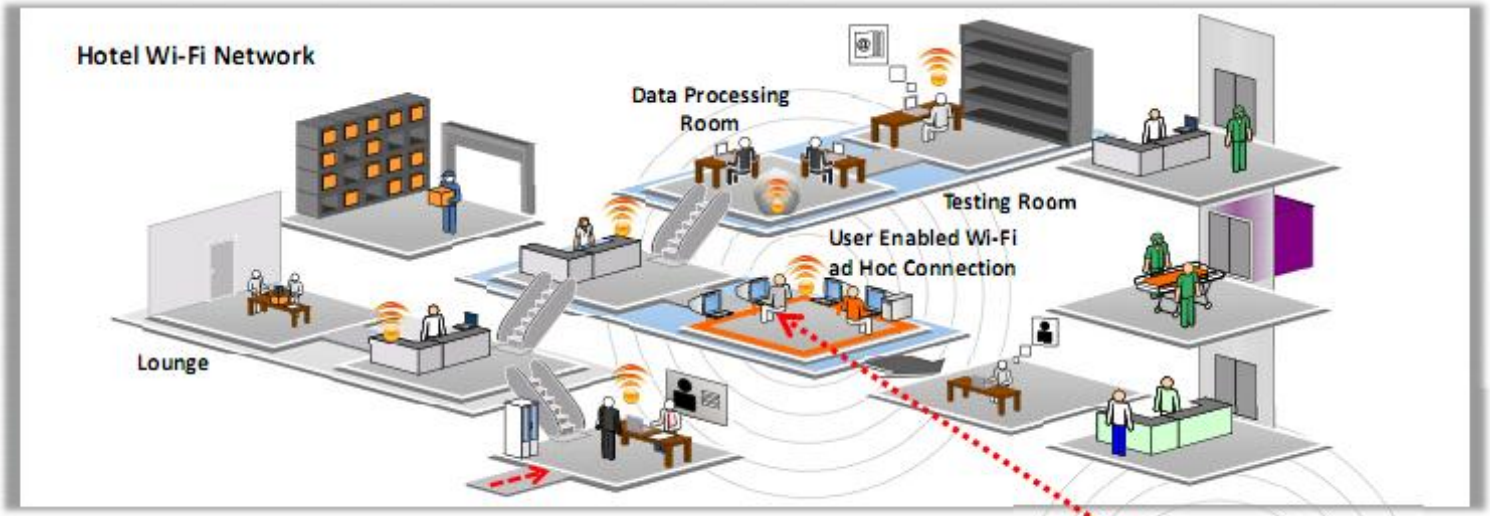
02

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

03

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

Ad Hoc Connection Attack

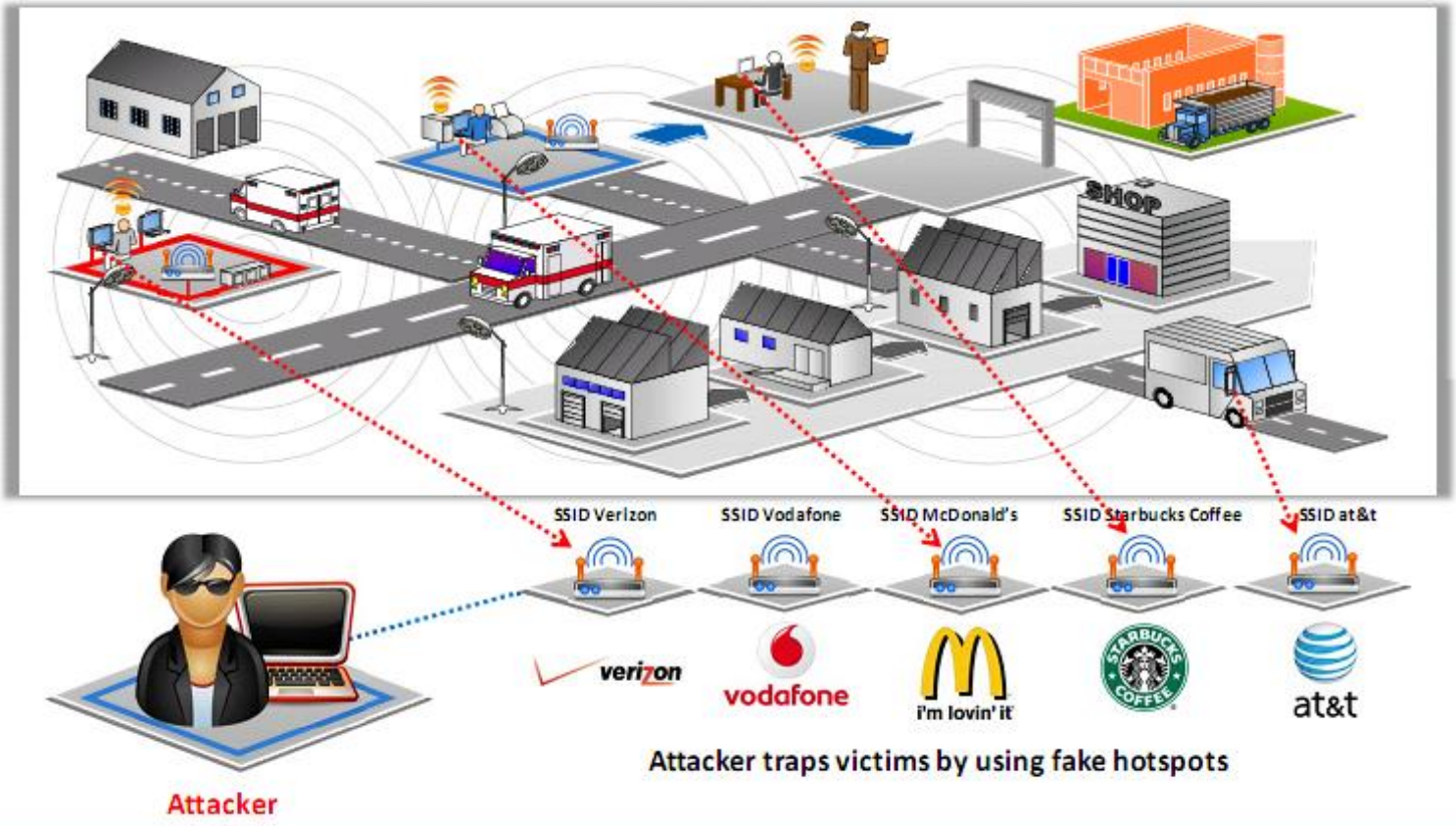


1. Wi-Fi clients communicate directly via an ad hoc mode that do not require an AP to relay packets

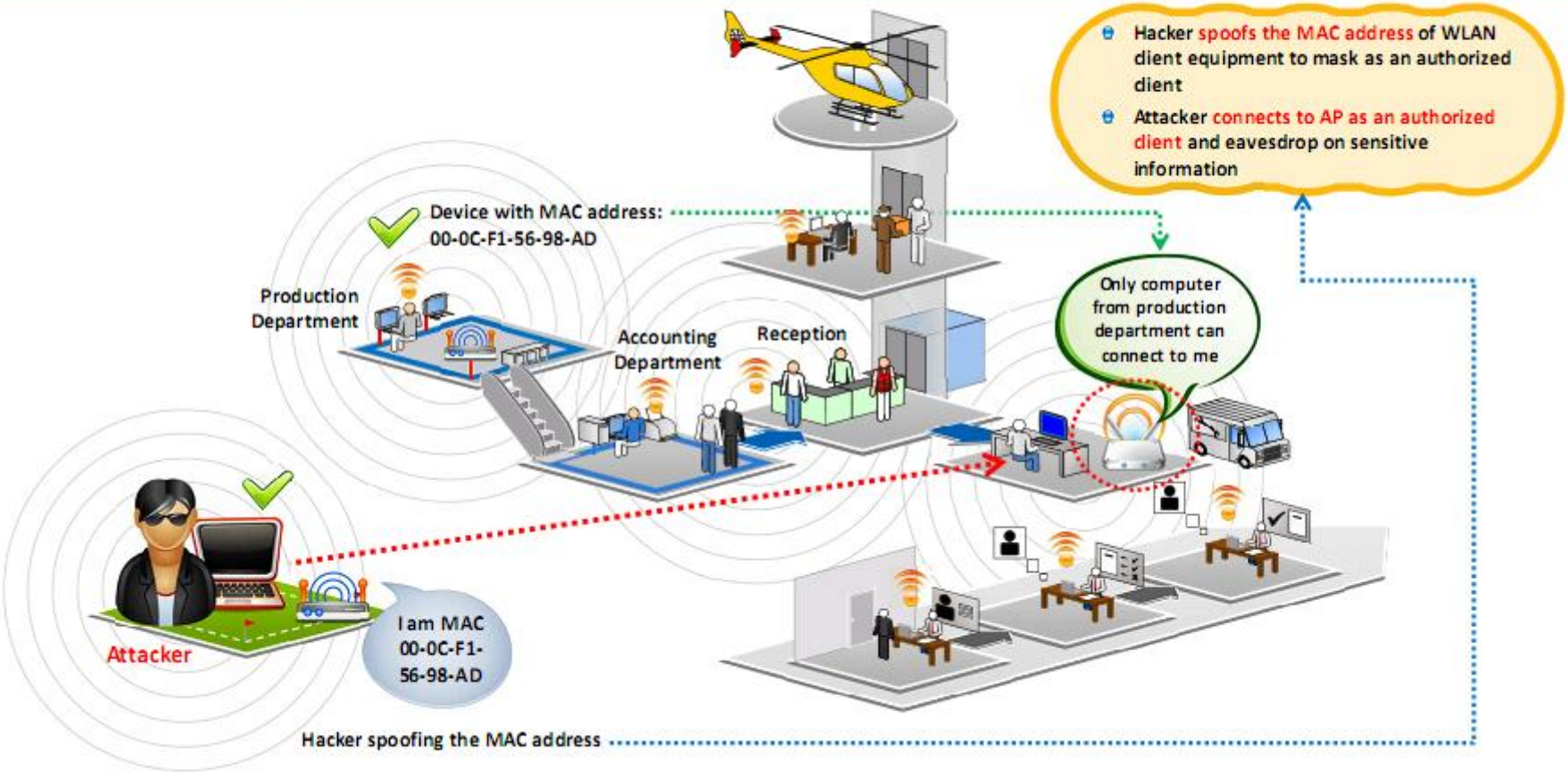
2. Ad hoc mode is inherently insecure and does not provide strong authentication and encryption

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

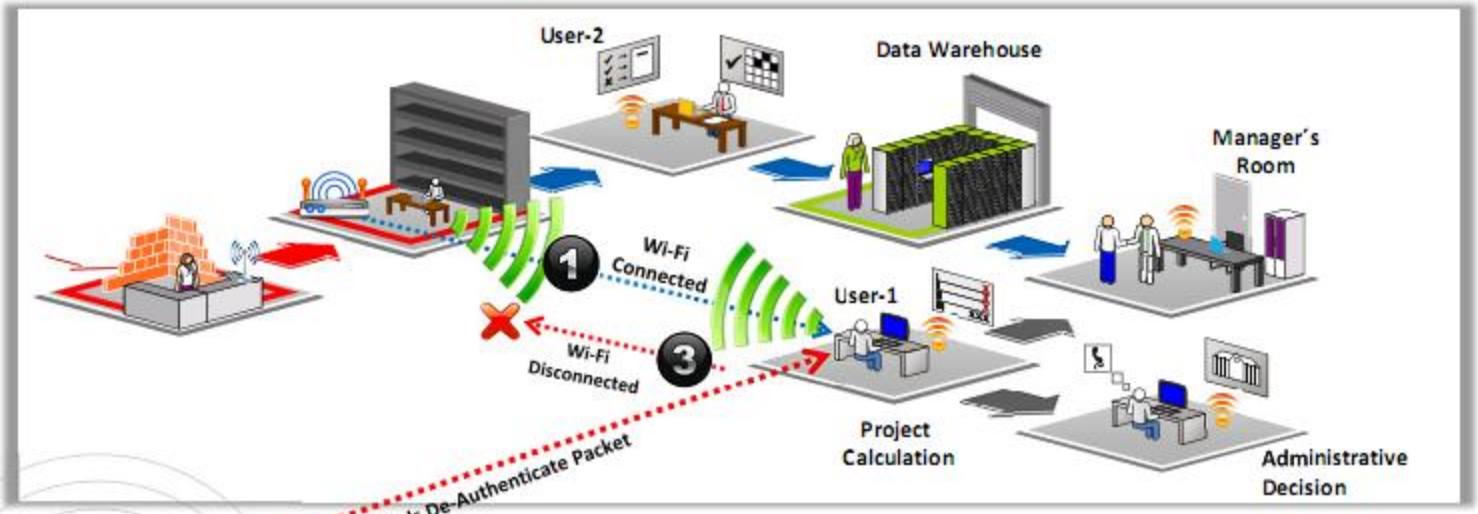
Honeypot Access Point Attack



AP MAC Spoofing



Denial-of-Service Attack

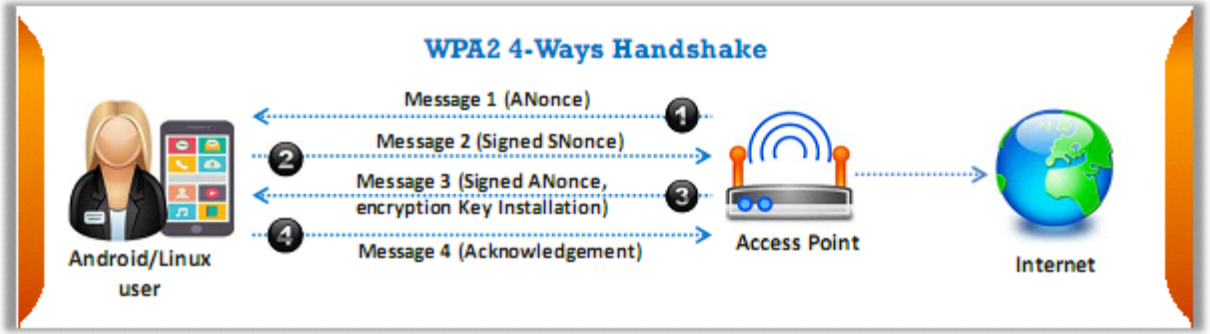


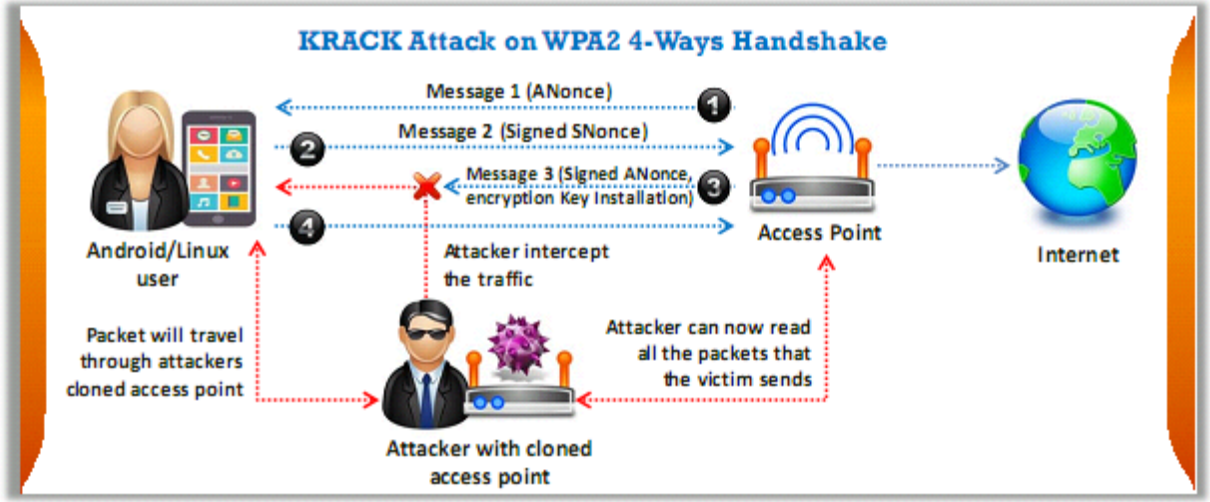
01 Wireless DoS attacks **disrupt network wireless connections** by sending broadcast "de-authenticate" commands

02 Transmitted deauthentication forces the clients to **disconnect from the AP**

Key Reinstallation Attack (KRACK)

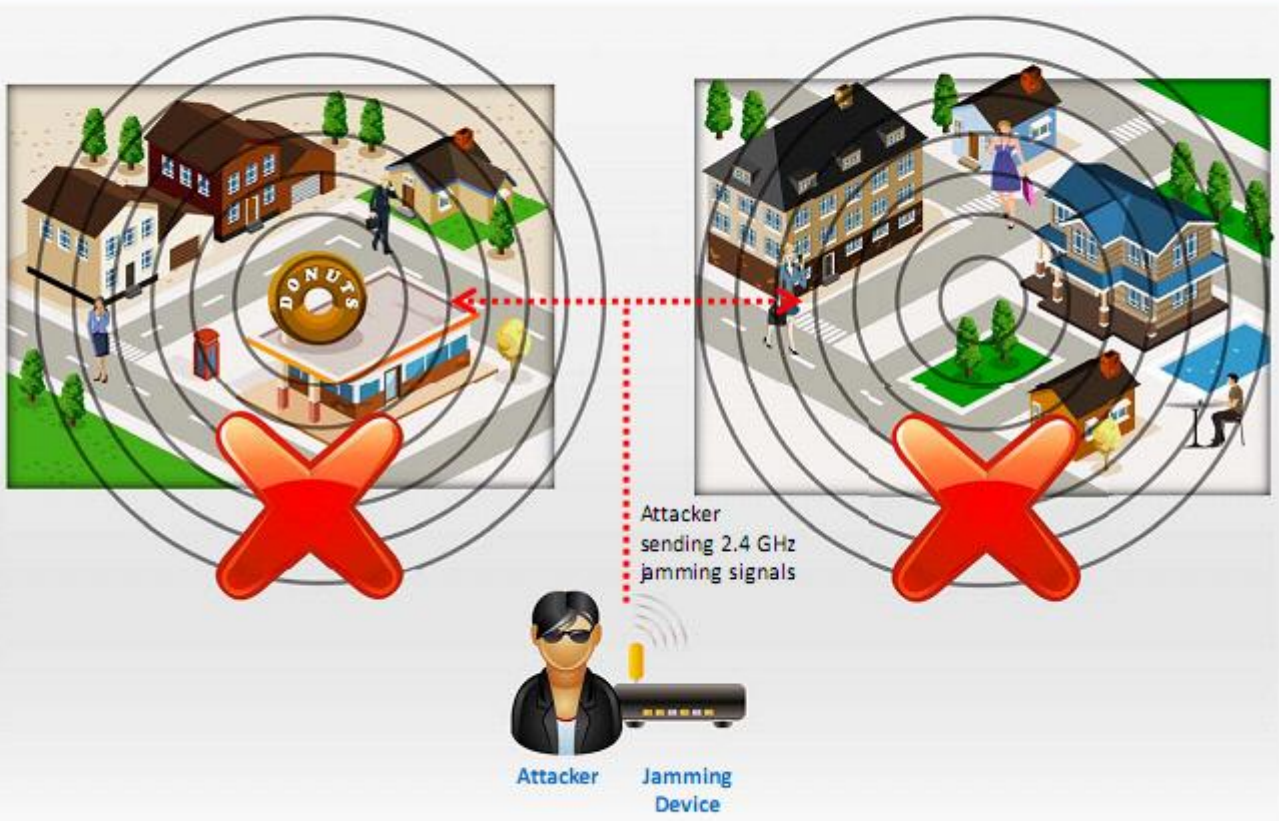
- All secure Wi-Fi networks use **the 4-way handshake process** to join the network and to generate a **fresh encryption key** that will be used to encrypt the network traffic
- The KRACK attack works by exploiting the 4-way handshake of the **WPA2 protocol** by forcing Nonce reuse
- KRACK works against all **modern protected Wi-Fi networks** and allows attacker to steal sensitive information such as credit card numbers, passwords, chat messages, emails, photos, etc.





