Hacking Wireless Networks

Prepared by:
Dr. Ahmed Redha
PSU

Wireless Security Overview

- Concerns for wireless security are similar to those found in a wired environment.
- Security requirements are the same:
  - Confidentiality, integrity, availability, authenticity, accountability
  - Most significant source of risk is the underlying communications medium.

Wireless Network Modes

- The 802.11 wireless networks operate in two basic modes:
  - Infrastructure mode
  - Ad-hoc mode
- **Infrastructure mode**
  - Each wireless client connects directly to a central device called Access Point (AP)
  - No direct connection between wireless clients
  - AP acts as a wireless hub that performs the connections and handles them between wireless clients.

Wireless Network Modes

- **Ad-hoc mode:**
  - Each wireless client connects directly with each other
  - No central device managing the connections.
  - Rapid deployment of a temporal network where no infrastructures exist (advantage in case of disaster…)
  - Each node must maintain its proper authentication list.

Key Factors Contributing to Risks

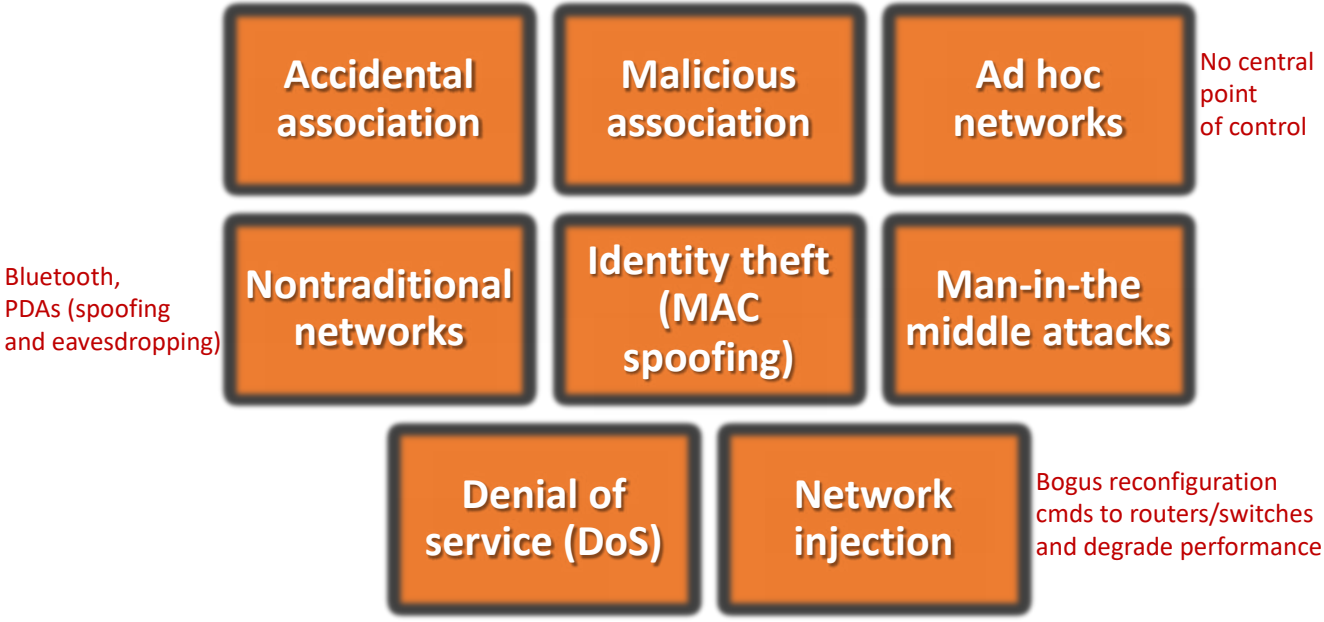
- Channel: broadcast communication (more susceptible to eavesdropping and jamming)
- Mobility: additional risks
- Resources: advanced OS (iPhone, Android), but limited resources (memory, processing)
- Accessibility: Certain devices may be left unattended.

Wireless Networking Components (Facilitating points of attack)



1. Wireless client: WIFI-enabled laptop/tablet, cell phone, Bluetooth device, …
2. Access point: Cell towers, WIFI hotspots, wireless routers
3. Transmission medium: carries signals

Wireless Network Threats



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

Table 11-1 Default SSIDs

Vendor	Default SSIDs
3Com	3Com
Apple	Airport Network
Belkin (54G)	Belkin54g
Cisco	Tsunami
Compaq	Compaq
D-Link	WLAN, default
Dell	Wireless
Intel	Intel, 101, xlan, 195
Linksys	linksys, Wireless, linksys-g
Microsoft	MSNHOME
Netgear	Wireless, NETGEAR
SMC	WLAN, BRIDGE, SMC
Symantec	101
US Robotics	WLAN, USR9106, USR808054

