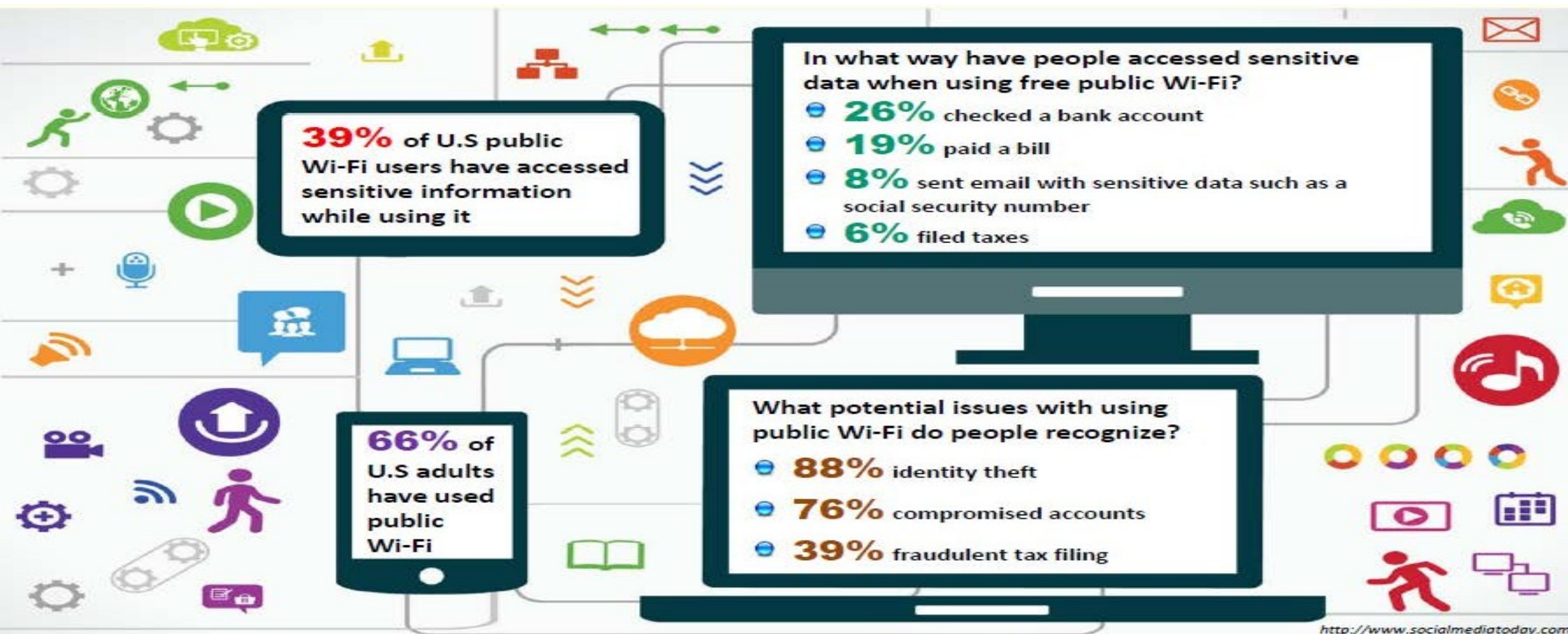# Hacking Wireless Network

Prof. Dr. M. Ameer Ali

Professor & Chairman

Department of Computer Science & Engineering

Bangladesh University of Business and Technology (BUBT)

Are You Protected from Hackers on Public Wi-Fi?

39% of U.S public Wi-Fi users have accessed sensitive information while using it

In what way have people accessed sensitive data when using free public Wi-Fi?
- **26%** checked a bank account
- **19%** paid a bill
- **8%** sent email with sensitive data such as a social security number
- **6%** filed taxes

66% of U.S adults have used public Wi-Fi

What potential issues with using public Wi-Fi do people recognize?
- **88%** identity theft
- **76%** compromised accounts
- **39%** fraudulent tax filing

http://www.socialmediatoday.com

Wi-Fi Statistics

Globally, **46 percent of total mobile data traffic** was offloaded onto the fixed network through Wi-Fi

By 2018, **40 percent** of enterprises will specify Wi-Fi as the default connection for non mobile devices, such as desktops, desk phones, projectors, conference room.

http://www.cisco.com, http://www.gartner.com

Module Objectives

- Understanding Wireless Concepts
- Understanding Wireless Encryption Algorithms
- Understanding Wireless Threats
- Understanding Wireless Hacking Methodology