Jamming Signal Attack

- All wireless networks are prone to jamming
- This jamming signal causes a DoS because **802.11 is a CSMA/CA protocol**, whose collision avoidance algorithms require a period of silence before a radio is allowed to transmit
- An attacker stakes out the area from a nearby location with a **high gain amplifier** drowning out the legitimate access point
- Users simply can't get through to log in or they are **knocked off** their connections by the overpowering nearby signal



Wi-Fi Jamming Devices

MGT-P1B Wi-Fi Jammer

- Range: 6 ~ 8 meters
- Internal Antennas
- 1 frequency bands jammed (Wi-Fi / Bluetooth)
- Portable

MGT-P6 Wi-Fi Jammer

- Range: 10 ~ 12 meters
- 4 antennas
- 4 Frequency bands jammed (GSM - DCS -3G - Wi-Fi - Bluetooth)

MGT-615 Jammer

- Range: 5 ~ 100 meters 6 antennas
- 6 Blurred frequency bands (2G - 3G - 4G - Wifi / Bluetooth)
- Wall mountable

MGT-04 WiFi Jammer

- Range: 5 ~ 80 meters
- 4 antennas
- 4 Frequency bands jammed (GSM - DCS - 3G - WiFi/Bluetooth)
- Wall mountable

MGT-06B Jammer

- Range: 20 ~ 45 meters
- 6 antennas
- 6 frequency bands jammed (GSM - DCS - 3G - 4G 800 - 4G 2600 - WiFi/Bluetooth)
- Internal battery : 3 hours of operating time

MGT-08 Jammer

- Range: 5 ~ 45 meters
- 8 antennas
- 8 frequency bands jammed (2G - 3G - 3G - 4G - GPS L1 - GPS L2 - WiFi/Bluetooth)
- Wall mountable

http://www.magnumtelecom.com

Module Flow

Wireless Hacking Methodology

- The objective of the wireless hacking methodology is to **compromise a Wi-Fi network** in order to gain unauthorized access to network resources

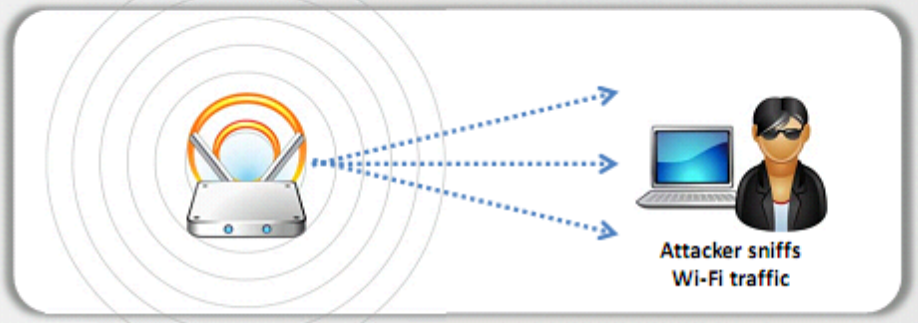
1. Wi-Fi Discovery
2. GPS Mapping
3. Wireless Traffic Analysis
4. Launch Wireless Attacks
5. Crack Wi-Fi Encryption
6. Compromise the Wi-Fi Network

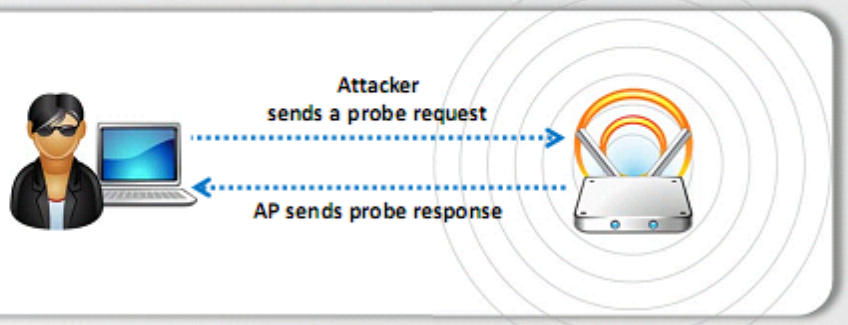
Wi-Fi Discovery: Footprint the Wireless Network

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

Passive Footprinting 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





Active Footprinting 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

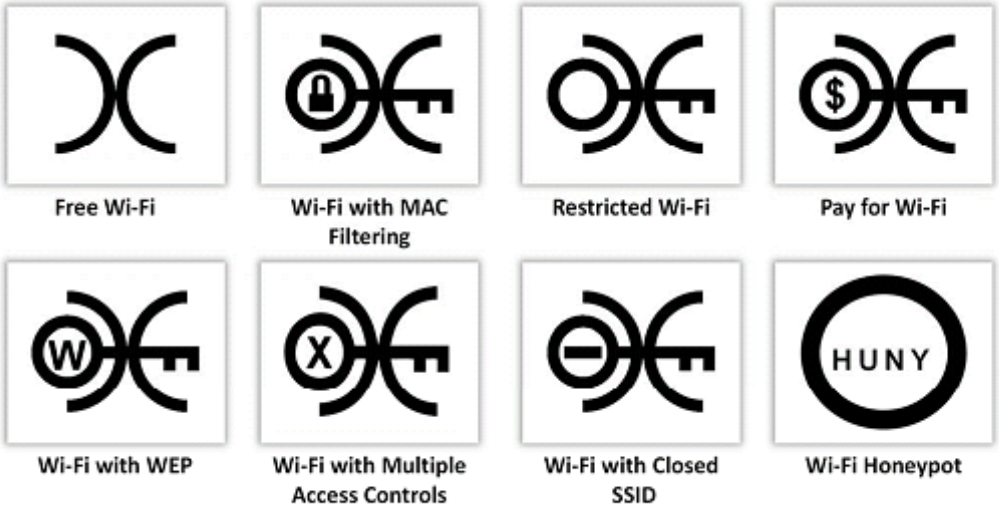
Wi-Fi Discovery: Find Wi-Fi Networks in Range to Attack

- 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
- Attackers use various **Wi-Fi Chalking techniques** such as WarWalking, WarChalking, WarFlying, WarDriving to find the target Wi-Fi network to attack
- Drive around with Wi-Fi enabled laptop installed with a **wireless discovery tool** and map out active wireless networks

Wi-Fi Chalking Techniques

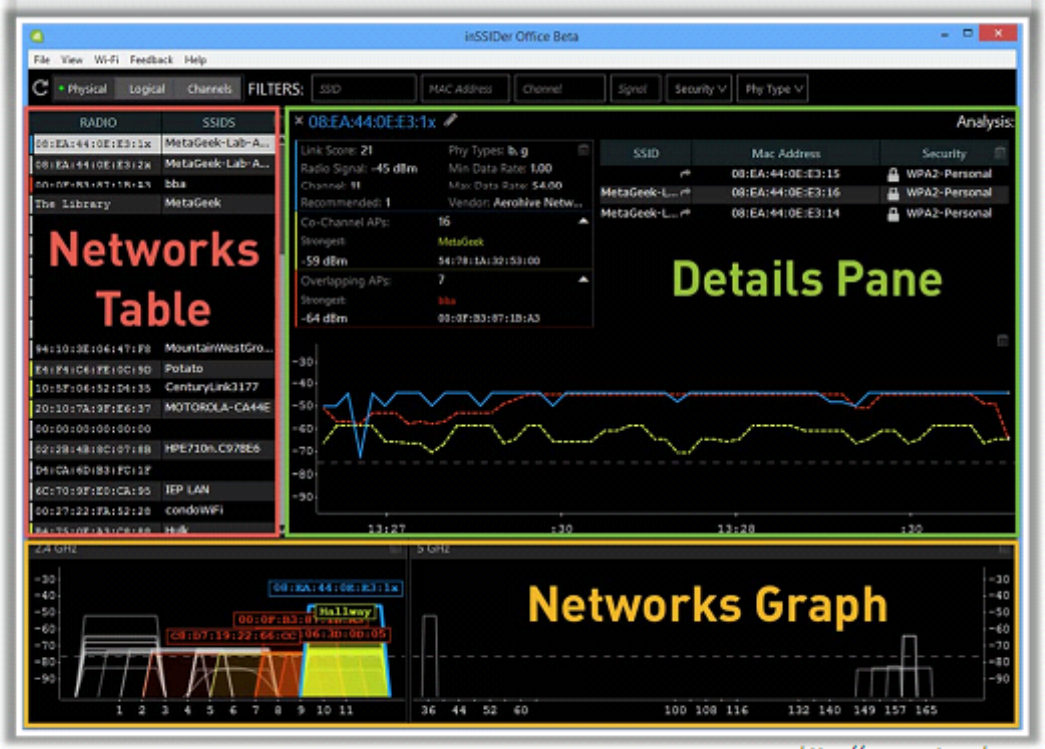
- **WarWalking**: Attackers walk around with Wi-Fi enabled laptops to detect open wireless networks
- **WarChalking**: A method used to draw symbols in public places to advertise open Wi-Fi networks
- **WarFlying**: Attackers use drones to detect open wireless networks
- **WarDriving**: Attackers drive around with Wi-Fi enabled laptops to detect open wireless networks

Wi-Fi Chalking Symbols



Wi-Fi Discovery Tools

inSSIDer Office Shows a **list of all the nearby wireless access points** and wireless networks with their signal strengths



https://www.metageek.com

NetSurveyor
http://nutsaboutnets.com

Xirrus Wi-Fi Inspector
https://www.xirrus.com

Acrylic Wi-Fi Home
https://www.acrylicwifi.com

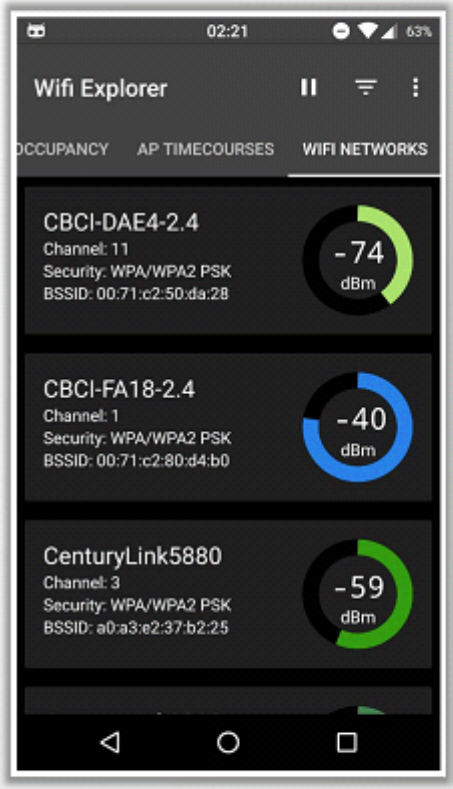
WirelessMon
https://www.passmark.com

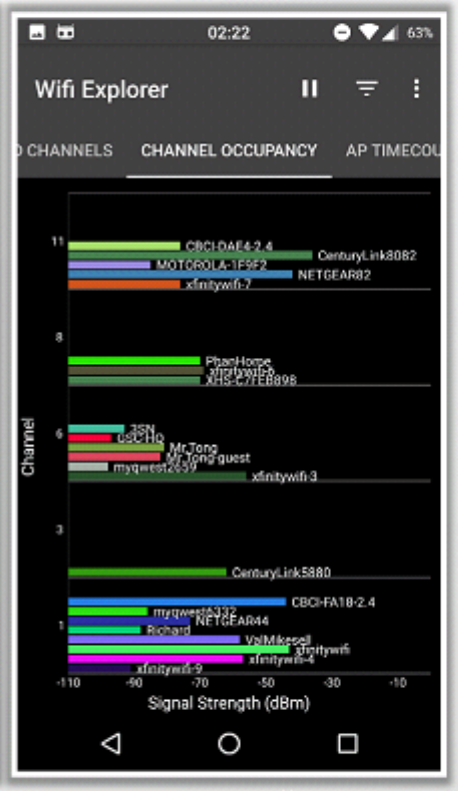
Ekahau HeatMapper
https://www.ekahau.com

Mobile-based Wi-Fi Discovery Tools

WifiExplorer

- WifiExplorer is an 802.11 network discovery tool -- also known as a Wi-Fi scanner which collects information about nearby wireless access points and displays the data in useful ways
- WifiExplorer uses 5 diagnostic views that collectively provide information about surrounding Wi-Fi networks





http://nutsaboutnets.com

WiFi Manager
https://kmansoft.com

OpenSignalMaps
https://opensignal.com

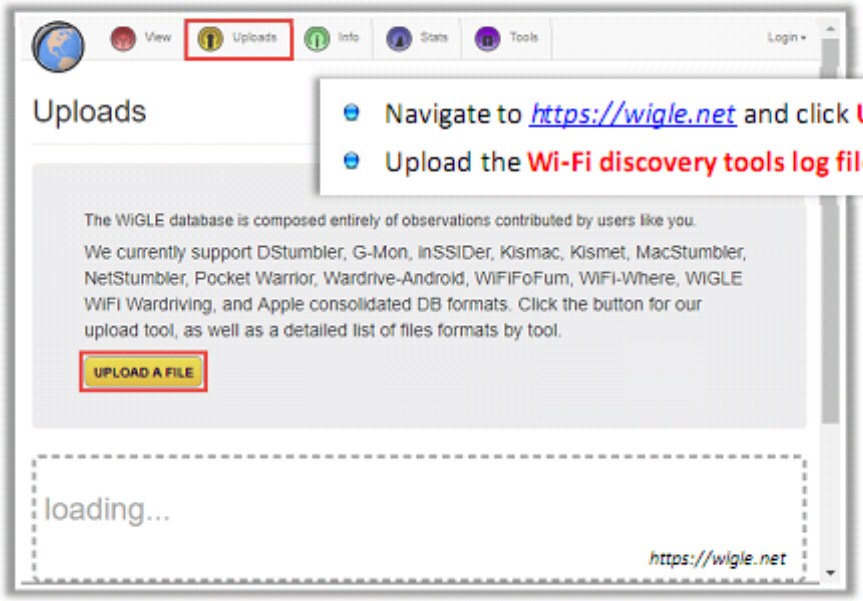
Network Signal Info Pro
http://www.kalbits-software.com

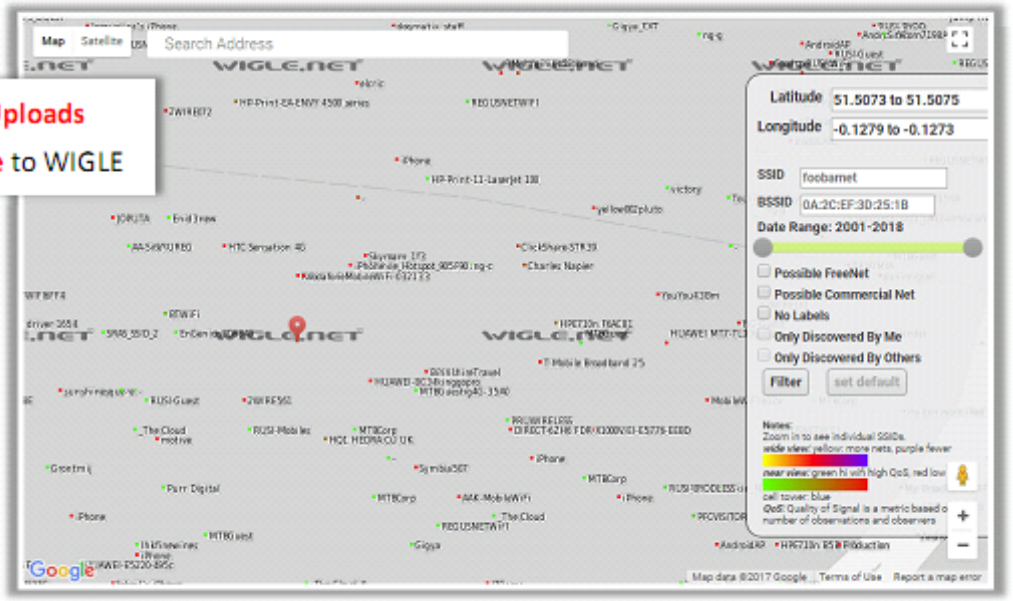
WiFiFoFum - WiFi Scanner
https://play.google.com

WiFinder
https://play.google.com

GPS Mapping

- Attackers create map of discovered Wi-Fi networks and **create a database** with statistics collected by Wi-Fi discovery tools
- GPS is used to **track the location** of the discovered Wi-Fi networks and the coordinates are uploaded to sites like **WiGLE**

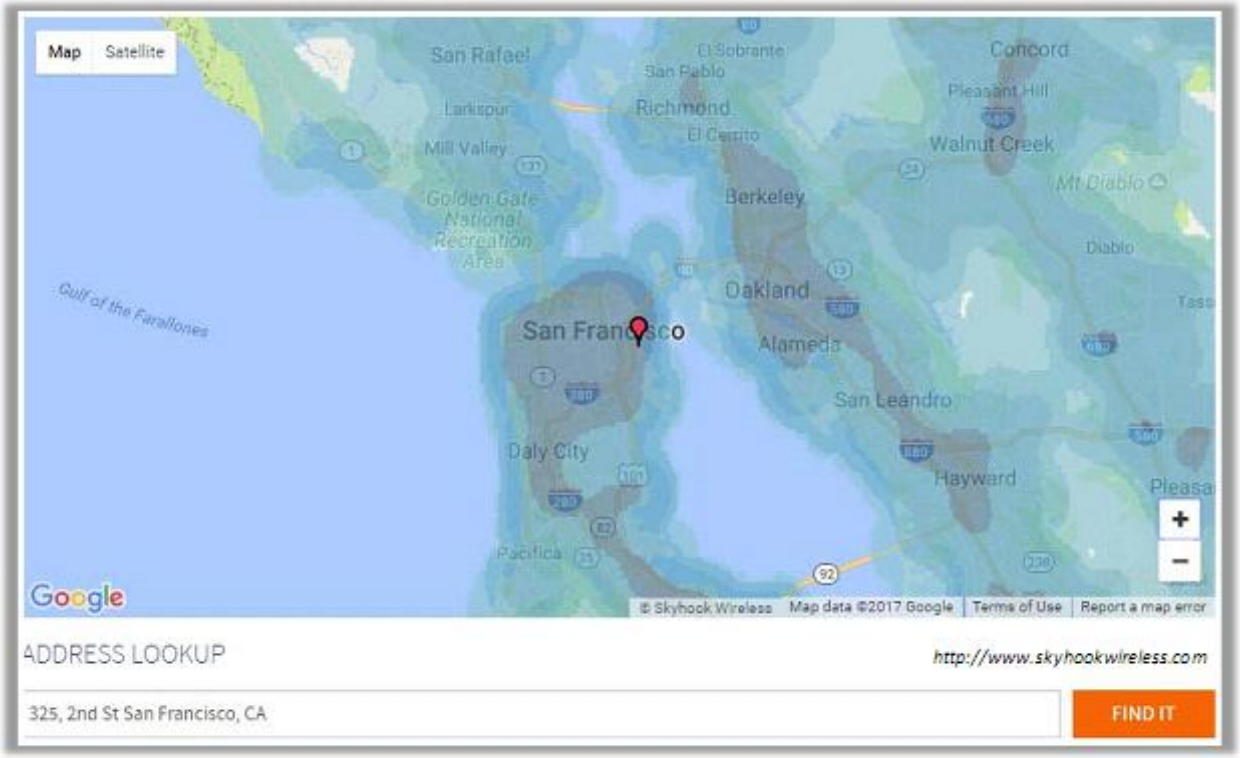




GPS Mapping Tools

Skyhook

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



- **Maptitude Mapping Software**
  http://www.caliper.com
- **ExpertGPS**
  https://www.expertgps.com
- **GPS Visualizer**
  http://www.gpsvisualizer.com
- **Mapwel**
  http://www.mapwel.eu
- **TrackMaker**
  http://www.trackmaker.com