Securing Wireless Networks

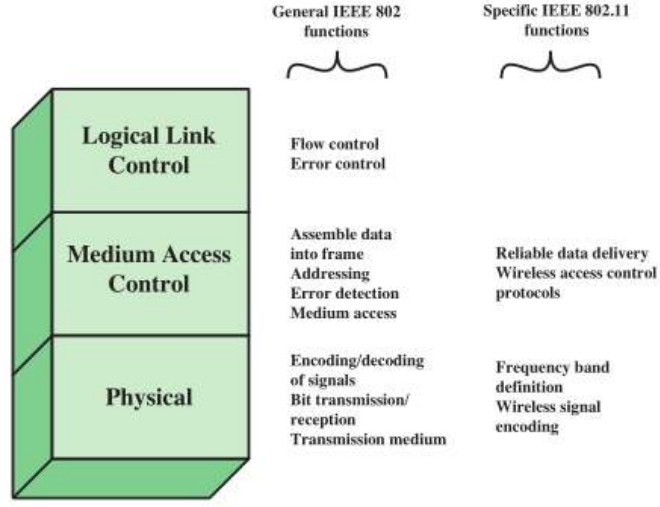
- Use encryption
- Use and enable anti-virus, anti-spyware, firewall
- Turn off SSID broadcasting
- Change default identifier on router
- Change router's preset password
- Apply MAC-filtering
  - Reduce signal strengths (place away from windows and external walls
  - Directional antennas

IEEE 802.11 Wireless LAN

- IEEE 802: a committee responsible for LANs
- IEEE 802.11: responsible for developing wireless protocols
  - Many standards
- The Wi-Fi alliance: became popular with 802.11b
  - Wi-Fi Protected Access (WPA, WPA2)

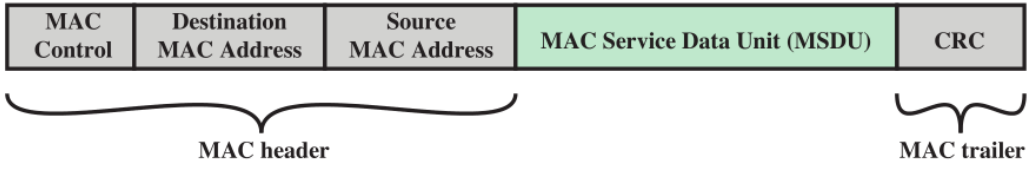
IEEE 802.11 Protocol Stack

- **Physical layer** (encode/decode signals)
- **MAC layer**: assembles MAC frame, disassembles frames and performs address recognition
- **LLC**: keeps track of frame transmission



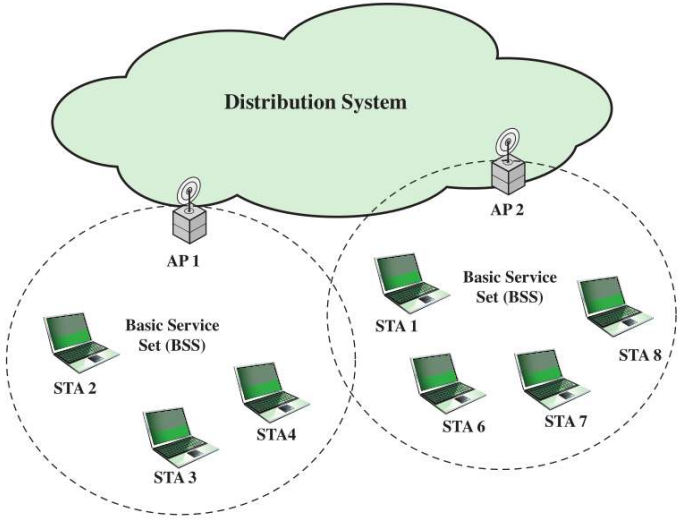
A MAC Frame (MPDU)

- MAC protocol data unit (MPDU)



IEEE 802.11 Extended Service Set

- **BSS**: the smallest building block
- BSSs connected via **APs**
  - APs functions as bridges
- **ESS:** two or more BSSs