- Wireless Hacking Tools
- Understanding Bluetooth Hacking Techniques
- Understanding Wireless Hacking Countermeasures
- Wireless Security Tools
- Overview of Wireless Penetration Testing

Module Flow

Wireless Concepts

Wireless Encryption

Wireless Threats

Wireless Hacking Methodology

Wireless Hacking Tools

Bluetooth Hacking

Countermeasures

Wireless Security Tools

Wi-Fi 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 network

Hotspot

Places where wireless network is available for public use

Association

The process of connecting a wireless device to an access point

Orthogonal Frequency-division Multiplexing (OFDM)

Method of encoding digital data on multiple carrier frequencies

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

1 ▶ Wi-Fi refers to wireless local area networks (WLAN) based on **IEEE 802.11 standard**

2 ▶ It is a widely used technology for wireless communication across a **radio channel**

3 ▶ 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**

Advantages

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

Disadvantages

- Security is a big issue and may **not meet expectations**
- As the number of computers on the network increases, the **bandwidth suffers**
- Wi-Fi enhancements can require new **wireless cards and/or access points**
- Some **electronic equipment** can interfere with the Wi-Fi networks

Wi-Fi Networks at Home and Public Places

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

🔲 You can find **free/paid Wi-Fi access** available in coffee shops, shopping malls, bookstores, offices, airport terminals, schools, hotels, and other public places

Wi-Fi at Home

Wi-Fi at Public Places

Wireless Technology Statistics

Why Wireless Technology Matters?

More than half of all open Wi-Fi networks are susceptible to abuse

There will be more than **7 billion** new Wi-Fi enabled devices in the next 3 years

90% of all smartphones are equipped with Wi-Fi capabilities

A Wi-Fi attack on an open network can take less than **2 seconds**

By 2017, **60%** of carrier network traffic will be offloaded to Wi-Fi

71% of all mobile communications flows over Wi-Fi

http://www.huffingtonpost.com

Types of Wireless Networks

Extension to a Wired Network
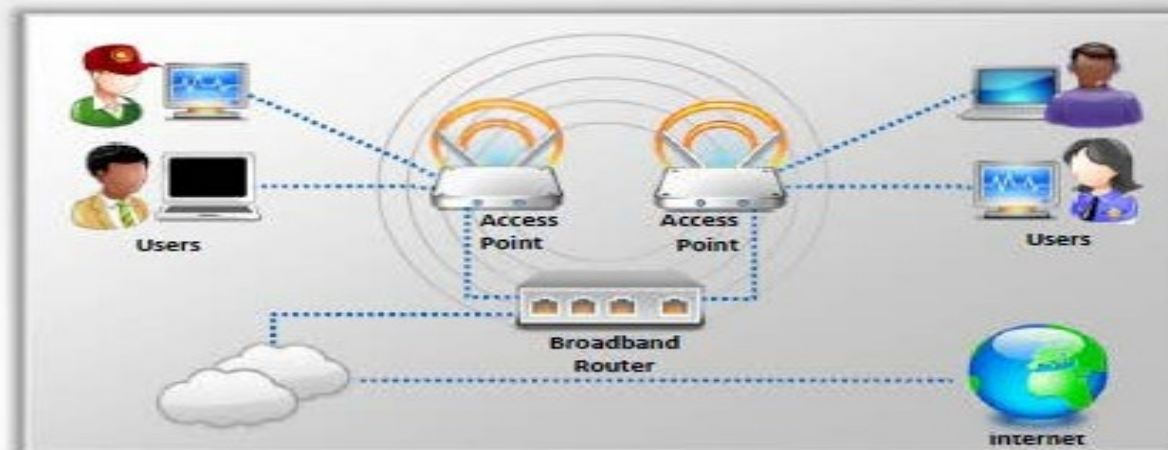
Multiple Access Points

LAN-to-LAN Wireless Network

3G/4G Hotspot

Wireless Standards

Amendments	Freq. (GHz)	Modulation	Speed (Mbps)	Range (ft)
802.11a	5	OFDM	54	25 – 75
802.11b	2.4	DSSS	11	150 – 150
802.11g	2.4	OFDM, DSSS	54	150 – 150
802.11i	Defines WPA2-Enterprise/WPA2-Personal for Wi-Fi			
802.11n	2.4, 5	OFDM	54	~100
802.16 (WiMAX)	10 - 66		70 – 1000	30 miles
Bluetooth	2.4		1 - 3	25