Wi-Fi Hotspot Finder Tools

Wi-Fi Finder

Wi-Fi Finder is an android mobile application that can be used for finding free or paid public Wi-Fi hotspots **online** or **offline**

http://www.appsapk.com

- **Homedale::Wi-Fi / WLAN Monitor**
  http://www.the-sz.com
- **Avast Wi-Fi Finder**
  https://www.avast.com
- **Open WiFi Finder**
  https://play.google.com
- **Free WiFi Finder**
  https://play.google.com
- **Fing - Network Tools**
  https://play.google.com

How to Discover Wi-Fi Network Using Wardriving

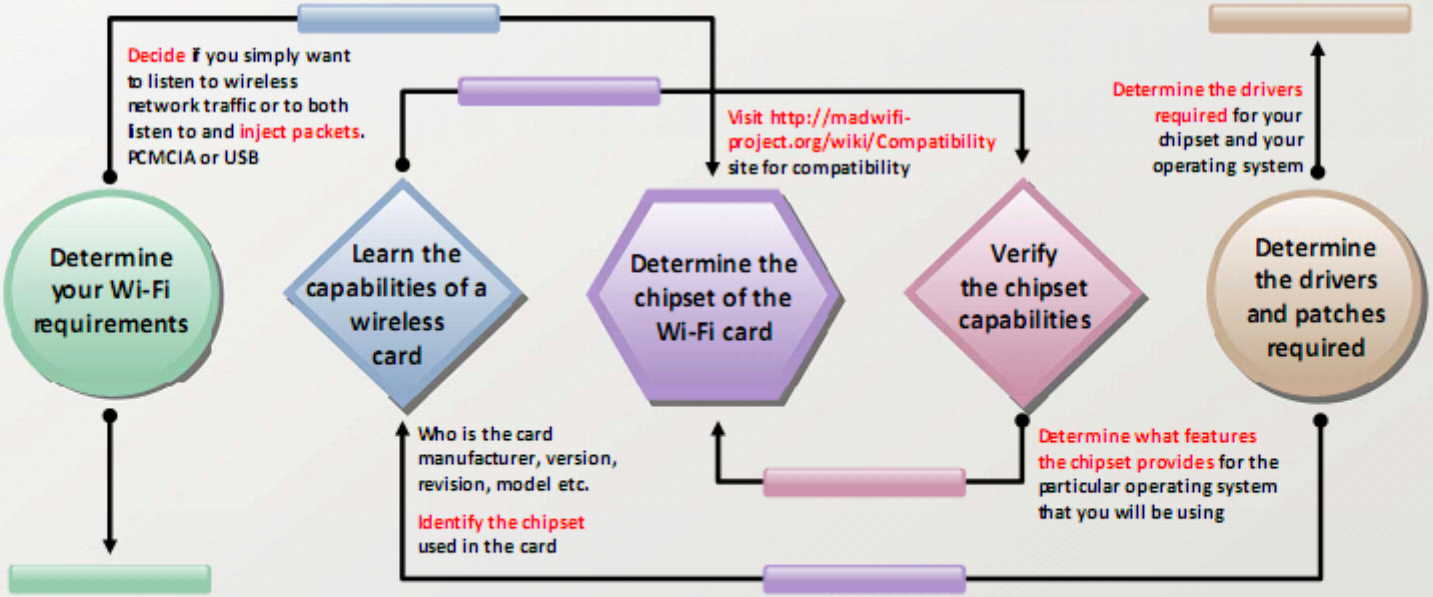
Step 1	Register with WIGLE and download map **packs of your area** to view the plotted access points on a geographic map
Step 2	Connect the antenna, GPS device to the laptop via a **USB serial adapter** and board on a car
Step 3	Install and **launch NetStumbler** and **WIGLE** client software and turn on the GPS device
Step 4	Drive the car at speeds of **35 mph** or below (At higher speeds, Wi-Fi antenna will not be able to detect Wi-Fi spots)
Step 5	Capture and save the **NetStumbler log files** which contains GPS coordinates of the access points
Step 6	Upload this log file to WIGLE, which will then automatically plot the **points onto a map**

Wireless Traffic Analysis

- Wireless traffic analysis enables attackers to **identify vulnerabilities** and susceptible victims in a target wireless network
- This helps in **determining the appropriate strategy** for a successful attack
- Attackers analyze a wireless network to **determine broadcasted SSID**, presence of multiple access points, possibility of recovering SSIDs, authentication method used, WLAN encryption algorithms, etc.
- Attackers use **Wi-Fi packet sniffing tools** such as Wireshark, SteelCentral Packet Analyzer, OmniPeek Enterprise, CommView for Wi-Fi, etc. to capture and analyze the traffic of a target wireless network

Choosing the Right Wi-Fi Card

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

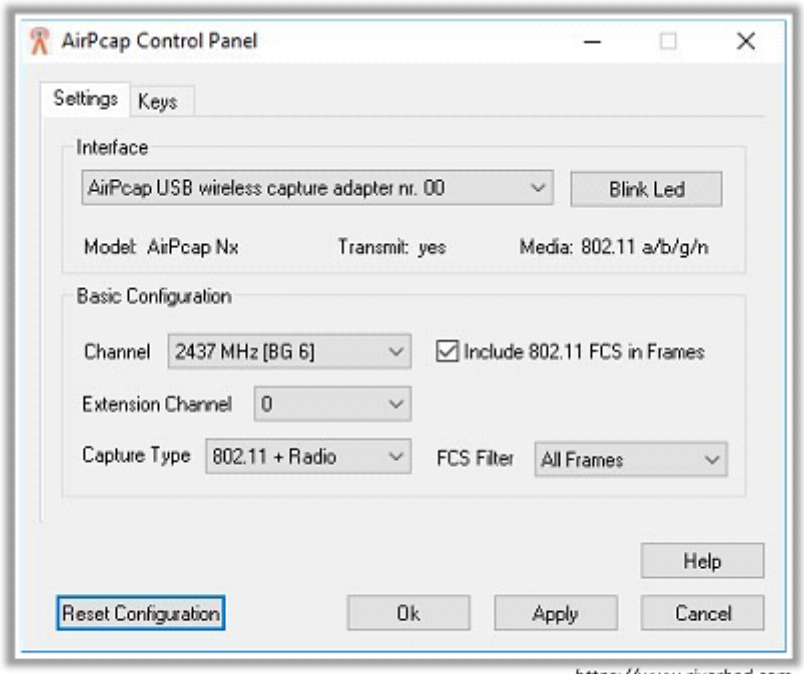


Wi-Fi USB Dongle: AirPcap

- 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**

Features

- 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 & Able**, and **Wireshark** tools
- **AirPcapReplay**, included in the AirPcap Software Distribution, replays 802.11 network traffic that is contained in a trace file

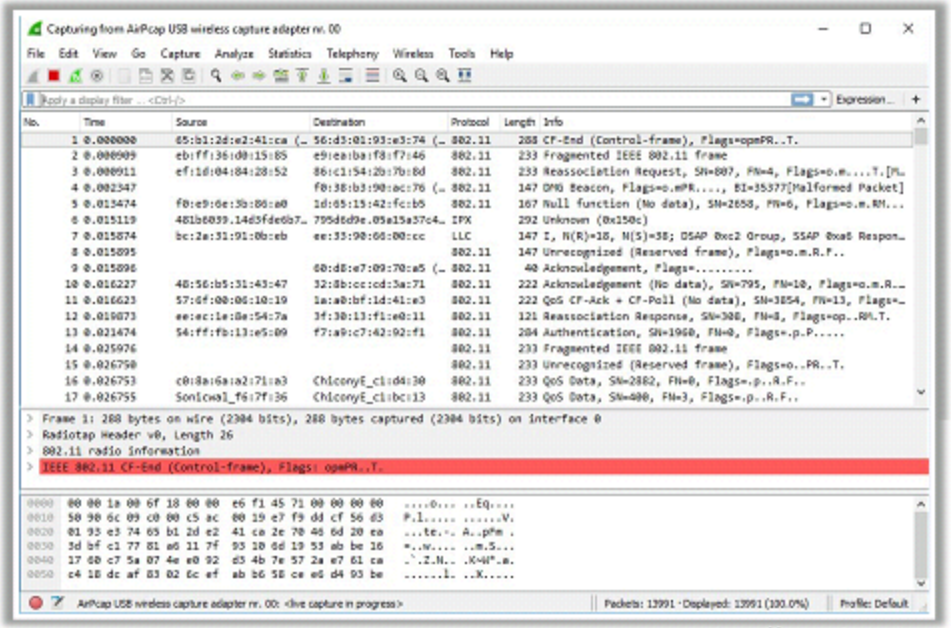


https://www.riverbed.com

Wi-Fi Packet Sniffer

Wireshark with AirPcap

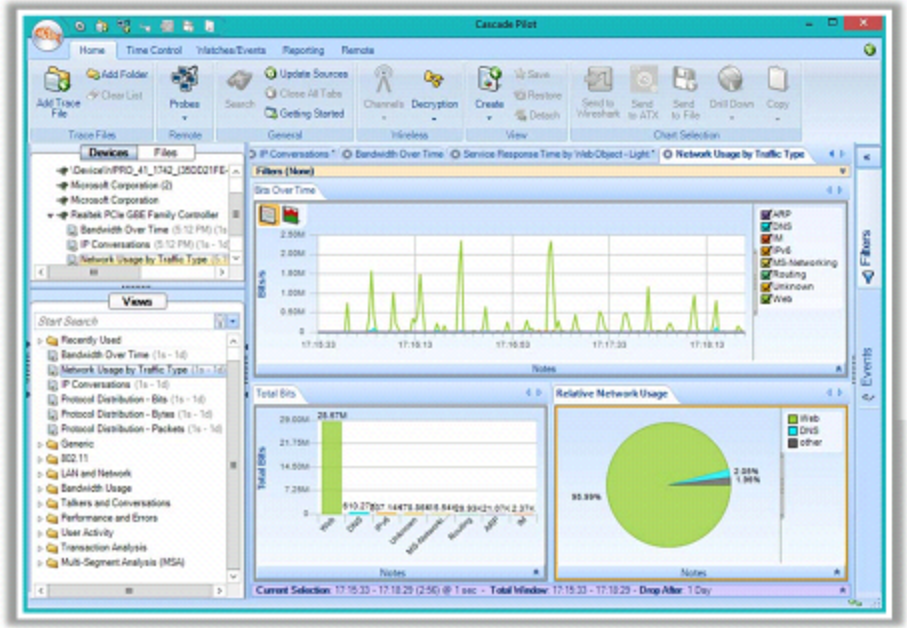
- Wireshark allows attacker to **read/capture live data** from Ethernet, Token-Ring, FDDI, serial (PPP and SLIP), 802.11 wireless LAN, ATM connections, etc.



https://www.wireshark.org

SteelCentral Packet Analyzer

- SteelCentral Packet Analyzer measures wireless channel utilization and helps in **identifying rogue wireless networks and stations**

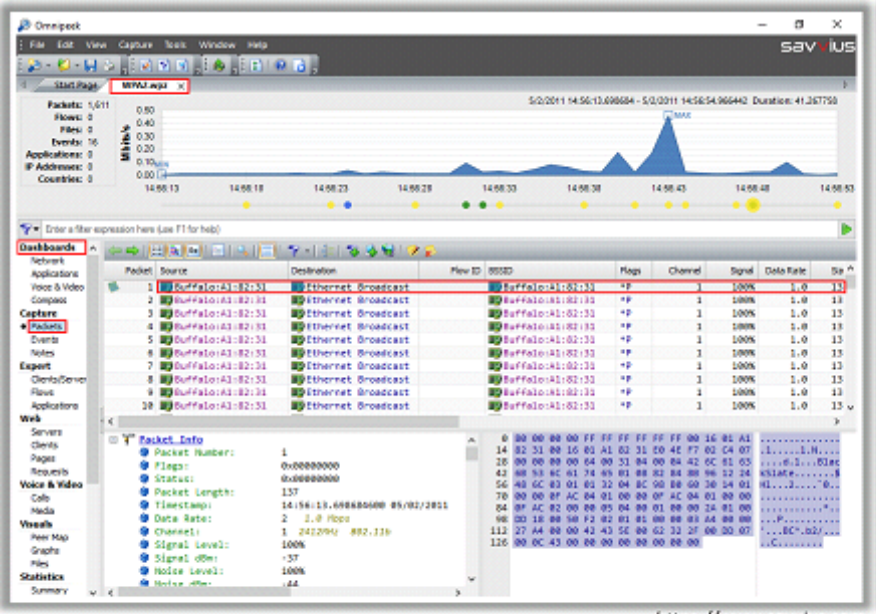


https://www.riverbed.com

Wi-Fi Packet Sniffer (Cont'd)

OmniPeek Enterprise

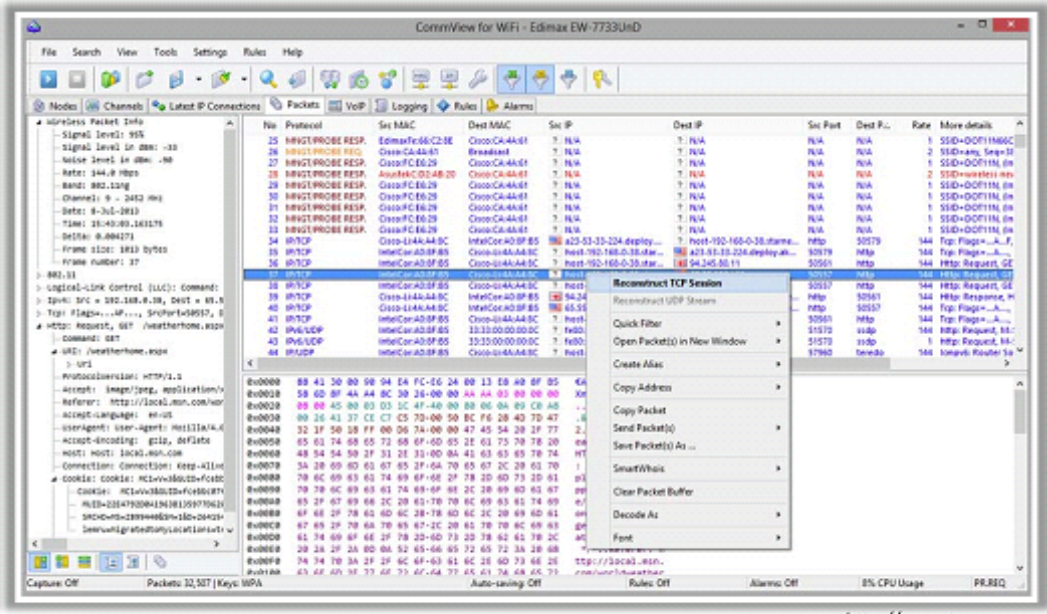
- OmniPeek Enterprise offers real-time visibility and analysis of the network traffic and provides a comprehensive view of all wireless network activity showing each wireless network, the APs comprising that network, and the users connected to each AP



https://www.savvius.com

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

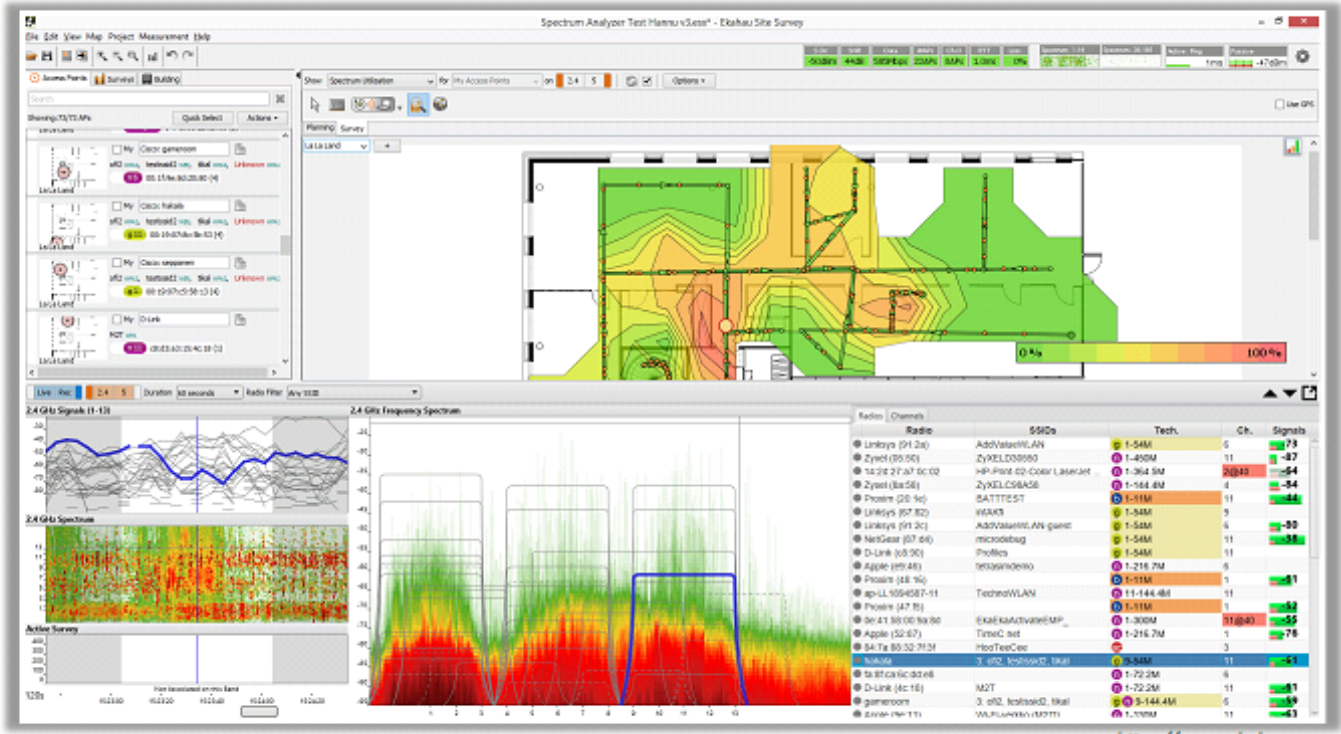


https://www.tamos.com

Perform Spectrum Analysis

- Spectrum analysis of wireless network helps an attacker to **actively monitor the spectrum usage in a particular area** and detect the spectrum signal of target network
- It helps the attacker to **measure the power of the spectrum** of known and unknown signals
- Attackers use spectrum analysis tools such as **Ekahau Spectrum Analyzer** to perform spectrum analysis