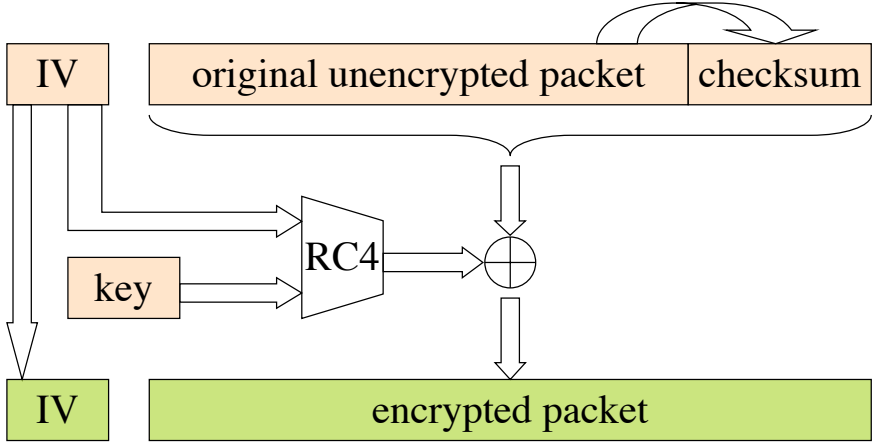
IEEE 802.11# Wireless Security

- Wired Equivalent Privacy (WEP)
- Wi-Fi Protected Access (WPA)
- WPA2
- WPA3

WEP - Wired Equivalent Privacy

- The original native security mechanism for WLAN
- Provides security through an 802.11 network
- Used to protect wireless communication from eavesdropping (confidentiality)
- Prevents unauthorized access to a wireless network (access control)
- Prevents tampering with transmitted messages
- Provides users with the equivalent level of privacy inbuilt in wireless networks.

How WEP works



WEP Flaws and Vulnerabilities

- Weak keys:
  - ✓It allows an attacker to discover the default key being used by the Access Point and client stations
  - ✓This enables an attacker to decrypt all messages being sent over the encrypted channel.
- IV (initialization vector) reuse and small size:
  - ✓There are 2^{24} different IVs
  - ✓On a busy network, the IV will surely be reused, if the default key has not been changed and the original message can be retrieved relatively easily.

Attacks on WEP



- WEP encrypted networks can be cracked in 10 minutes
- Goal is to collect enough IVs to be able to crack the key
- IV = Initialization Vector, plaintext appended to the key to avoid repetition
- Injecting packets generates IVs

WPA - WI-FI Protected Access

- New technique in 2002
- Replacement of security flaws of WEP
- Improved data encryption
- Strong user authentication
- Because of many attacks related to static key, WPA minimize shared secret key in accordance with the frame transmission
- Use the RC4 algorithm in a proper way and provide fast transfer of the data before someone can decrypt the data.

WPA2 - WI-FI Protected Access 2

- Based on the IEEE 802.i standard
- 2 versions: Personal & Enterprise
- The primary enhancement over WPA is the use of the AES (Advanced Encryption Standard) algorithm
- The encryption in WPA2 is done by utilizing either AES or TKIP

WPA2

- WPA2 has immunity against many types of hacker attacks
  - ✓Man-in-the middle
  - ✓Authentication forging
  - ✓Replay
  - ✓Key collision
  - ✓Weak keys
  - ✓Packet forging
  - ✓Dictionary attacks

WPA3

Wi-Fi Protected Access 3, or WPA3, superseded WPA2 in 2018. WPA3 is the latest, updated implementation of WPA.

- WPA3 support is not automatically added to every device. Users who wish to use WPA3-approved devices, such as wireless routers, must either buy new routers that support WPA3 or have the device updated by the manufacturer.
- New updates and features of WPA3 include the following:

✓ 256-bit Galois/Counter Mode Protocol encryption (GCMP-256);

✓ 384-bit Hashed Message Authentication Mode (HMAC);

✓ 256-bit Broadcast/Multicast Integrity Protocol (BIP-GMAC-256);

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



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

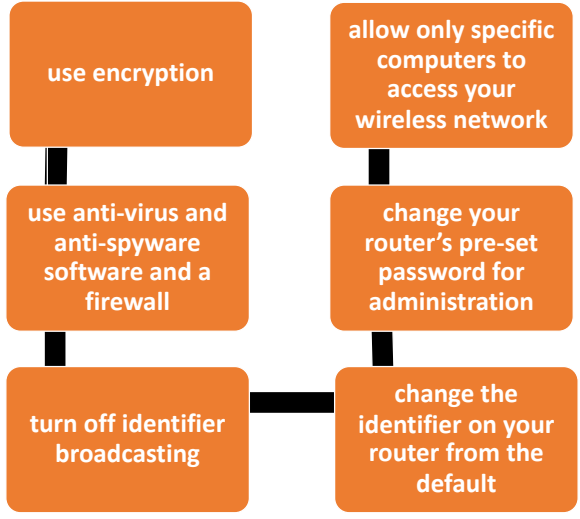
Securing Wireless Transmission

- Signal hiding (and SSID hiding)
  - Reduce signal strengths
- Encryption: encrypt all wireless transmissions

Securing Access Point

- Disallow unauthorized access to the AP
- Require authentication for any access including for devices wishing to attach themselves to the AP

Securing Wireless Networks



Association Services

Association

- Establishes an initial association between a station and an AP

Reassociation

- Enables an established association to be transferred from one AP to another, allowing a mobile station to move from one BSS to another

Disassociation

- A notification from either a station or an AP that an existing association is terminated

Wireless Hacking Methodology

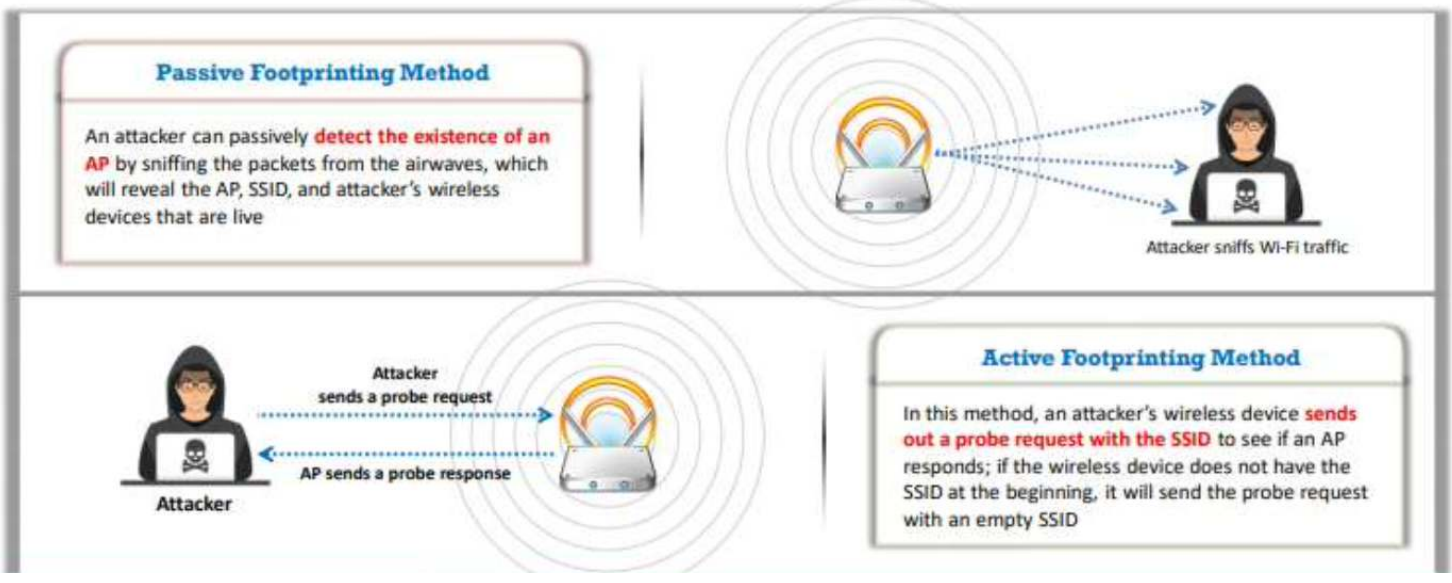
The wireless hacking methodology helps an attacker reach the goal of hacking a target wireless Network. An attacker usually follows a hacking methodology to be sure of finding every single entry point to break into the target network.

The attacker uses the following steps to perform wireless hacking:

1- Wi-Fi discovery
2- GPS mapping
3- Wireless traffic analysis
4- Launch of wireless attacks
5- Wi-Fi encryption cracking

1- Wi-Fi Discovery:
1.1- Wireless Network Footprinting

- Attacking a wireless network begins with **discovering** and **footprinting** the wireless network actively or passively



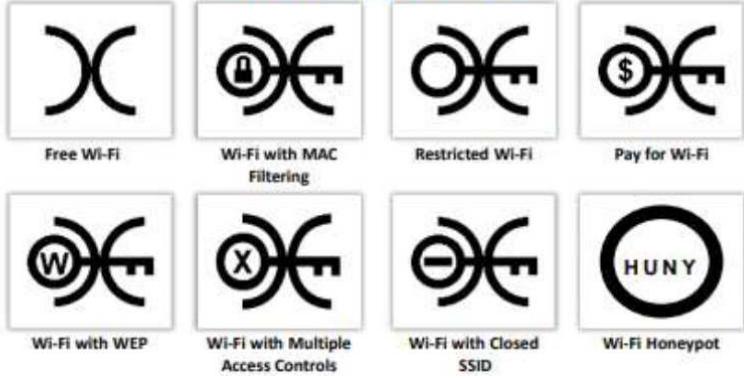
Wi-Fi Discovery (cont..)
1.2-Finding Wi-Fi Networks in Range to attack

- 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, and 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 chalking Symbols



Free Wi-Fi



Wi-Fi with MAC Filtering



Restricted Wi-Fi



Pay for Wi-Fi



Wi-Fi with WEP



Wi-Fi with Multiple Access Controls



Wi-Fi with Closed SSID



Wi-Fi Honeypot





Attackers use the following tools to discover Wi-Fi networks for launching attacks:

- Laptop with a Wi-Fi card
- External Wi-Fi antenna
- Network discovery software

Some of the tools used to discover Wi-Fi networks in range to attack are inSSIDer Plus, NetSurveyor, Wi-Fi Scanner, and Acrylic Wi-Fi Home.