Ekahau Spectrum Analyzer | It provides powerful on-the-spot and post-site analysis capabilities and combines both Wi-Fi and spectrum information into easy-to-read displays



https://www.ekahau.com

Launch Wireless Attacks: 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

http://www.aircrack-ng.org

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

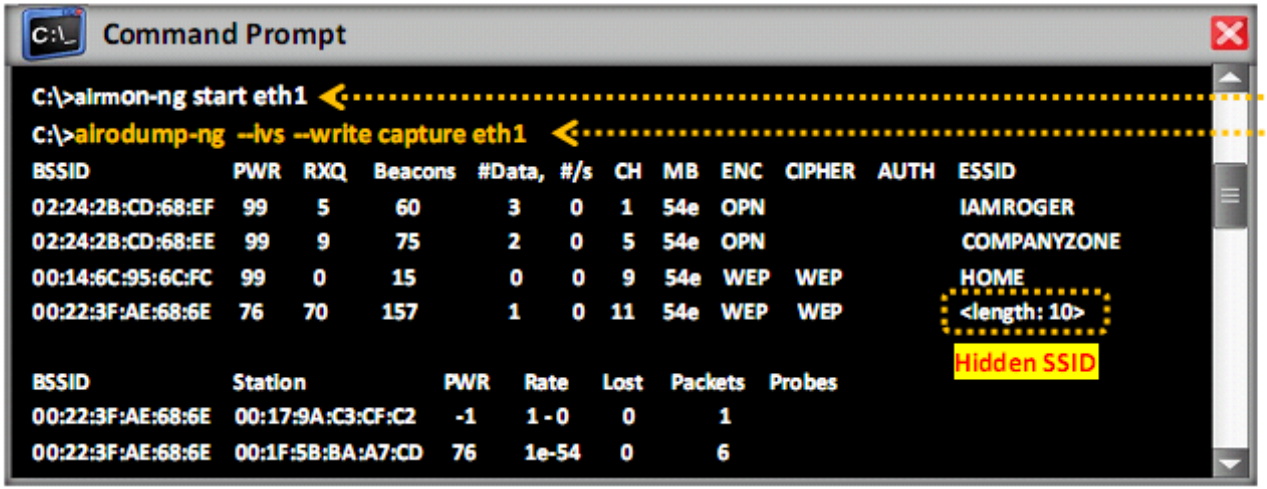
Tkiptun-ng

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

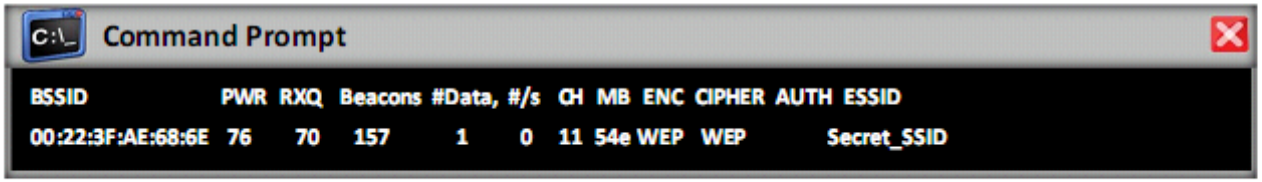
Launch Wireless Attacks: How to Reveal Hidden SSIDs



Step 1: Run airmon-ng in monitor mode

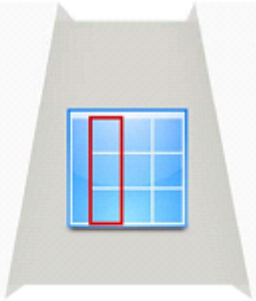
Step 2: Start airodump to discover SSIDs on interface

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



Step 4: Switch to airodump to see the revealed SSID

Launch Wireless Attacks: 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

Command Prompt

```
C:\>aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0
Waiting for a data packet...
Read 96 packets...
      Size: 120, FromDS: 1, ToDS: 0 (WEP)
      BSSID  =  00:14:6C:7E:40:80
      Dest. MAC  =  00:0F:B5:AB:CB:9D
      Source MAC  =  00:D0:CF:03:34:8C

0x0000:  0842 0201 000f b5ab cb9d 0014 6c7e 4080  .B..........l~@.
0x0010:  00d0 cf03 348c e0d2 4001 0000 2b62 7a01  ....4...@...+bz.
0x0020:  6d6d b1e0 92a8 039b ca6f cacb 5364 6e16  mm.......o..Sdn.
0x0030:  a21d 2a70 49cf eef8 f9b9 279c 9020 30c4  ..*pI.....'.. 0.
0x0040:  7013 f7f3 5953 1234 5727 146c eeaa a594  p...YS.4W'.l....
0x0050:  fd55 66a2 030f 472d 2682 3957 8429 9ca5  .Uf...G-&.9W.)..
0x0060:  517f 1544 bd82 ad77 fe9a cd99 a43c 52a1  Q .D...w.....<R.
0x0070:  0505 933f af2f 740e                      ...?./t.
Use this packet ? y
```

Command Prompt

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

PRGA is stored in the file

How to Launch MAC Spoofing Attack

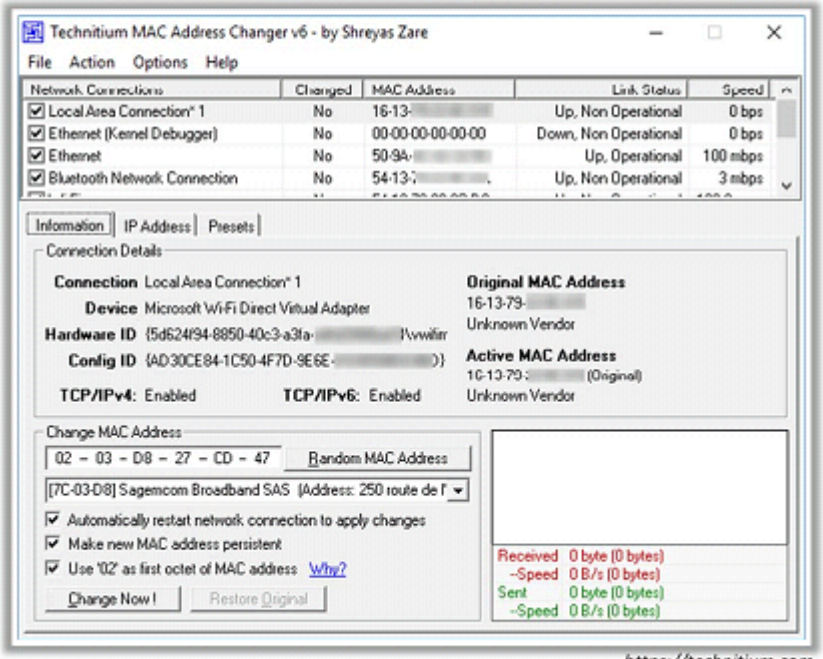
- In MAC spoofing, attackers **change the MAC address** to that of an authenticated user to bypass the MAC filtering configured in an access point
- To spoof a MAC address, the attacker needs to set the value returned from ifconfig to **another hex value** in the format of aa:bb:cc:dd:ee:ff
- Attacker use MAC spoofing tools such as **Technitium MAC Address Changer**, MAC Address Changer, etc. to change the MAC address

Linux Shell

```
[root@localhost root]# ifconfig wlan0 down        <-- Logging as root and disable the network interface
[root@localhost root]# ifconfig wlan0 hw ether 02:25:ab:4c:2a:bc   <-- Enter the new MAC address
[root@localhost root]# ifconfig wlan0 up          <-- Bring the interface back up
```

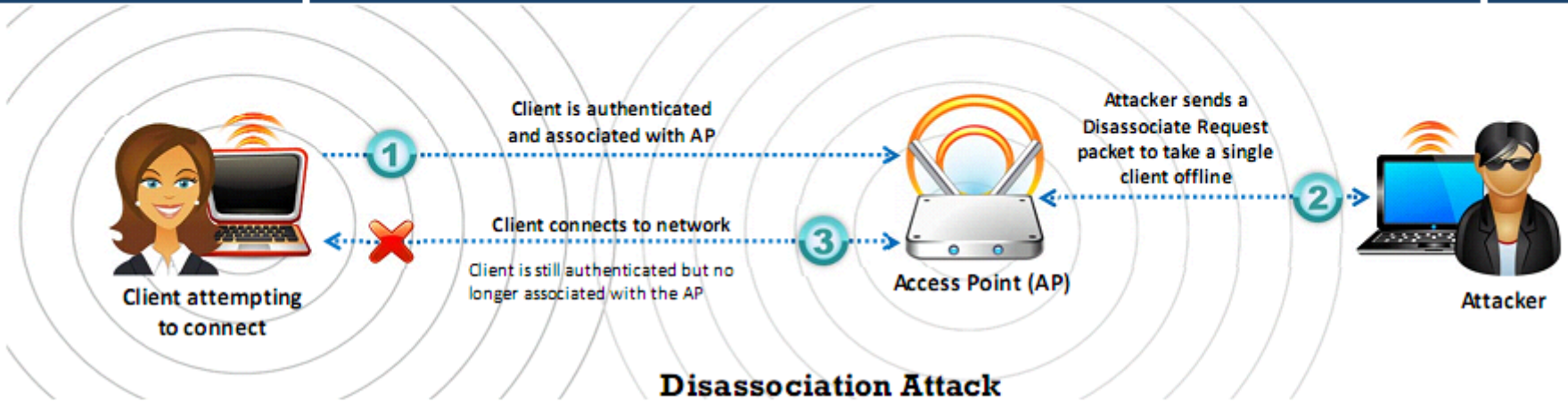
Technitium MAC Address Changer

Technitium MAC Address Changer allows you to change (spoof) **Media Access Control** (MAC) Address of your **Network Interface Card** (NIC) instantly

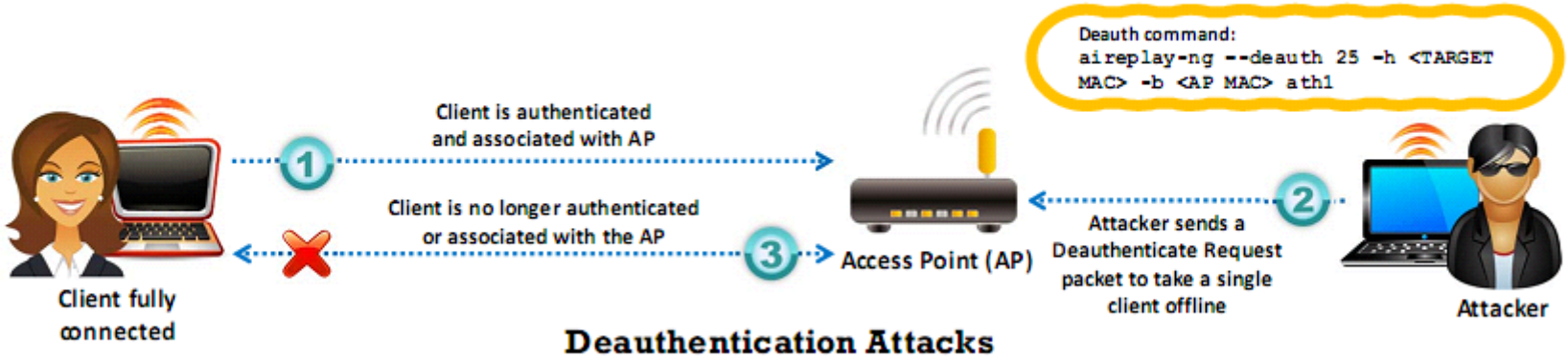


https://technitium.com

Denial-of-Service: Disassociation and Deauthentication Attacks



Disassociation Attack



Deauthentication Attacks

Launch Wireless Attacks: Man-in-the-Middle Attack

Attacker sniffs the victim's wireless parameters (the MAC address, ESSID/BSSID, number of channels)

Sends a DEAUTH request to the victim with the spoofed source address of the victim's AP

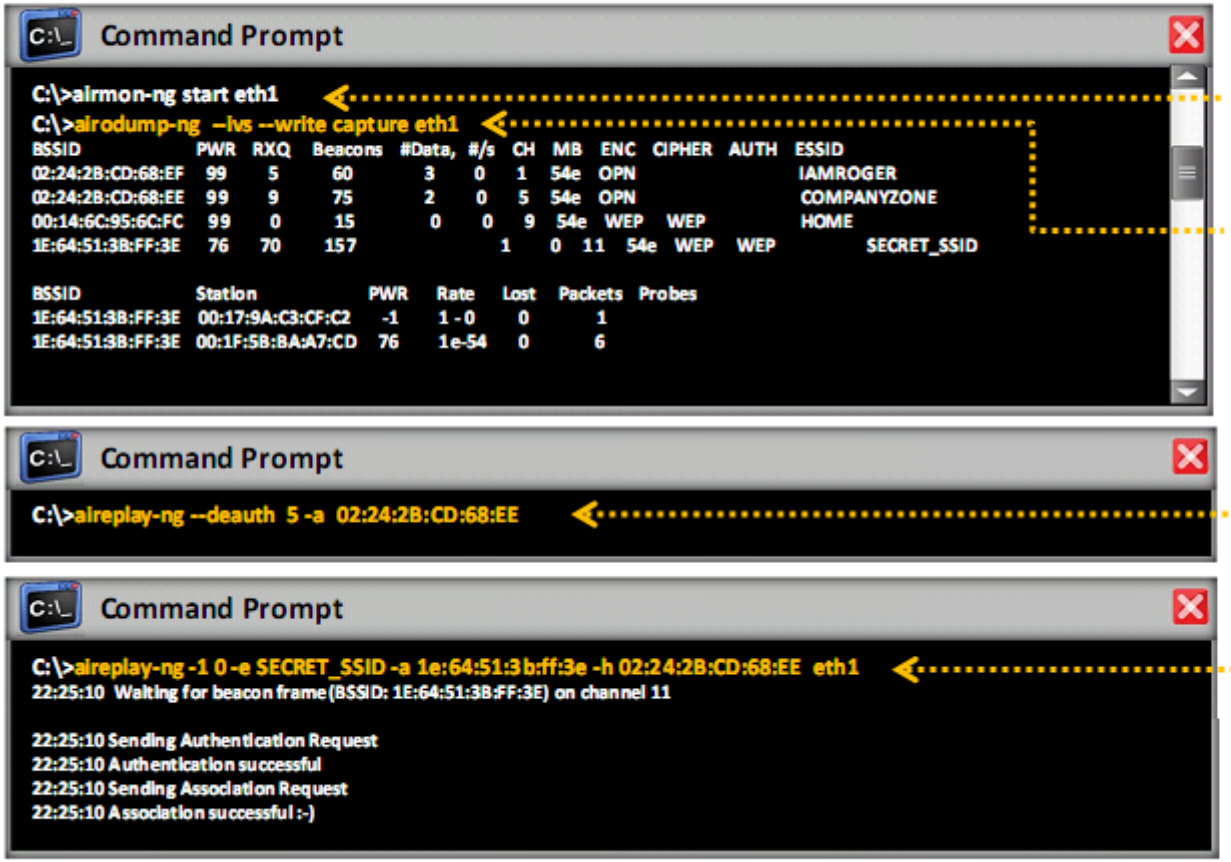
Victim is deauthenticated and starts to search all channels for a new valid AP

Attacker sets a forged AP on a new channel with the original MAC address (BSSID) and ESSID of the victim's AP

After the victim's successful association to the forged AP, the attacker spoofs victim to connect to the original AP

Attacker sits in between the access point and the victim and listens all the traffic

Launch Wireless Attacks: MITM Attack Using Aircrack-ng



Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump to discover SSIDs on interface

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

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

Launch Wireless Attacks: Wireless ARP Poisoning Attack

1. Attacker spoofs the MAC address of Jessica's Wireless Laptop and attempts to authenticate to AP1

2. AP1 sends updated MAC address info to the network routers and switches, which in turn update their routing and switching tables

3. Traffic now destined from the network backbone to Jessica's system is no longer sent to AP2

Launch Wireless Attacks: Rogue Access Points

- Rogue AP **provides backdoor access** to the target wireless network

Scenarios for Rogue AP Installation and Setup

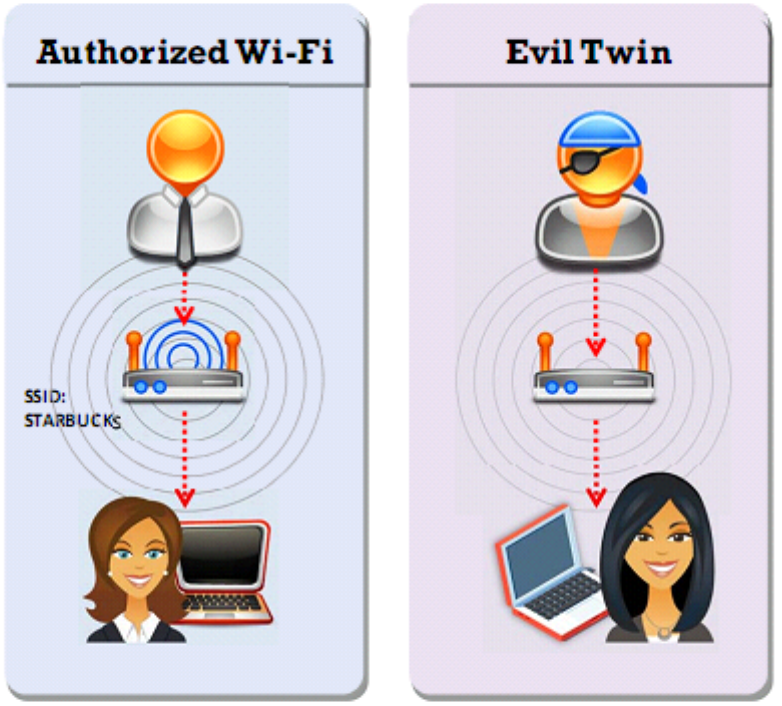
- **Compact, pocket-sized rogue AP** device plugged into an Ethernet port of corporate network
- **Rogue access point device** connected to corporate networks over a Wi-Fi link
- **USB-based rogue access point** device plugged into a corporate machine
- **Software-based rogue access point** running on a corporate Windows machine