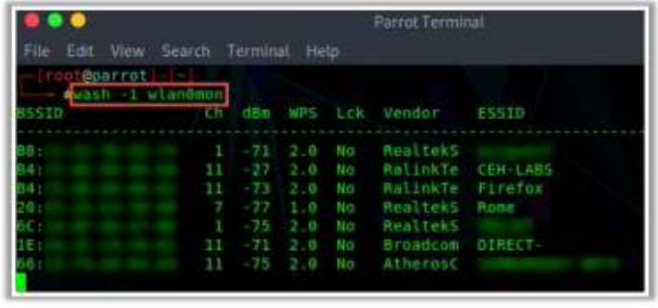
Wi-Fi Discovery (cont..)
1.3- Finding WPS-Enables APs

- Attackers use **Wash utility** to identify the WPS-enabled APs and detect if the AP is in locked or unlocked state

- Most of the WPSs in the routers usually lock when brute-forced for more than five times and can be unlocked only in the administrator interface of the router manually

- The Wash command can support the 5 GHz channel

- The attacker **discovers the AP, ESSID,** and **BSSID of a device or router** using the following wash command
  - `# sudo wash -i wlan0`

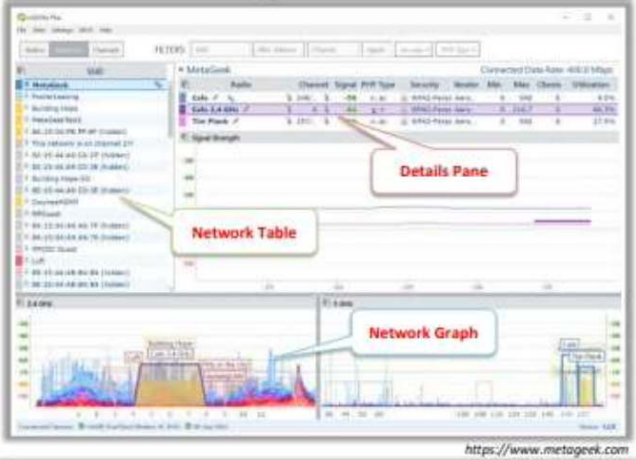




Wi-Fi Discovery (cont..)

1.4- Wi-Fi Discovery Tools

inSSIDer Plus Shows a **list of all the nearby wireless APs** and wireless networks with their signal strengths



https://www.metageek.com

NetSurveyor Gathers information about **nearby wireless APs in real-time** and displays it in useful ways



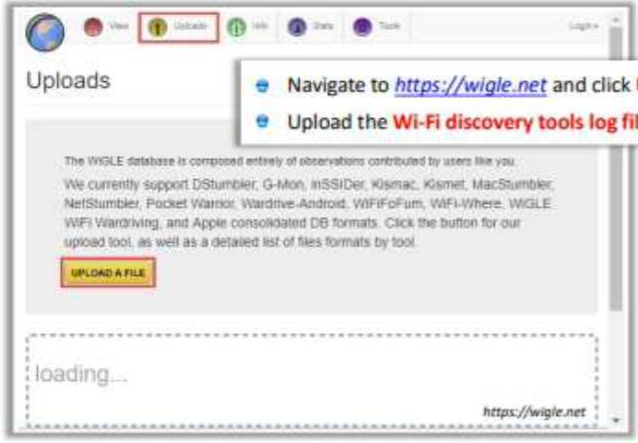
http://nutsaboutnets.com

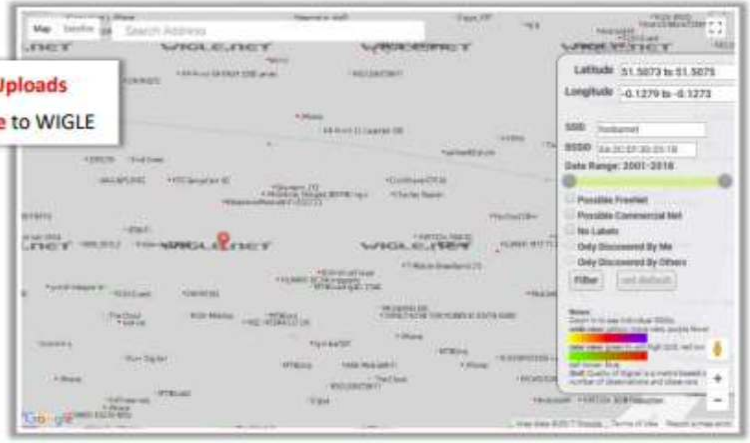
Other Wi-Fi Discovery Tools:

- **Wi-Fi Scanner** https://lizardsystems.com
- **Acrylic Wi-Fi Home** https://www.acrylicwifi.com
- **WirelessMon** https://www.passmark.com
- **Ekahau HeatMapper** https://www.ekahau.com

2- GPS Mapping

- Attackers create a map of discovered Wi-Fi networks and **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**





3-Wireless Traffic Analysis

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

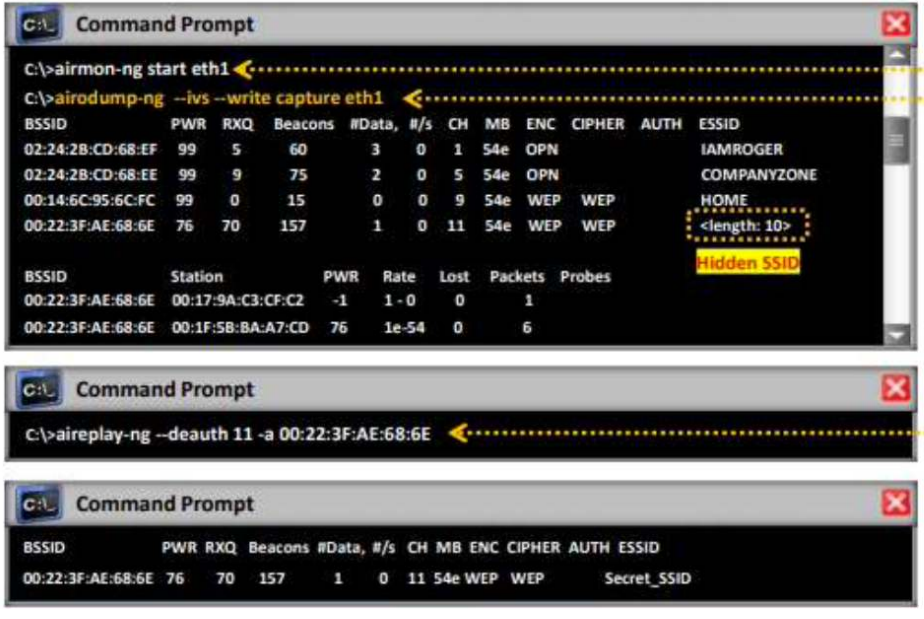
4- Launch of Wireless Attack: Aircrack-ng Suite

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

http://www.aircrack-ng.org

Airbase-ng Captures WPA/WPA2 handshake and can act as an ad-hoc AP	**Aircrack-ng** Defacto WEP and WPA/WPA2-PSK cracking tool	**Airdecap-ng** Decrypts 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	**Airdrop-ng** 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	**Airmon-ng** Used to enable monitor mode on wireless interfaces from managed mode and vice versa		**Airodump-ng** Used to capture packets of raw 802.11 frames and collect WEP IVs	**Airolib-ng** Stores and manages essid and password lists used in WPA/WPA2 cracking	**Airserv-ng** Allows multiple programs to indepen-dently use a Wi-Fi card via a client-server TCP connection
Airtun-ng Creates a virtual tunnel interface to monitor encrypted traffic and inject arbitrary traffic into a network	**Easside-ng** Enables communication via a WEP-encrypted AP without the knowledge of the WEP key	**Packetforge-ng** Used to create encrypted packets that can subsequently be used for injection	**Tkiptun-ng** Injects frames into a WPA TKIP network with QoS and can recover a MIC key and keystream from Wi-Fi traffic	**Wesside-ng** Incorporates different techniques to seamlessly obtain a WEP key within minutes	**WZCook** Recovers WEP keys from XP's wireless zero configuration utility

4.1- Launch of Wireless Attacks: Detection of Hidden SSIDs



Step 1: Run airmon-ng in monitor mode

Step 2: Start airodump-ng 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

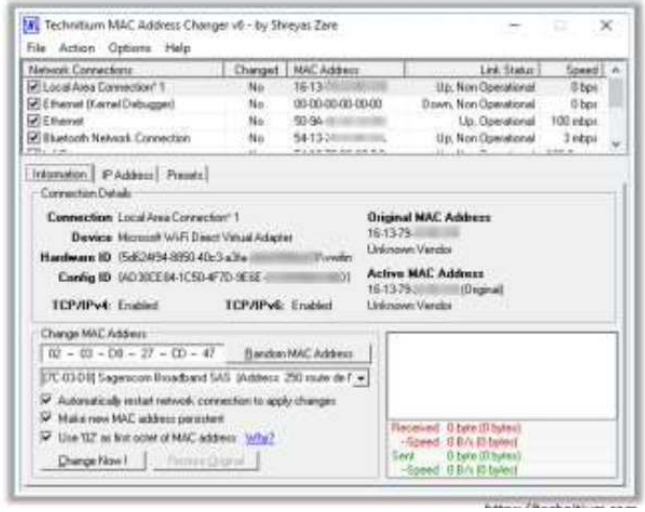
4.2- MAC Spoofing Attack

- In Media Access Control (MAC) spoofing, attackers **change the MAC address** to that of an authenticated user to bypass the MAC filtering configured in an AP
- 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
- Attackers use MAC spoofing tools, such as **Technitium MAC Address Changer** and MAC Address Changer, to change the MAC address