Steps to Deploy Rogue Access Point

- 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 short period

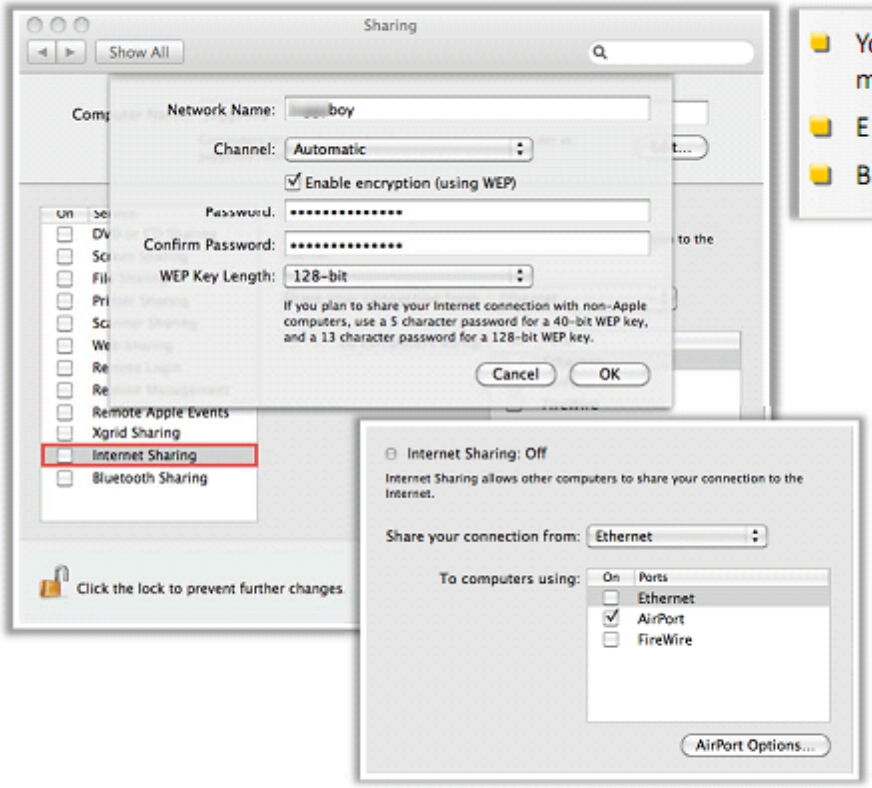
Launch Wireless Attacks: Evil Twin

- 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



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)



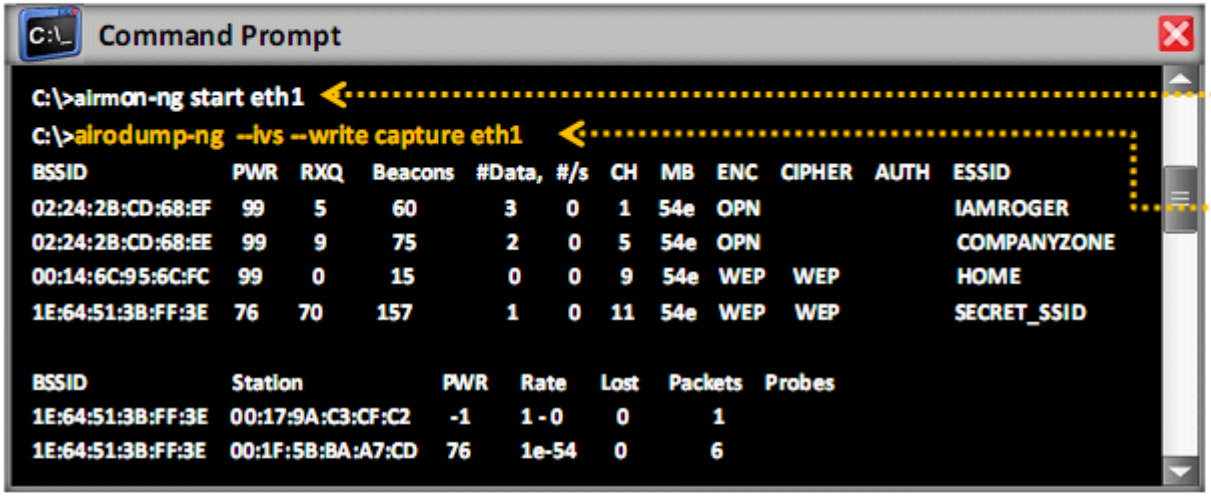
- You will need a laptop with **Internet connectivity** (3G or wired connection) and a mini access point
- Enable **Internet Connection Sharing** in Windows OS or **Internet Sharing** in Mac OS X
- Broadcast your Wi-Fi connection and run a **sniffer program** to capture passwords

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.

Crack Wi-Fi Encryption: How to Break WEP Encryption

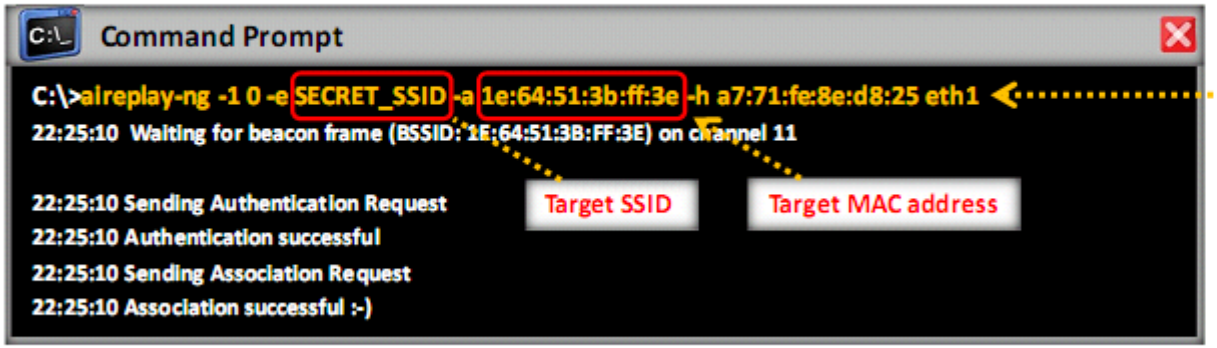
- Start the wireless interface in **monitor mode** on the specific access point channel
- Test the **injection capability** of the wireless device to the access point
- Use a tool such as aireplay-ng to do a **fake authentication** with the access point
- Start Wi-Fi sniffing tool such as airodump-ng or Cain & Abel with a BSSID filter to **collect unique IVs**
- Start a Wi-Fi packet encryption tool such as aireplay-ng in ARP **request replay mode to inject packets**
- Run a cracking tool such as Cain & Abel or aircrack-ng to **extract encryption key** from the IVs

Crack Wi-Fi Encryption: How to Crack WEP Using Aircrack-ng



Step 1: Run airmon-ng in monitor mode

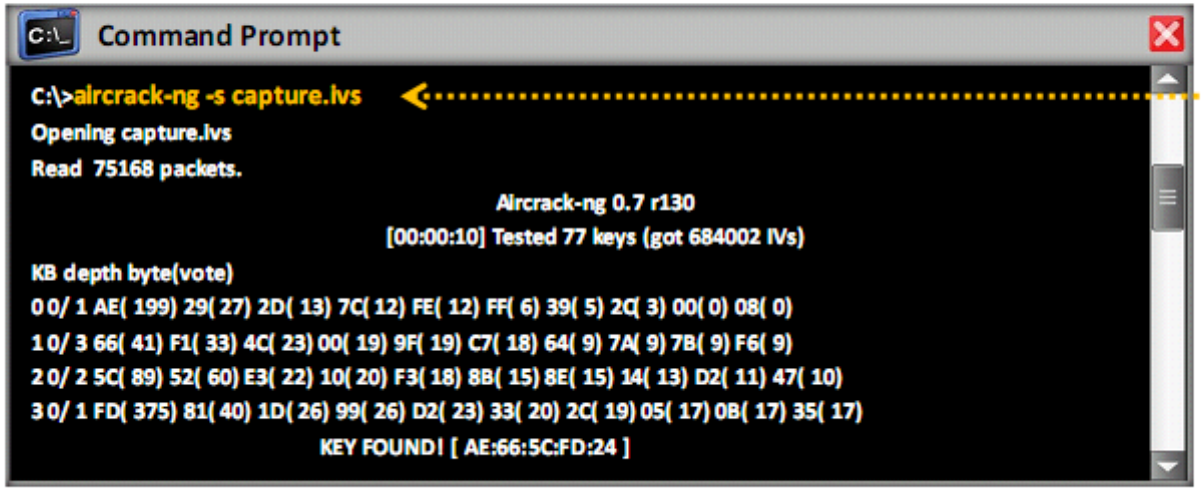
Step 2: Start airodump to discover SSIDs on interface and keep it running.
Your capture file should contain more than 50,000 IVs to successfully crack the WEP key.



Step 3: Associate your wireless card with target access point

Crack Wi-Fi Encryption: How to Crack WEP Using Aircrack-ng (Cont'd)

Step 4: Inject packets using aireplay-ng to generate traffic on target access point



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

Crack Wi-Fi Encryption: 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

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 aireplay; you should be able to re-authenticate in a few seconds then attempt to Dictionary Brute Force the PMK

Brute-Force WPA Keys

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

Crack Wi-Fi Encryption: How to Crack WPA-PSK Using Aircrack-ng

Step 1 Monitor wireless traffic with airmon-ng

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

Step 2 Collect wireless traffic data with airodump-ng

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

Command Prompt

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

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

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

Step 3: 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)

Command Prompt

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

Step 4: Run the capture file through aircrack-ng

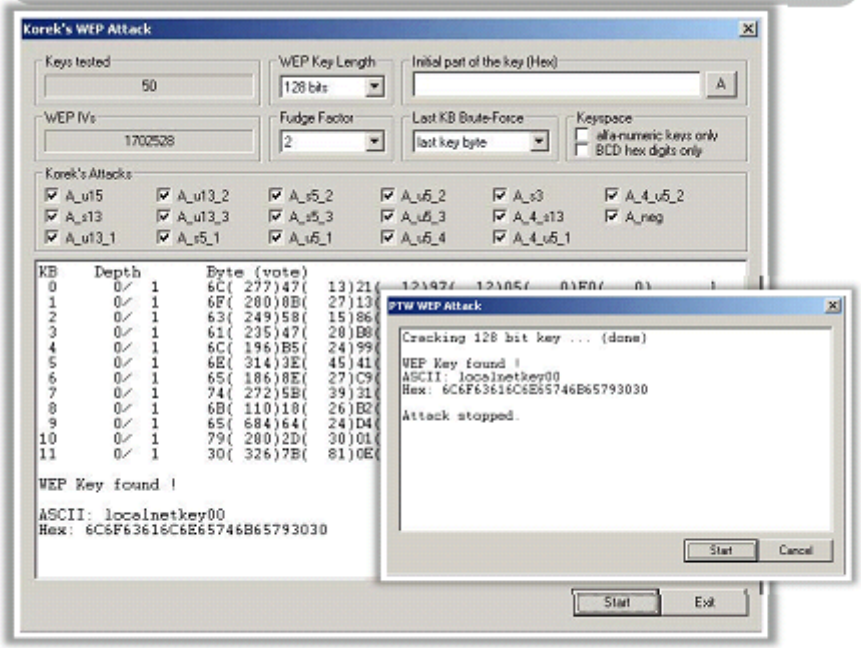
Command Prompt

```
C:\>aircrack-ng.exe -a 2 -w capture.cap
Opening capture.cap
Read 607 packets
#  BSSIS          ESSID         Encryption
102:24:2B:CD:68:EE  COMPANYZONE      WPA <1 handshake>
Choosing first network as target.
Opening ../capture.cap
Pending packets, please wait...
                                Aircrack-ng 0.7 r130
                            [00:00:03] 230 keys tested (73.41 k/s)
                                KEY FOUND! [ passkey ]
      Master Key     : CD D7 9A 5A CF B0 70 C7 E9 D1 02 3B 87 02 85 D6
                       39 E4 30 B3 2F 31 AA 37 AC 82 5A 55 B5 55 24 EE
      Transcient Key : 33 55 0B FC 4F 24 84 F4 9A 38 B3 D0 89 83 D2 49
                       73 F9 DE 89 67 A6 6D 2B 8E 46 2C 07 47 6A CE 08
                       AD FB 65 D6 13 A9 9F 2C 65 E4 A6 08 F2 5A 67 97
                       D9 6F 76 5B 8C D3 DF 13 2F BC DA 6A 6E D9 62 CD
      EAPOL HMAC     : 52 27 B8 3F 73 7C 45 A0 05 97 69 5C 30 78 60 BD
```

WEP Cracking and WPA Brute Forcing Using Cain & Abel

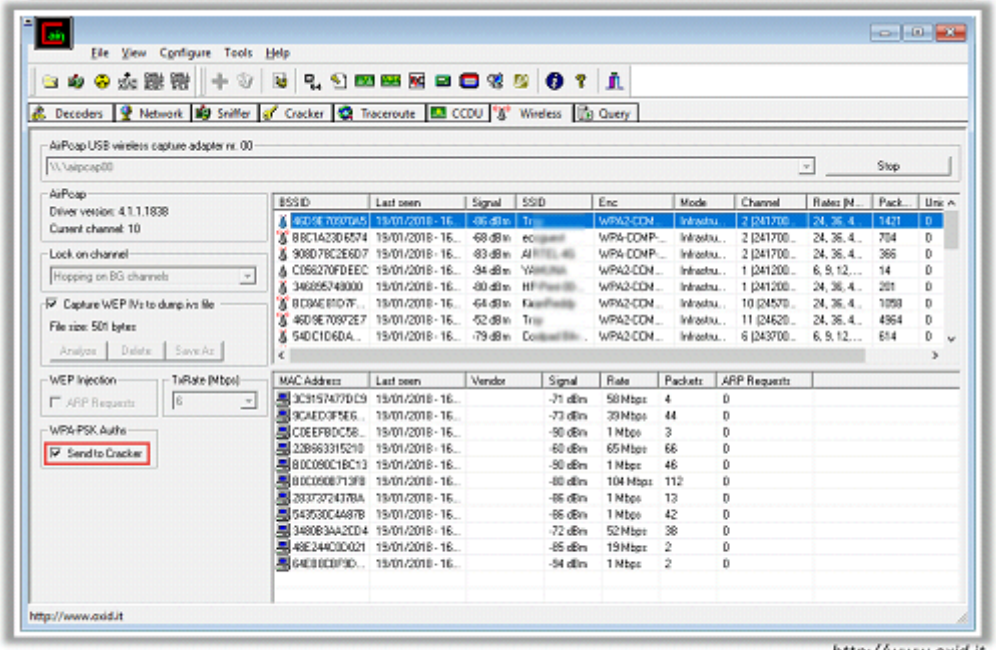
WEP Cracking

WEP Cracker utility in Cain implements **statistical cracking** and **PTW cracking** methods for the recovery of a WEP Key



WPA Brute Forcing

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



http://www.oxid.it

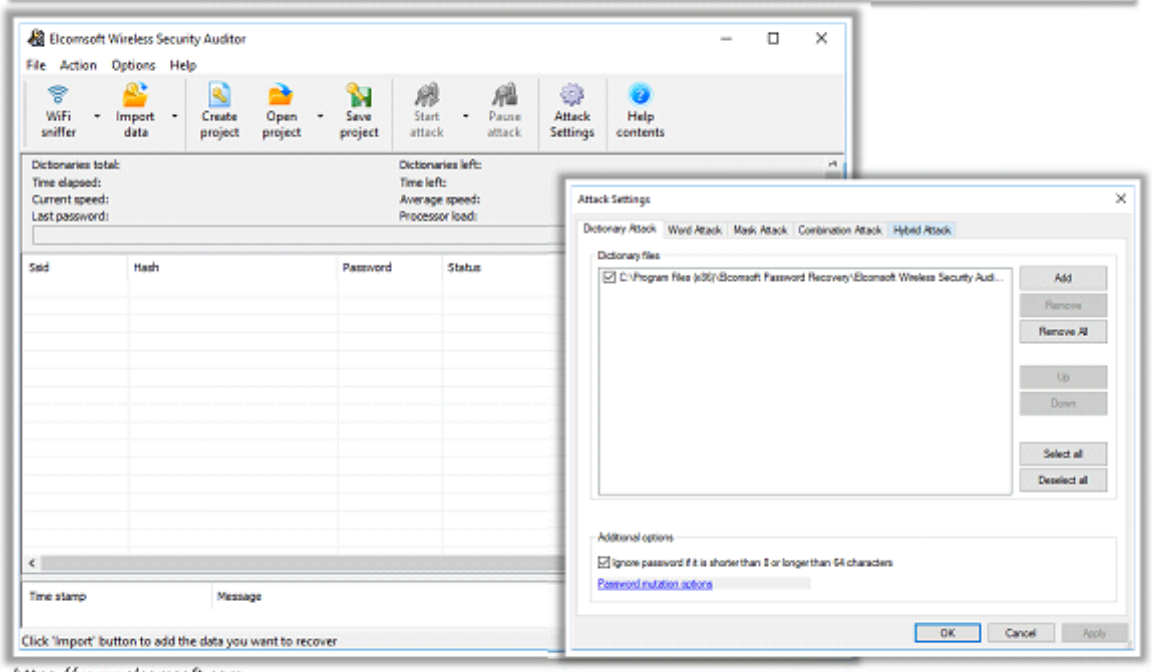
Module Flow

1. Wireless Concepts
2. Wireless Encryption
3. Wireless Threats
4. Wireless Hacking Methodology
5. Wireless Hacking Tools
6. Bluetooth Hacking
7. Countermeasures
8. Wireless Security Tools
9. Wireless Pen Testing

WEP/WPA Cracking Tools

Elcomsoft Wireless Security Auditor

It allows attacker to **break into a secured Wi-Fi network** by sniffing wireless traffic and running an attack on the network's WPA/WPA2-PSK password



https://www.elcomsoft.com

WepAttack
http://wepattack.sourceforge.net

Wesside-ng
https://www.aircrack-ng.org

coWPAtty
http://www.willhackforsushi.com

Reaver Pro
https://code.google.com

WepCrackGui
https://sourceforge.net

WEP/WPA Cracking Tool for Mobile

WIBR – WIFI BRUTEFORCE HACK

- WIBR+ is an application for testing of security of the **WPA/WPA2 PSK Wi-Fi networks**
- It **discovers weak password** using dictionary and brute force attacks

https://auradesign.cz

- **WIFI WPS WPA TESTER** *https://play.google.com*
- **iWep PRO** *https://play.google.com*
- **AndroDumpper (WPS Connect** *https://play.google.com*
- **Wifi Password WPA-WEP FREE** *https://play.google.com*
- **WPS WPA WiFi Tester** *https://play.google.com*