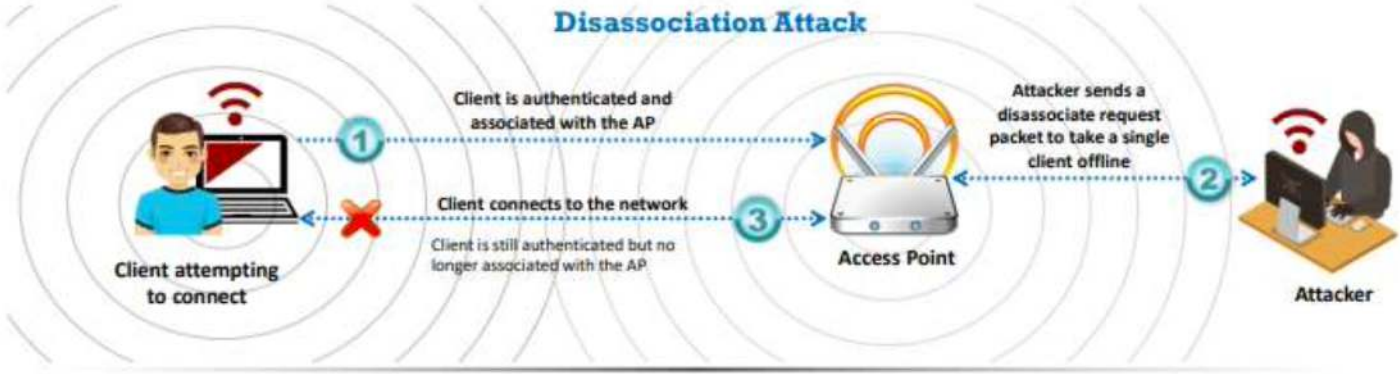


Technitium MAC Address Changer

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



4.3- DoS: Disassociation and De-authentication Attacks





4.4- Man in the Middle Attack



4.5- Rogue Access Point

- A rogue AP **provides backdoor access** to the target wireless network

Scenarios for Rogue AP Installation and Setup

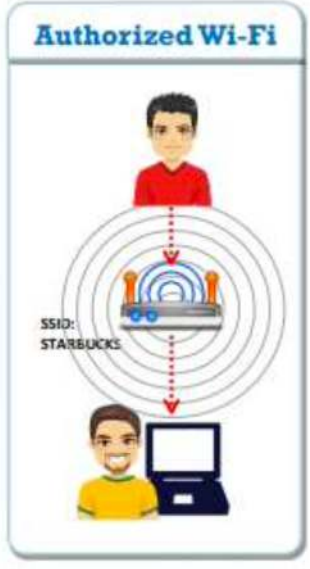
- A **compact, pocket-sized rogue AP** device plugged into an Ethernet port of a corporate network
- A **rogue AP device** connected to corporate networks over a Wi-Fi link
- A **USB-based rogue AP** device plugged into a corporate machine
- A **software-based rogue AP** running on a corporate Windows machine

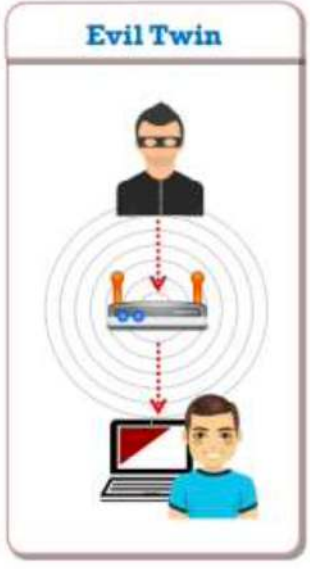
Steps to Deploy a Rogue AP

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

4.6 Evil Twin

- Evil Twin is a **wireless AP** that pretends to be a **legitimate AP** by replicating another network name
- Attackers set up a **rogue AP outside the corporate perimeter** and lures users 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 a company's WLAN SSID





4.7 Misconfigured Access Point Attack

Most organizations spend significant amounts of time defining and implementing Wi-Fi security policies, but it may be possible for a client of a wireless network to change the security setting on AP unintentionally.

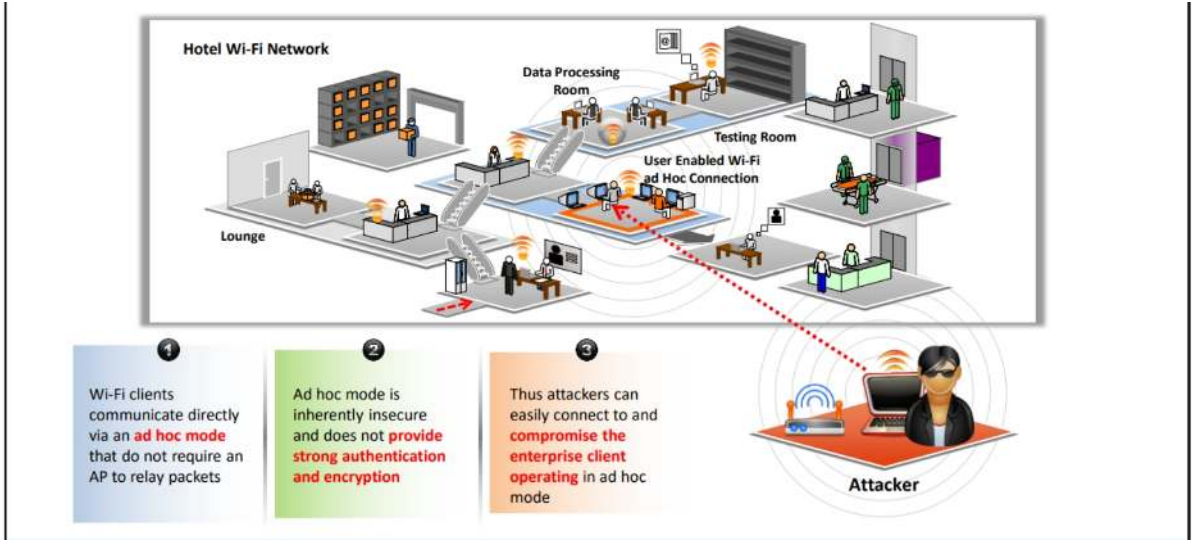
This in turn may lead to misconfigurations in APs. A misconfigured AP can expose an otherwise well-secured network to attacks. It is difficult to detect a misconfigured AP, as it is an authorized, legitimate device on the network.

Attackers can easily connect to the secured network through misconfigured APs, and the device continues to function normally as it will not trigger any alerts even if the attacker uses it to compromise security.

Some of the key elements that play an important role in this kind of attack include:

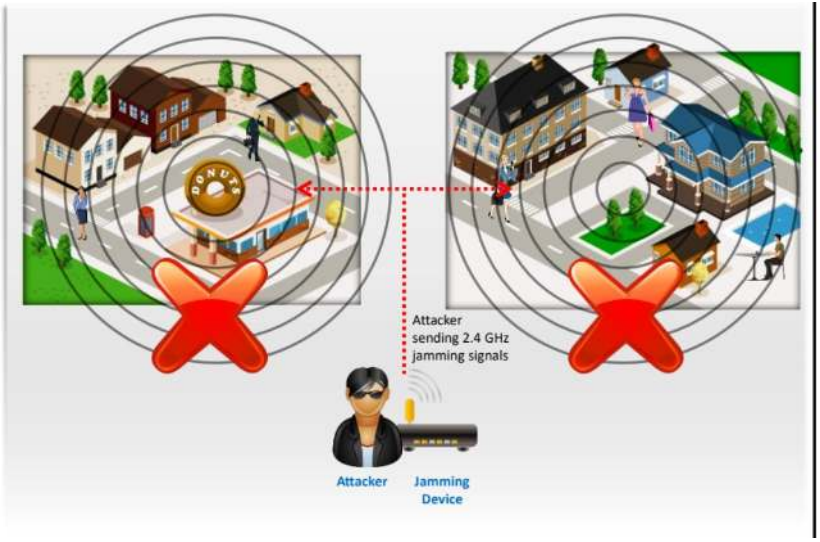
- **SSID Broadcast**
- **Weak Password**
- **Configuration Error**

4.8- Ad Hoc Connection Attack



4.9- 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



5- Wi-Fi Encryption Cracking: WEP Encryption Cracking

- Start the wireless interface in **monitor mode** on the specific AP channel
- Test the **injection capability** of the wireless device to the AP
- Use a tool, such as aireplay-ng, to do a **fake authentication** with the AP
- Start a Wi-Fi sniffing tool, such as airodump-ng, 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 aircrack-ng, to **extract encryption keys** from the IVs

How to Defend Against Wireless Attacks

Best Practices for Configuration

- Change the **default SSID** after WLAN configuration
- Set the **router access password** and enable firewall protection
- Disable **SSID broadcasts**
- Disable **remote router login** and wireless administration
- Enable **MAC Address filtering** on your AP or router
- Enable **encryption** on your AP and change passphrase often

Best Practices for SSID Settings

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

Best Practices for Authentication

- Choose **Enterprise WPA2 with 802.1x** authentication instead of WPA and WEP
- Implement **WPA2/WPA3 Enterprise** wherever possible
- Disable the **network** when not required
- Place wireless APs in a **secure location**
- Keep drivers on all wireless equipment **updated**
- Use a centralized server for **authentication**

How to Defend Against Wireless Attacks (cont'd)