Wi-Fi Sniffer

Kismet

It is an 802.11 Layer2 **wireless network detector**, sniffer, and intrusion detection system which **identifies networks** by passively collecting packets

https://www.kismetwireless.net

Tcpdump
(http://www.tcpdump.org

SmartSniff
http://www.nirsoft.net

Acrylic WiFi Professional
https://www.acrylicwifi.com

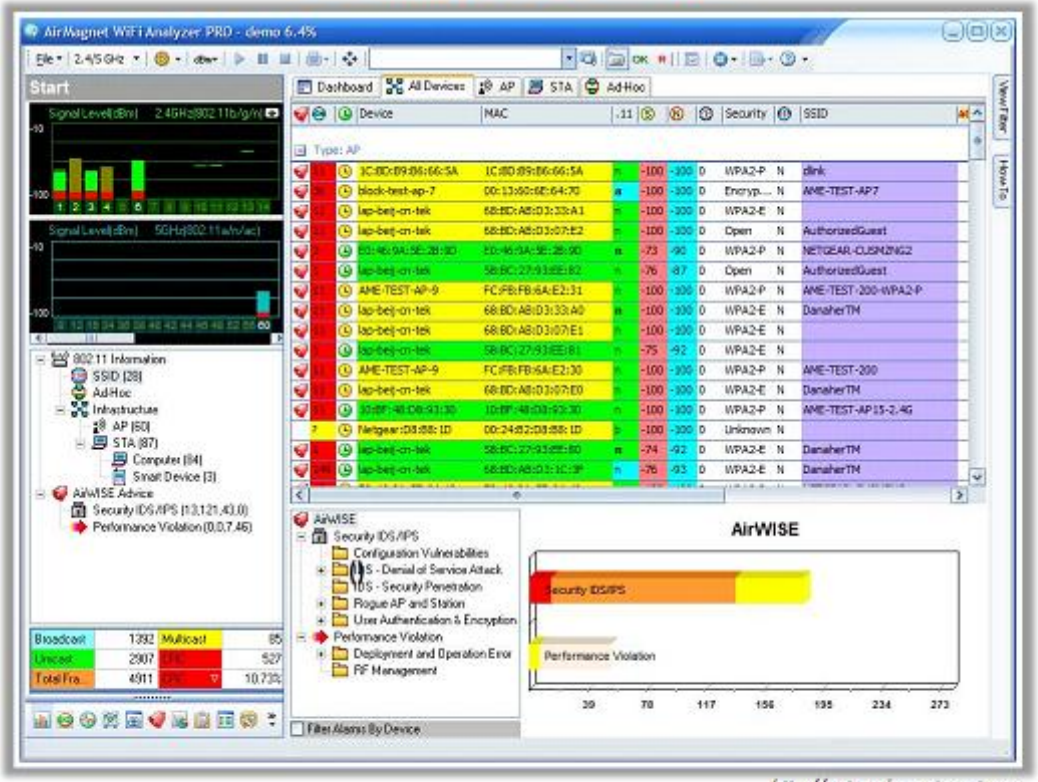
NetworkMiner
http://www.netresec.com

WifiScanner
http://wifiscanner.sourceforge.net

Wi-Fi Traffic Analyzer Tools

AirMagnet WiFi Analyzer

It is a Wi-Fi networks traffic **auditing** and **troubleshooting** tool which provides real-time accurate, independent and reliable Wi-Fi analysis of 802.11a/b/g/n and ac wireless networks, including 3 X 3 802.11ac wireless network analysis without missing any traffic



http://enterprise.netscout.com

- **Capsa Network Analyzer**
  http://www.colasoft.com
- **PRTG Network Monitor**
  https://www.paessler.com
- **Observer Analyzer**
  https://www.viavisolutions.com
- **Sniffer Portable Professional Analyzer**
  https://www.netscout.com
- **Xirrus Wi-Fi Inspector**
  https://www.xirrus.com

Other Wireless Hacking Tools

Wardriving Tools

- Airbase-ng — *https://aircrack-ng.org*
- MacStumbler — *http://www.macstumbler.com*
- AirFart — *https://sourceforge.net*
- 802.11 Network Discovery Tools — *https://sourceforge.net*
- G-MoN — *https://play.google.com*

RF Monitoring Tools

- Sentry Edge II — *https://www.tek.com*
- NetworkManager — *https://wiki.gnome.org*
- xosview — *http://xosview.sourceforge.net*
- CPRIAdvisor — *https://www.viavisolutions.com*
- sigX — *http://www.kratoscomms.com*

Raw Packet Capturing Tools

- WirelessNetView — *http://www.nirsoft.net*
- PRTG Network Monitor — *https://www.telerik.com*
- Tcpdump — *http://www.tcpdump.org*
- RawCap — *http://www.netresec.com*
- Airodump-ng — *https://www.aircrack-ng.org*

Spectrum Analyzing Tools

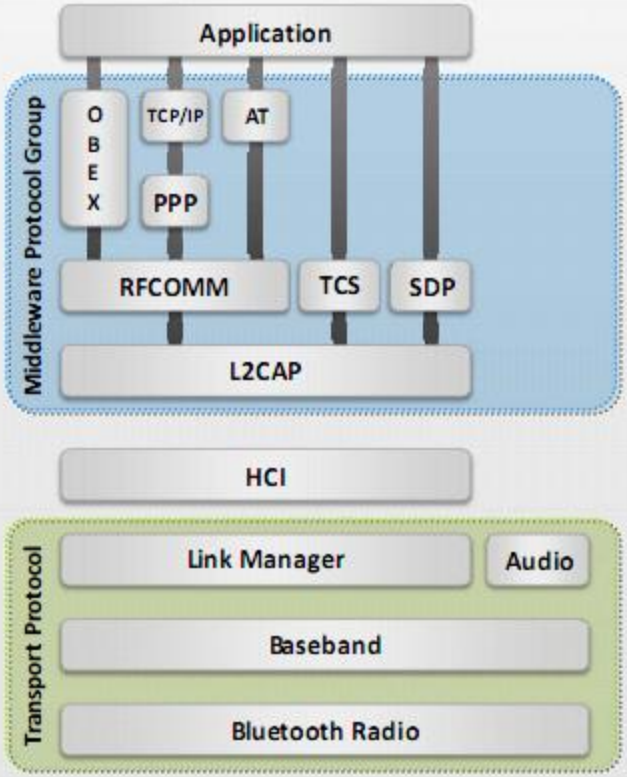
- Wi-Spy and Chanalyzer — *https://www.metageek.com*
- AirMagnet Spectrum XT — *http://enterprise.netscout.com*
- Cisco Spectrum Expert — *https://www.cisco.com*
- RSA306B USB Spectrum Analyzer — *https://www.tek.com*
- AirSleuth-Pro — *http://nutsaboutnets.com*

Module Flow

1. Wireless Concepts
2. Wireless Encryption
3. Wireless Threats
4. Wireless Hacking Methodology
5. Wireless Hacking Tools
6. Bluetooth Hacking
7. Countermeasures
8. Wireless Security Tools
9. Wireless Pen Testing

Bluetooth Stack

- Bluetooth is a short-range wireless communication technology that **replaces the cables connecting portable or fixed devices** while maintaining high levels of security
- It allows devices to **share data** over short distances



Bluetooth Modes

Discoverable modes

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 Hacking

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

Bluetooth Attacks

Bluesmacking

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

Bluejacking

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

Blue Snarfing

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

BlueSniff

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

Bluebugging

Remotely accessing the **Bluetooth-enabled** devices and using its features

BluePrinting

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

MAC Spoofing Attack

Intercepting data intended for other Bluetooth-enabled devices

Man-in-the-Middle/ Impersonation Attack

Modifying data between Bluetooth-enabled devices communicating in a Piconet

Bluetooth Threats

Leaking Calendars and Address Books

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

Remote Control

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

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

Social Engineering

Attackers trick Bluetooth users to lower security or disable authentication for Bluetooth connections in order to pair with them and steal information

Sending SMS Messages

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

Malicious Code

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

Causing Financial Losses

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

Protocol Vulnerabilities

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

How to BlueJack a Victim

- Bluejacking is the activity of sending **anonymous messages** over Bluetooth to Bluetooth-enabled devices such as laptops, mobile phones, etc. via the **OBEX** protocol

STEP 1

- **Select an area** with plenty of mobile users, like a café, shopping center, etc.
- **Go to contacts** in your address book (You can delete this contact entry later)

STEP 2

- **Create a new contact** on your phone address book
- **Enter the message** into the name field

  Ex: "Would you like to go on a date with me?"

STEP 3

- **Save the new contact** with the name text and without the telephone number
- **Choose "send via Bluetooth"**. These searches for any Bluetooth device within range

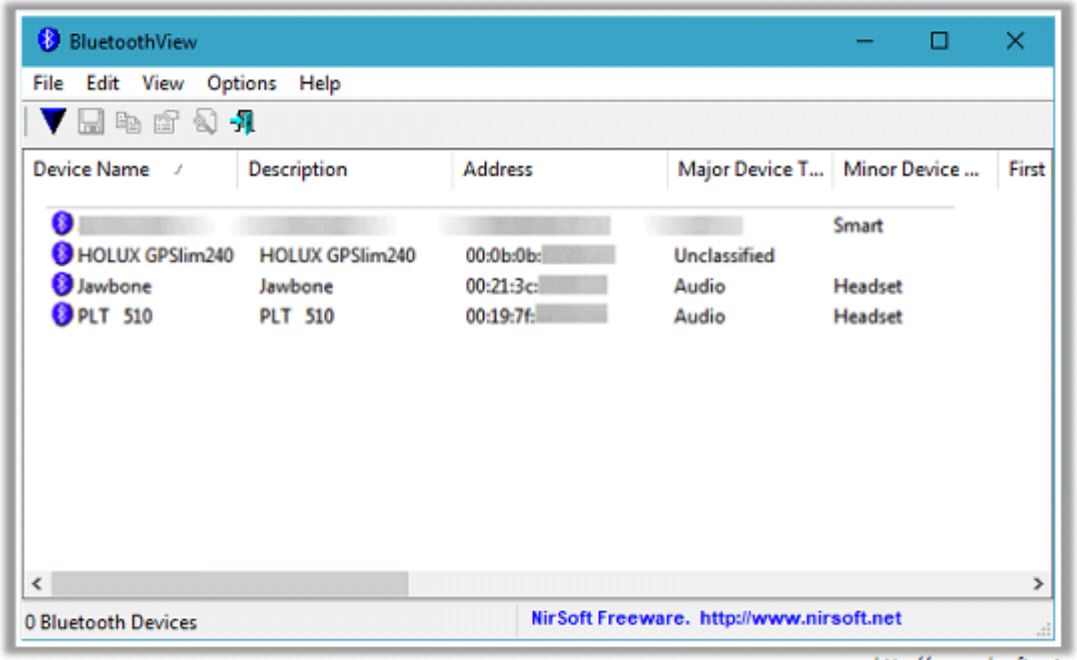
STEP 4

- **Choose one phone** from the list discovered by Bluetooth and send the contact
- You will get the message "**card sent**" and then listen for the SMS message tone of your victim's phone

Bluetooth Hacking Tools

BluetoothView

It monitors the activity of Bluetooth devices around you and displays the following information like Device Name, Bluetooth Address, Major Device Type, Minor Device Type, First Detection Time, Last Detection Time, etc.



http://www.nirsoft.net

BTCrawler
http://petronius.sourceforge.net

BlueScan
http://bluescanner.sourceforge.net

bt_rng
http://www.digifail.com

Bluesnarfer
http://www.alighieri.org

Bluetooth (JABWT) Browser
http://www.benhui.net

Module Flow

1. Wireless Concepts
2. Wireless Encryption
3. Wireless Threats
4. Wireless Hacking Methodology
5. Wireless Hacking Tools
6. Bluetooth Hacking
7. Countermeasures
8. Wireless Security Tools
9. Wireless Pen Testing

Wireless Security Layers

Wireless Signal Security

RF Spectrum Security, Wireless IDS

Data Protection

WPA2 and AES

Connection Security

Per-Packet Authentication, Centralized Encryption

Network Protection

Strong Authentication

Device Security

Vulnerabilities and Patches

End-user Protection

Stateful Per User Firewalls

How to Defend Against WPA/WPA2 Cracking

Passphrases

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

How to Defend Against KRACK Attacks

- Update all the routers and Wi-Fi devices with the **latest security patches**
- **Turn On auto updates** for all the wireless devices and patch the device firmware
- Avoid using public **Wi-Fi networks**
- Browse only secured websites and **do not access sensitive resource** when your device is connected to an unprotected network
- If you own IoT devices, **audit the devices** and do not connect to the insecure Wi-Fi routers
- Always enable **HTTPS Everywhere extension**
- Make sure to enable **two factor authentication**

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

How to Defend Against Wireless Attacks

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

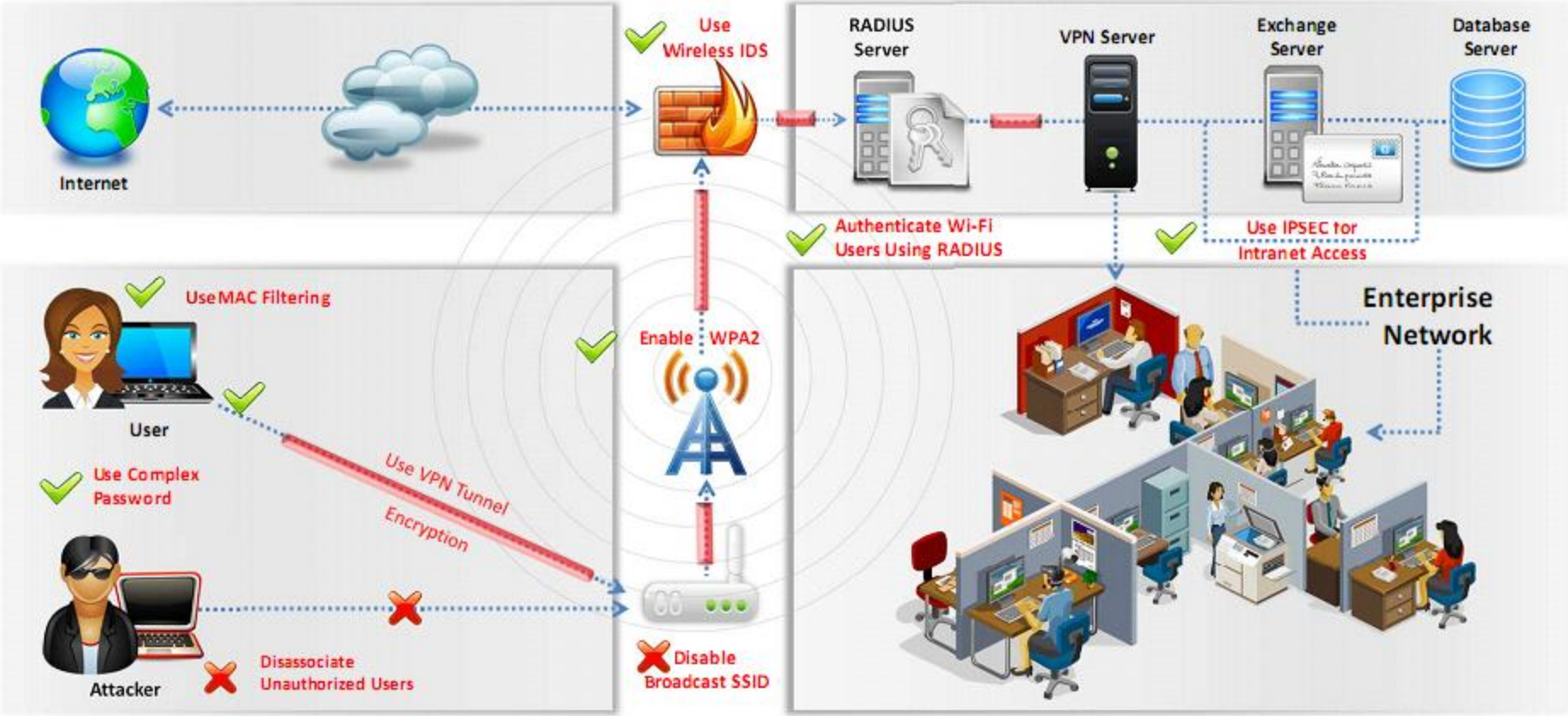
SSID Settings Best Practices

- 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 an additional technique for **encrypting traffic**, such as IPSEC over wireless

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**

How to Defend Against Wireless Attacks (Cont'd)



How to Defend Against Bluetooth Hacking

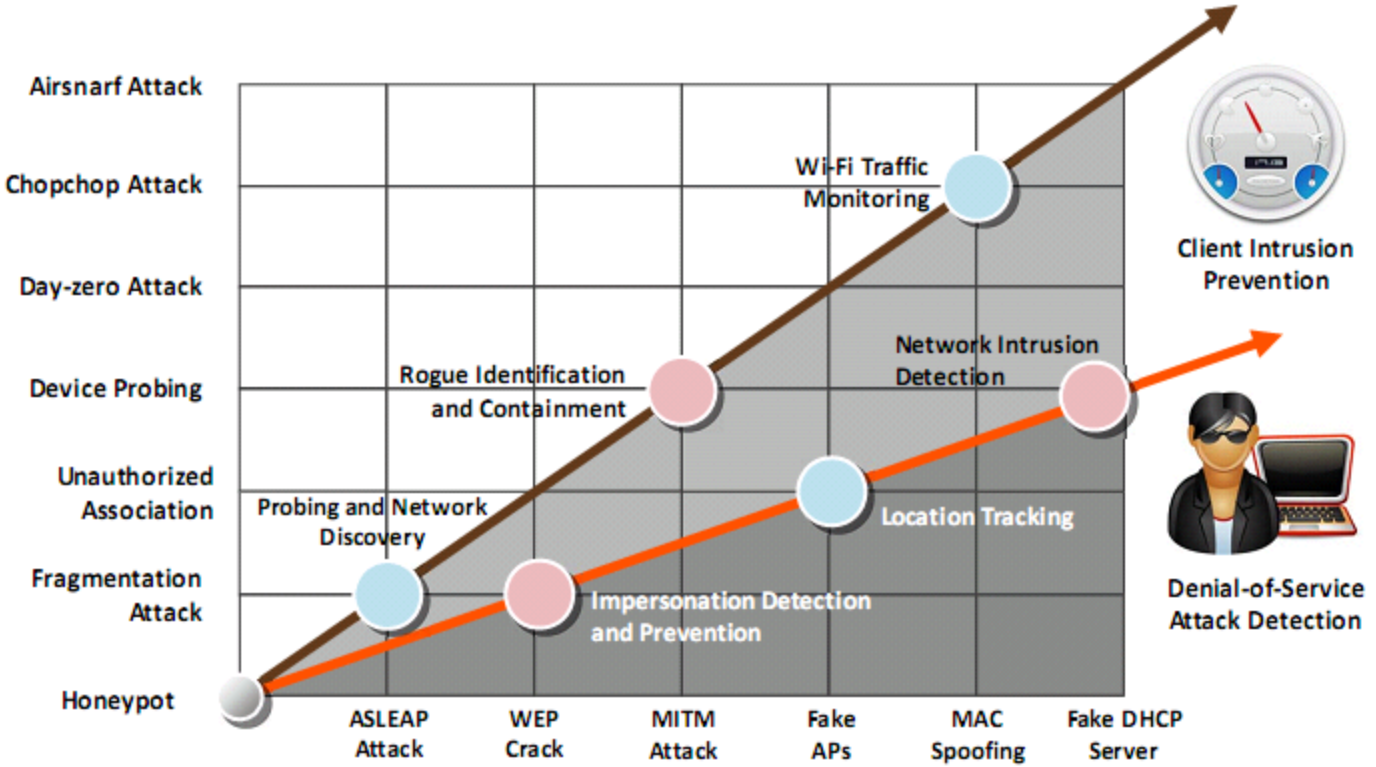
1. Use non-regular patterns as PIN keys while pairing a device
2. Keep the device in non-discoverable (hidden) mode
3. DO NOT accept any unknown and unexpected request for pairing your device
4. Always enable encryption when establishing BT connection to your PC
5. Keep a check of all paired devices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

Module Flow

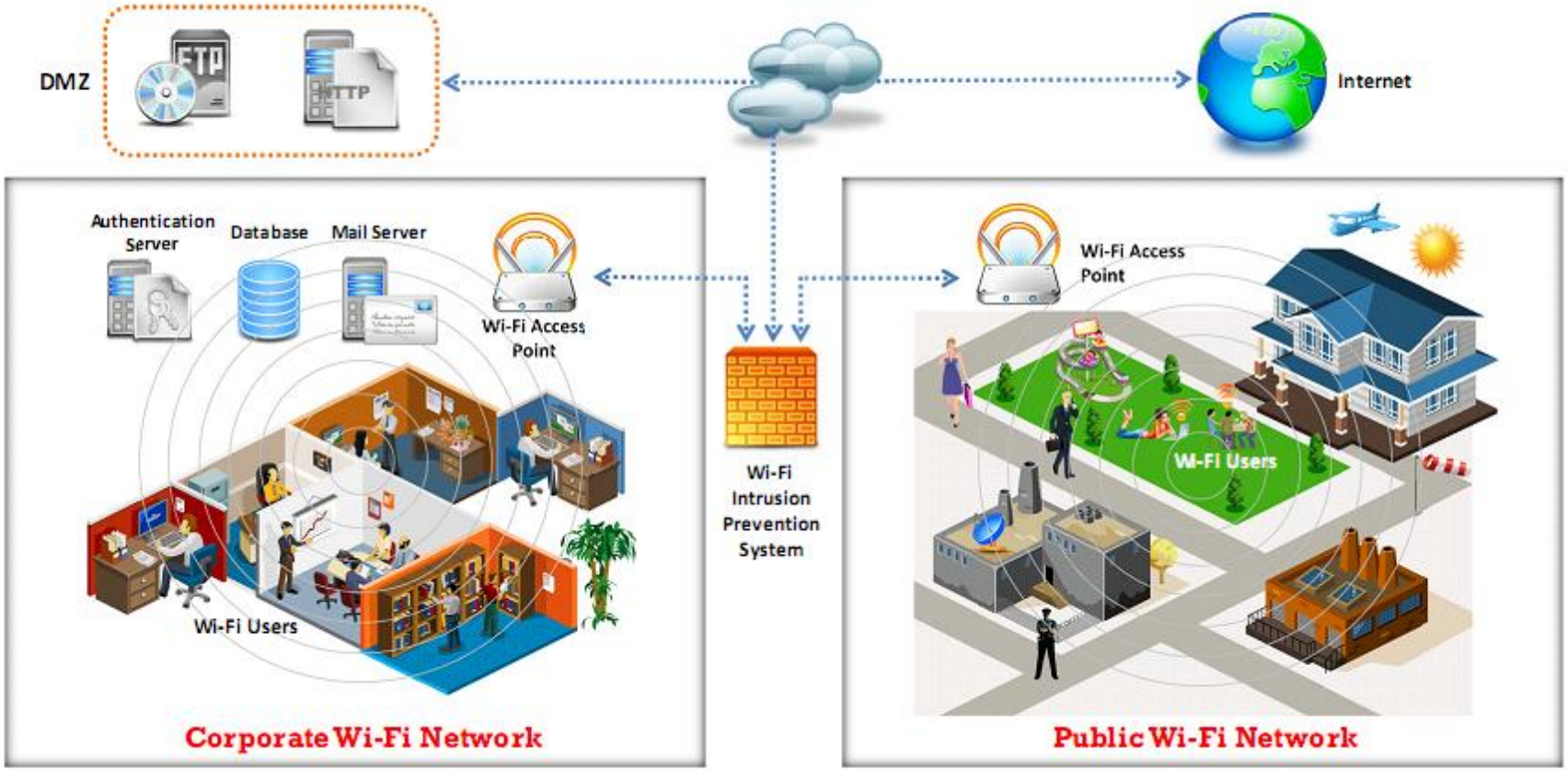
1. Wireless Concepts
2. Wireless Encryption
3. Wireless Threats
4. Wireless Hacking Methodology
5. Wireless Hacking Tools
6. Bluetooth Hacking
7. Countermeasures
8. Wireless Security Tools
9. Wireless Pen Testing

Wireless Intrusion Prevention Systems

- Wireless intrusion prevention systems **protect networks against wireless threats**, and enable administrators to detect and prevent various network attacks



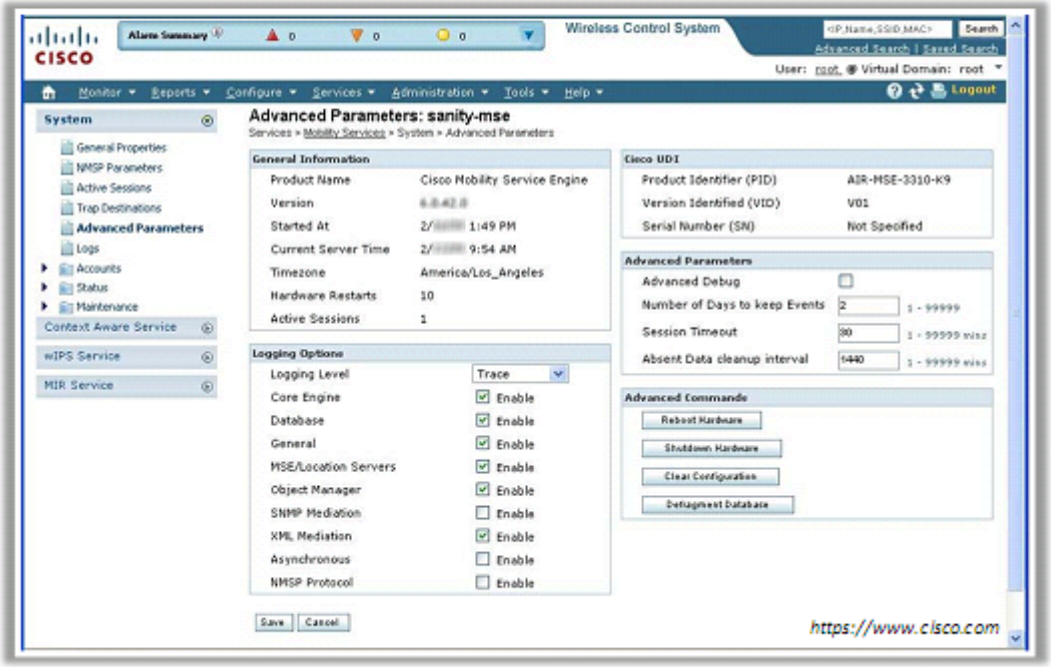
Wireless IPS Deployment



Wi-Fi Security Auditing Tools

Cisco Adaptive Wireless IPS

- 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**



AirMagnet WiFi Analyzer
http://enterprise.netscout.com

RFProtect
http://www.arubanetworks.com

Fern Wifi Cracker
https://github.com

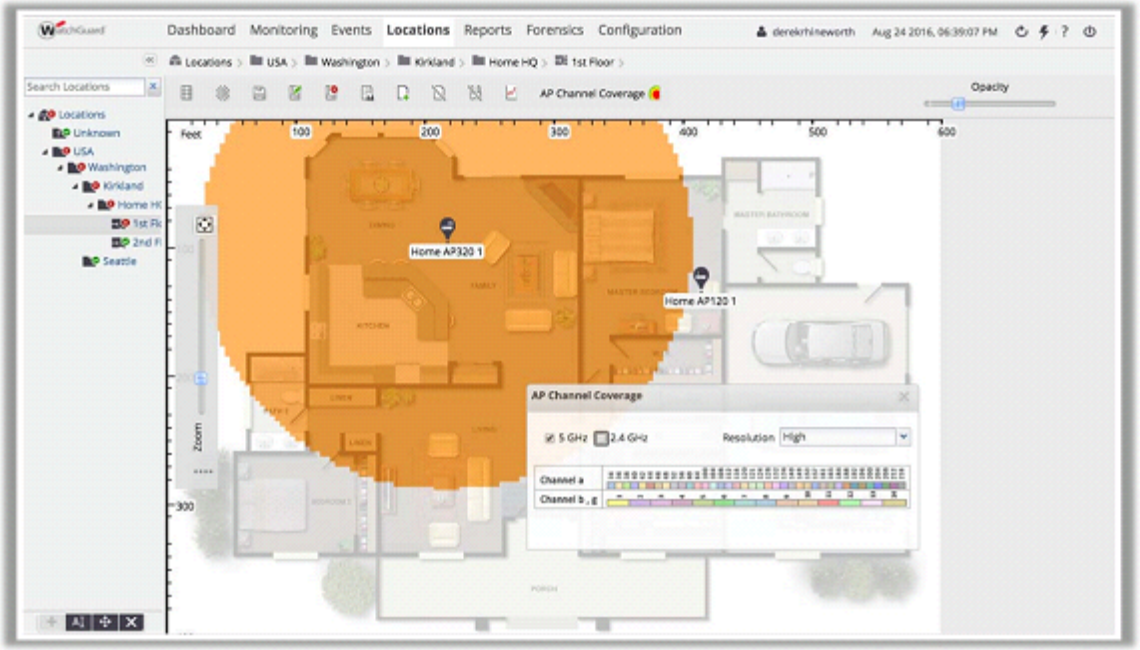
OSWA-Assistant
http://securitystartshere.org

Zebra's AirDefense Services Platform (ADSP)
https://www.zebra.com

Wi-Fi Intrusion Prevention System

WatchGuard WIPS

- WatchGuard WIPS defends your airspace 24/7 from **unauthorized devices**, **rogue APs**, and **malicious attacks** and with close to zero false positives



https://www.watchguard.com

Enterasys IPS
http://www.extremenetworks.com

AirMagnet Enterprise
http://enterprise.netscout.com

SONICWALL SONICPOINT N2
http://www.dell.com

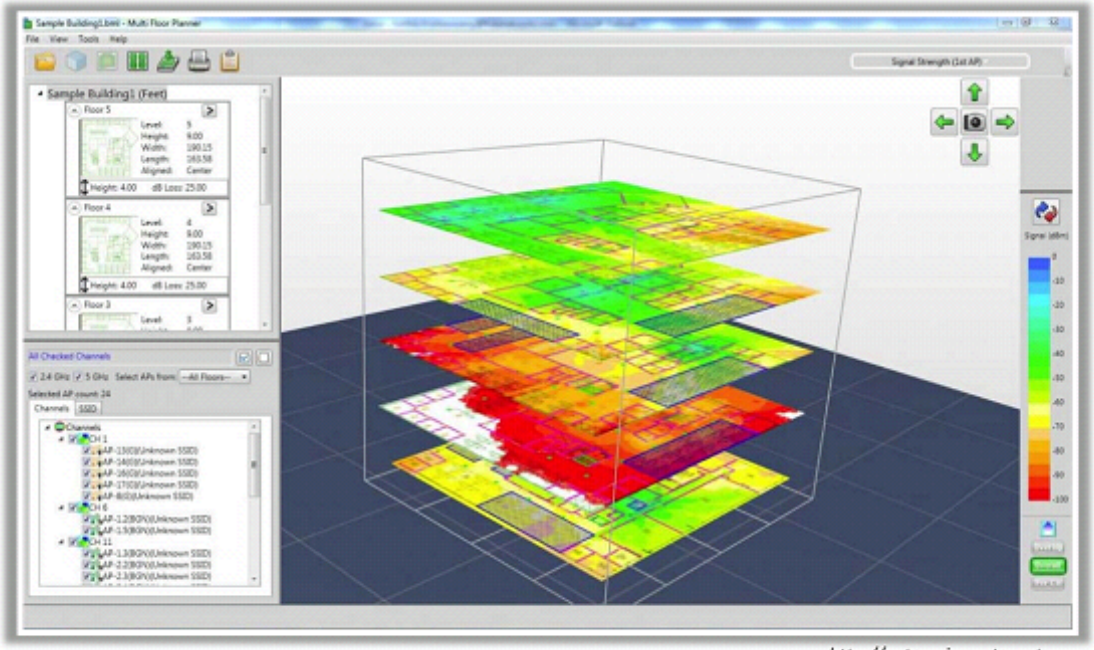
SonicPoint Wireless Security Access Point Series
http://www.sonicwall.com

HP TippingPoint NX Platform NGIPS
https://www8.hp.com

Wi-Fi Predictive Planning Tools

AirMagnet Planner

AirMagnet Planner is a wireless network planning tool that accounts for building materials, obstructions, AP configurations, antenna patterns, and a host of other variables to provide a reliable predictive map of Wi-Fi signal and performance



http://enterprise.netscout.com

Cisco Prime Infrastructure
https://www.cisco.com

AirTight Planner
http://www.moupiri.co.nz

LANPlanner
http://www.prologixdistribution.com

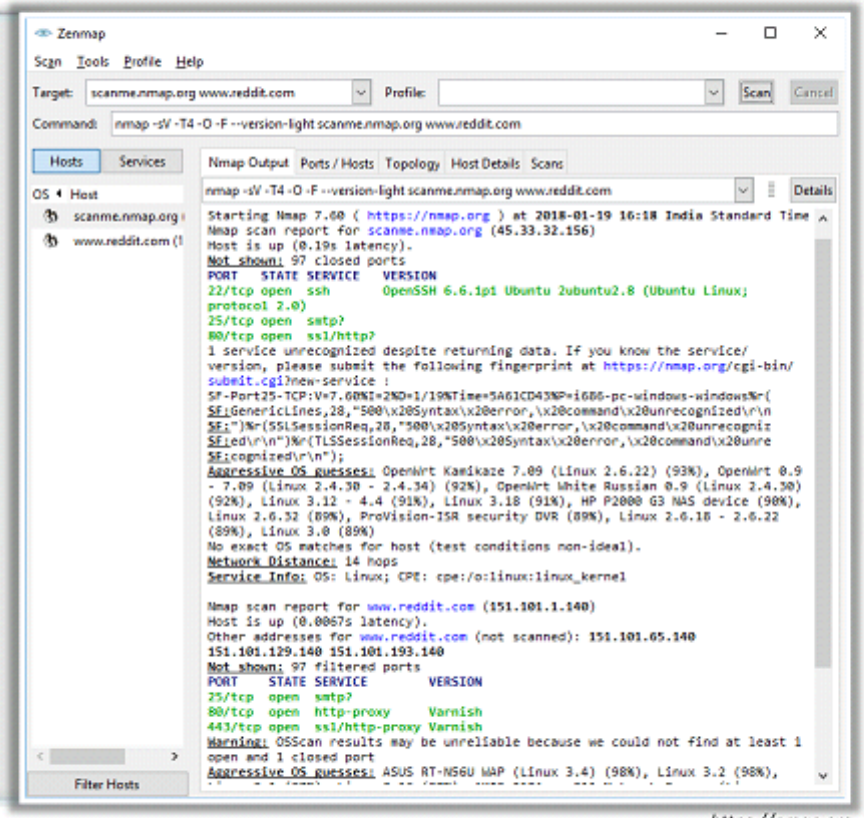
RingMaster Software
https://www.juniper.net

Ekahau Site Survey (ESS)
https://www.ekahau.com

Wi-Fi Vulnerability Scanning Tools

Zenmap

- Zenmap is a multi-platform GUI for the Nmap Security Scanner, which is useful for **scanning vulnerabilities on wireless networks**
- This tool saves the vulnerability **scans as profiles** to make them run repeatedly
- The results of recent scans are stored in a **searchable database**



https://nmap.org

Nessus
https://www.tenable.com

Network Security Toolkit
https://networksecuritytoolkit.org

Nexpose
https://www.rapid7.com

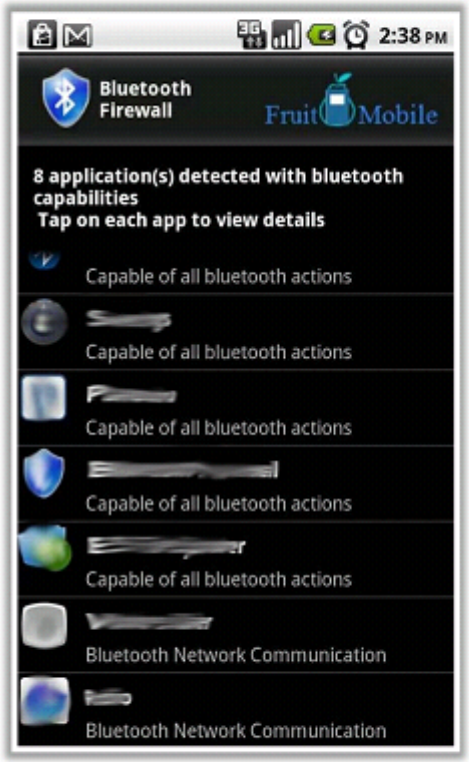
WiFish Finder
https://www.mojonetworks.com

Penetrator Vulnerability Scanner
https://www.secpoint.com

Bluetooth Security Tools

Bluetooth Firewall

- FruitMobile Bluetooth Firewall protects your android device against all sorts of bluetooth attack from devices around you
- It displays alerts when bluetooth activities take place
- You can also scan your device and detect apps with bluetooth capabilities



http://www.fruitmobile.com

Bluediving
http://bluediving.sourceforge.net

Bluelog
http://www.digifail.com

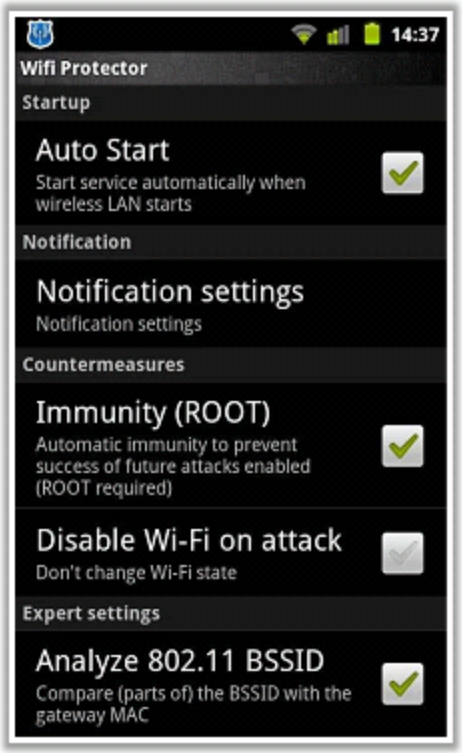
Blooover II
https://trifinite.org

Btscanner
https://packages.debian.org

BlueRanger
http://cyborg.ztrela.com

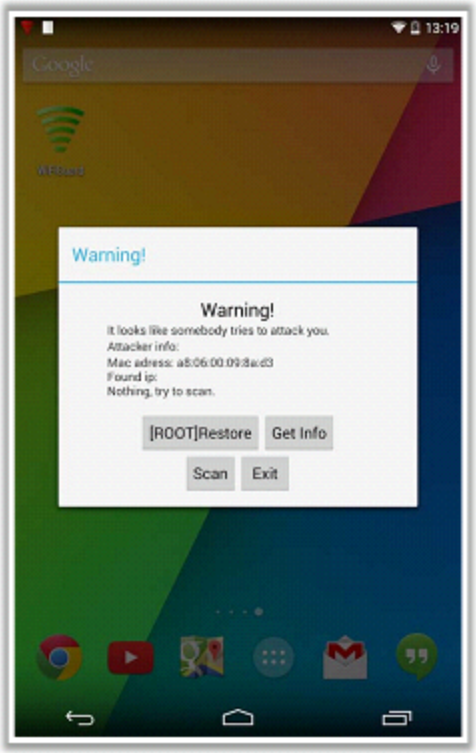
Wi-Fi Security Tools for Mobile

Wifi Protector



http://forum.xda-developers.com

WiFiGuard



https://play.google.com

Wifi Inspector

https://play.google.com

ARP Guard
https://play.google.com

Secure WiFi
https://play.google.com

Wifi Security Checker
https://play.google.com

Module Flow

1. Wireless Concepts
2. Wireless Encryption
3. Wireless Threats
4. Wireless Hacking Methodology
5. Wireless Hacking Tools
6. Bluetooth Hacking
7. Countermeasures
8. Wireless Security Tools
9. Wireless Pen Testing

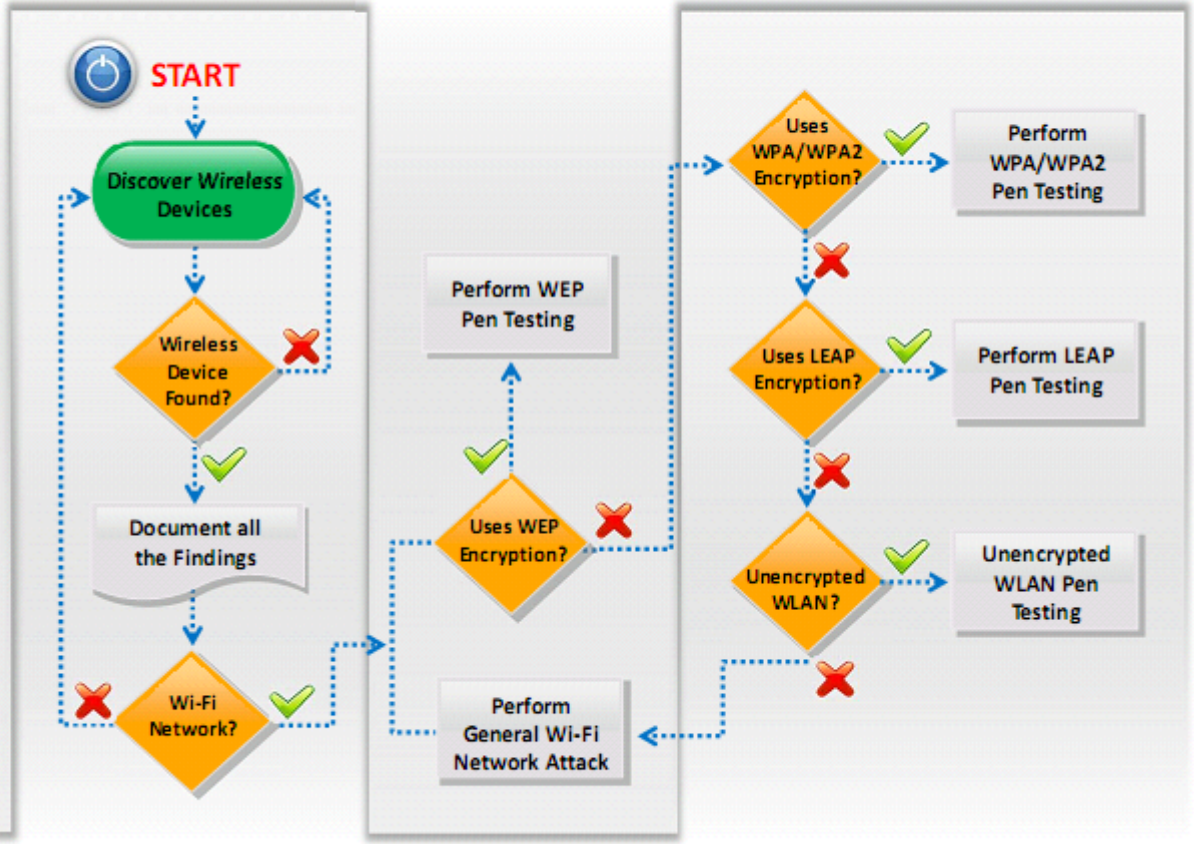
Wireless Penetration Testing

- Wireless penetration testing is a process of actively **evaluating information security measures** implemented in a wireless network to analyze design weaknesses, technical flaws, and vulnerabilities

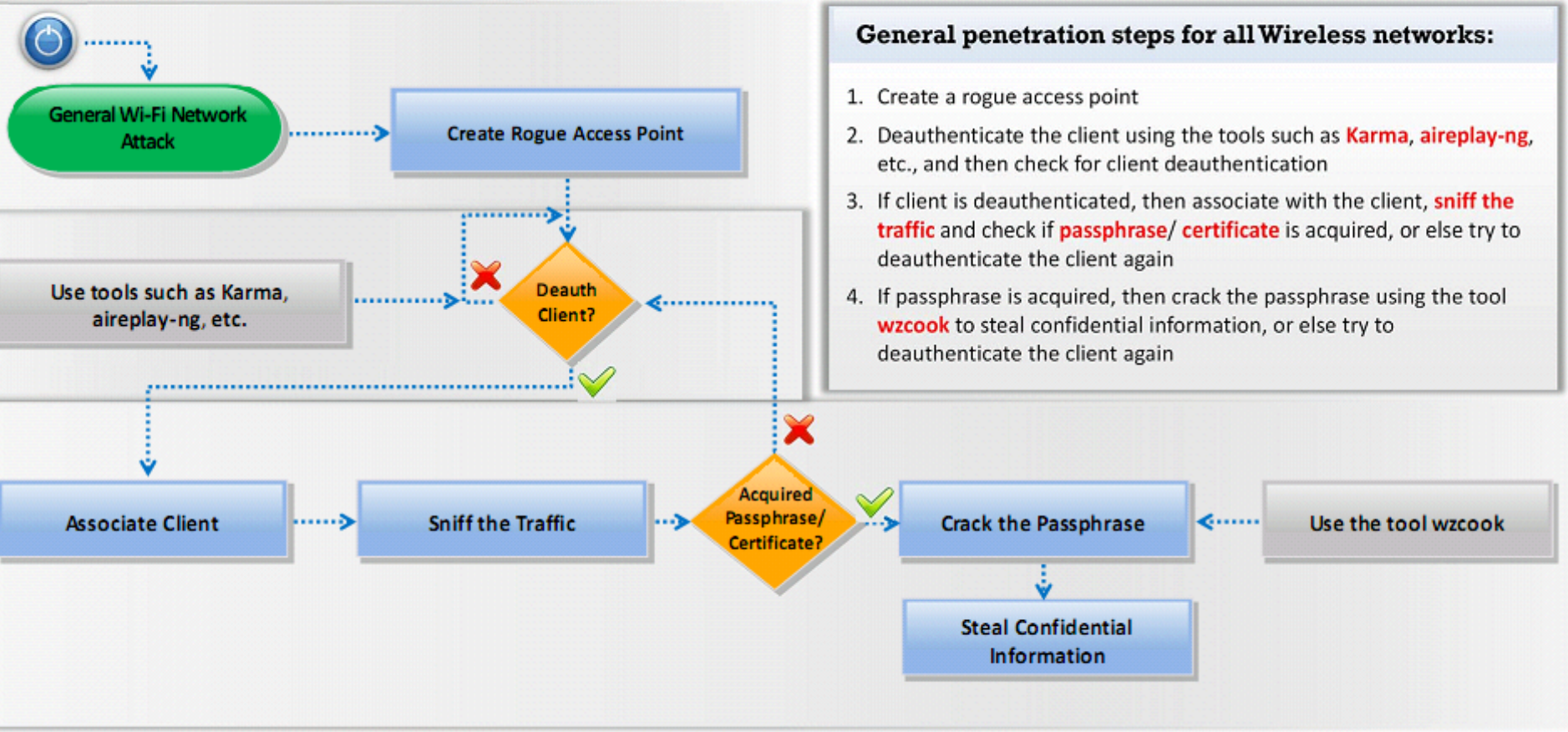
Threat Assessment	Identify the **wireless threats** facing an organization's information assets
Upgrading Infrastructure	Change or upgrade existing infrastructure of software, hardware, or network design
Risk Prevention and Response	Provide comprehensive **approach of preparation steps** that can be taken to prevent inevitable 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

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



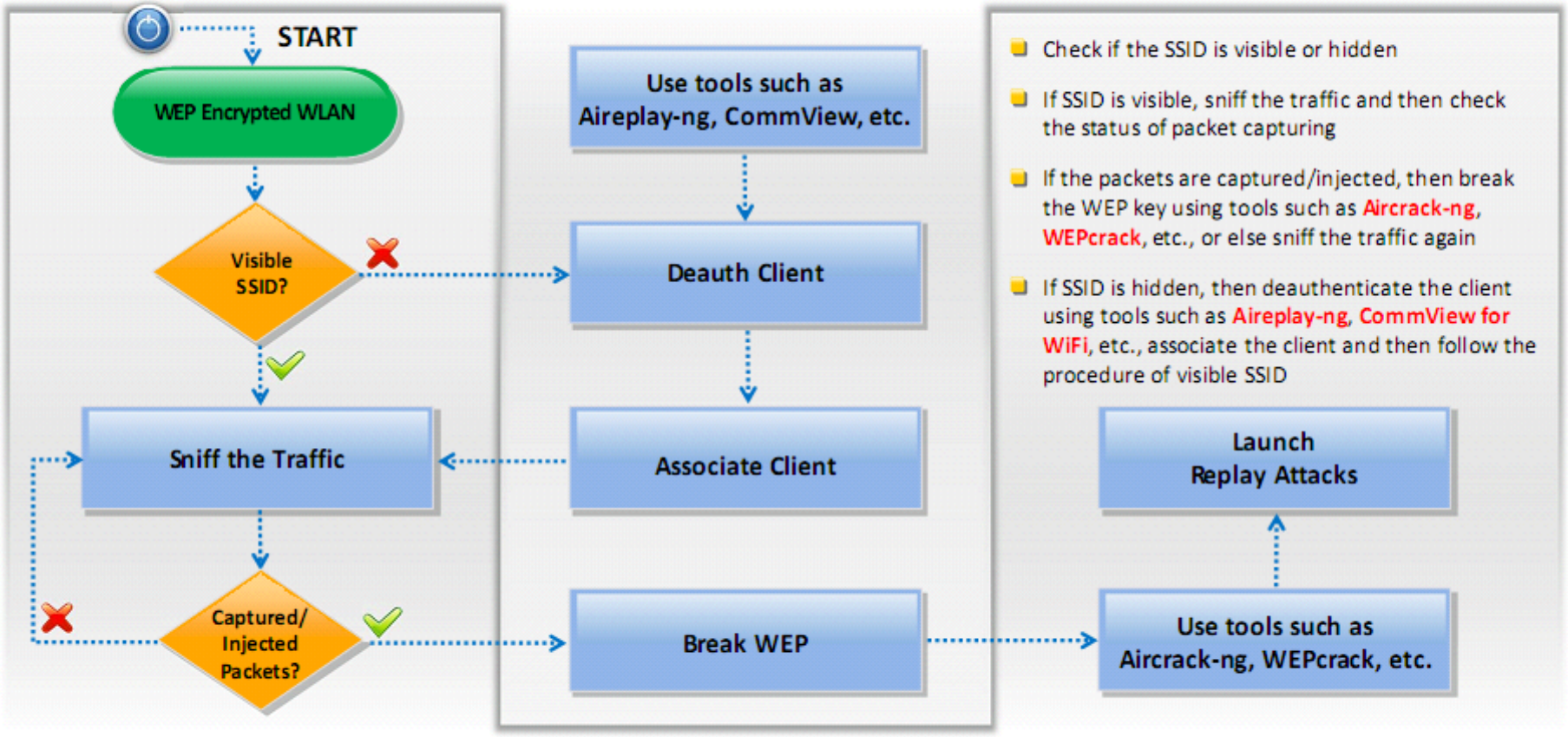
Pen Testing for General Wi-Fi Network Attack



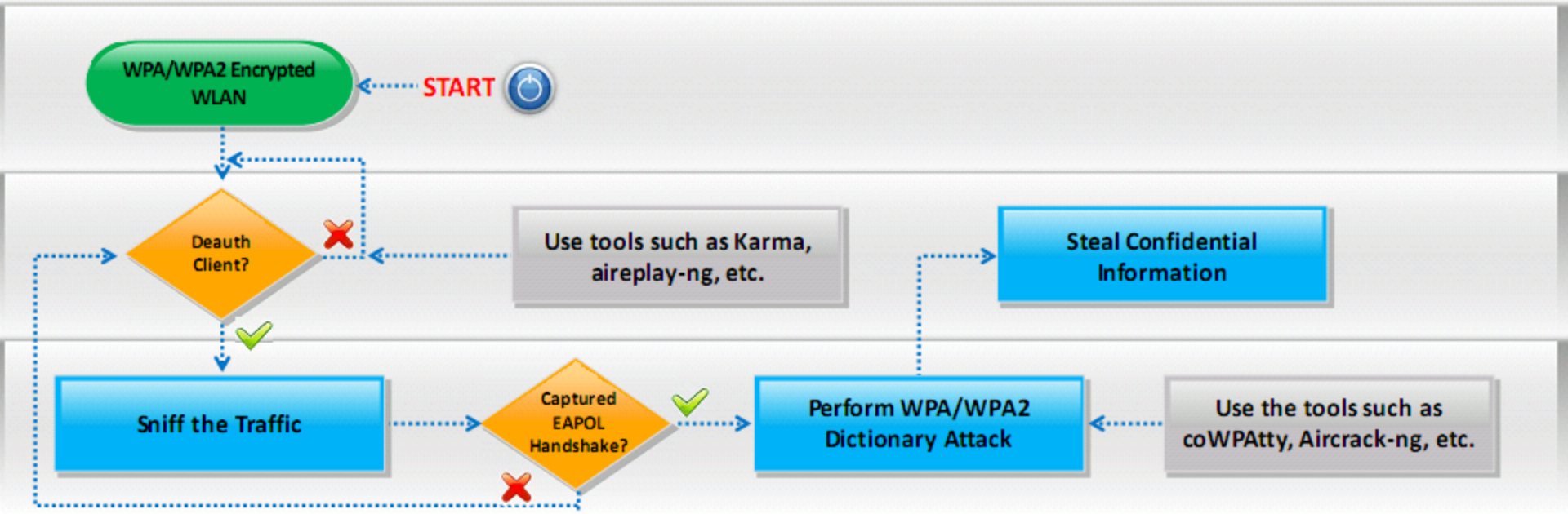
General penetration steps for all Wireless networks:

1. Create a rogue access point
2. Deauthenticate the client using the tools such as Karma, aireplay-ng, etc., and then check for client deauthentication
3. If client is deauthenticated, then associate with the client, sniff the traffic and check if passphrase/ certificate is acquired, or else try to deauthenticate the client again
4. If passphrase is acquired, then crack the passphrase using the tool wzcook to steal confidential information, or else try to deauthenticate the client again

Pen Testing WEP Encrypted WLAN

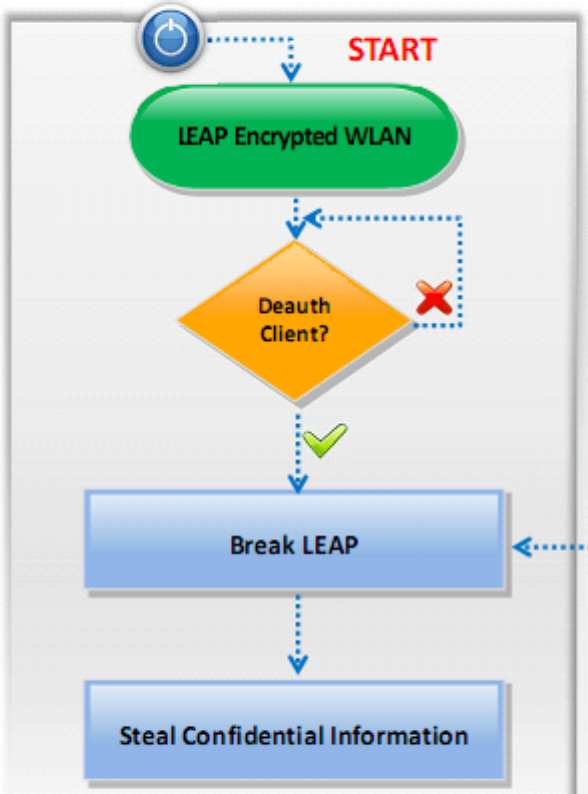


Pen Testing WPA/WPA2 Encrypted WLAN



- Deauthenticate the client using tools such as Karma, aireplay-ng, etc.
- If client is deauthenticated, sniff the traffic and then check the status of capturing EAPOL handshake or else try to deauthenticate the client again
- If EAPOL handshake is captured, then perform PSK dictionary attack using tools such as coWPAtty, Aircrack-ng, etc. to steal confidential information, or else try to deauthenticate the client again

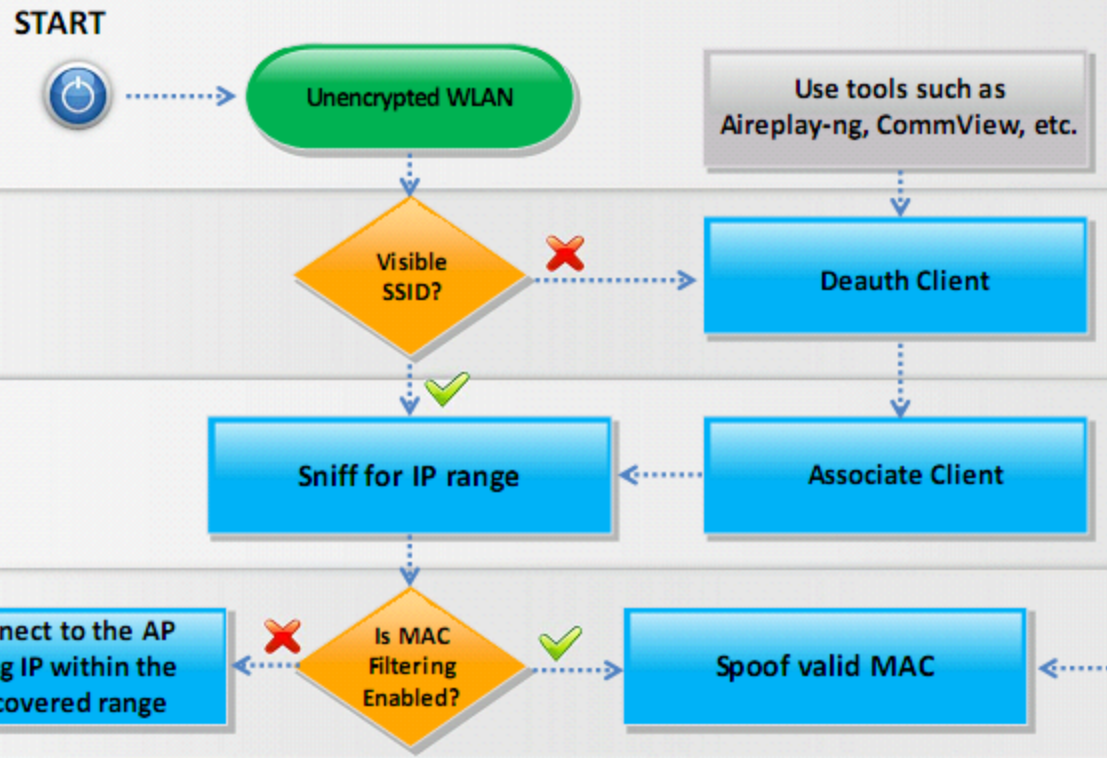
Pen Testing LEAP Encrypted WLAN



Use tools such as Asleap, THC-LEAPcracker, etc.

- Deauthenticate the client using tools such as Karma, aireplay-ng, etc.
- If client is deauthenticated, then break the LEAP encryption using tools such as Asleap, THC-LEAPcracker, etc. to steal confidential information, or else try to deauthenticate the client again

Pen Testing Unencrypted WLAN



- Check if the SSID is visible or hidden
- If SSID is visible, sniff for IP range and then check the status of MAC filtering
- If MAC filtering is enabled, spoof valid MAC using tools such as Technitium MAC Address Changer (TMAC), MAC Address Changer, Change MAC Address, etc. or connect to the AP using IP within the discovered range
- If SSID is hidden, then deauthenticate the client using tools such as Aireplay-ng, CommView for WiFi, etc., associate the client and then follow the procedure of visible SSID

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
- 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 attacks 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