Wi Fi

Service Set Identifier (SSID)

01 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)

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

03 **Access points continuously broadcasts SSID**, if enabled, for the client machines to identify the presence of wireless network

04 **SSID is a human-readable text** string with a maximum length of 32 bytes

05 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

06 **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"

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

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

Wi-Fi Authentication Modes

Open System Authentication Process

1. Probe Request
2. Probe Response (Security Parameters)
3. Open System Authentication Request
4. Open System Authentication Response
5. Association Request (Security Parameters)
6. Association Response

Client attempting to connect — Access Point (AP) — Switch or Cable Modem — Internet

Shared Key Authentication Process

1. Authentication request sent to AP
2. AP sends challenge text
3. Client encrypts challenge text and sends it back to AP
4. AP decrypts challenge text, and if correct, authenticates client
5. Client connects to network

Client attempting to connect — Access Point (AP) — Switch or Cable Modem — Internet

Wi-Fi Authentication Process Using a Centralized Authentication Server

Client

Access Point

RADIUS Server

1. Client request connection

2. AP sends an EAP-Request to determine identity

3. EAP-Response with identity

4. Forward the identity to the RADIUS server using the uncontrolled port

5. Sends a request to the wireless client via the AP specifying the authentication mechanism to be used

6. The wireless client responds to the RADIUS server with its credentials via the AP

8. Sends a multicast/global authentication key encrypted with a per-station unicast session key

7. Sends an encrypted authentication key to the AP if the credentials are acceptable

Wi-Fi Chalking

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

WarChalking — A method used to **draw symbols in public places** to advertise open Wi-Fi networks
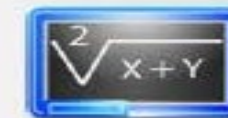
WarFlying — In this technique, attackers **use drones** to detect open wireless networks

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

Wi-Fi Chalking Symbols

Free Wi-Fi
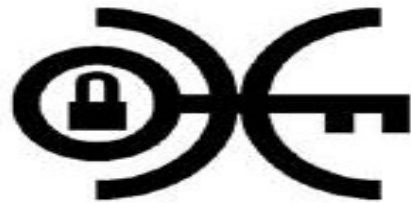
Wi-Fi with MAC Filtering

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

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

Unidirectional Antenna

Omnidirectional Antenna

Parabolic Grid Antenna

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

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

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

Module Flow

Types of Wireless Encryption

WPA2 Enterprise

It integrates EAP standards with WPA2 encryption

WEP

- WEP is an encryption algorithm for IEEE 802.11 wireless networks
- It is an old and original wireless security standard which can be cracked easily

AES

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

WPA2

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

WPA

- It is an advanced wireless encryption protocol using TKIP, MIC, and AES encryption
- Uses a 48 bit IV, 32 bit CRC and TKIP encryption for wireless security

EAP

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

802.11i

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

TKIP

A security protocol used in WPA as a replacement for WEP

CCMP

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

RADIUS

It is a centralized authentication and authorization management system

LEAP

It is a proprietary WLAN authentication protocol developed by Cisco

WEP Encryption

What is WEP?

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

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

WEP encryption can be easily cracked

64-bit WEP uses a 40-bit key

128-bit WEP uses a 104-bit key size

256-bit WEP uses 232-bit key size

WEP Flaws

- It has significant vulnerabilities and design flaws

It was developed without:

- Academic or public review
- Review from cryptologists

How WEP Works

01 CRC-32 checksum is used to calculate a 32-bit **Integrity Check Value** (ICV) for the data, which, in turn, is added to the data frame

02 A 24-bit arbitrary number known as **Initialization Vector (IV)** is added to WEP key; WEP key and IV are together called as **WEP seed**

03 The WEP seed is used as the input to **RC4** algorithm to generate a key stream (key stream is bit-wise **XORed** with the combination of data and ICV to produce the encrypted data)

04 The IV field (IV+PAD+KID) is added to the ciphertext to generate a **MAC frame**

WEP Key Store (K1, K2, K3, K4)

RC4 Cipher

WEP Seed

Data | ICV

CRC-32 Checksum

XOR Algorithm **X**

WEP Key | IV

Keystream

IV | PAD | KID | Ciphertext

WEP-encrypted Packet (Frame body of MAC Frame)
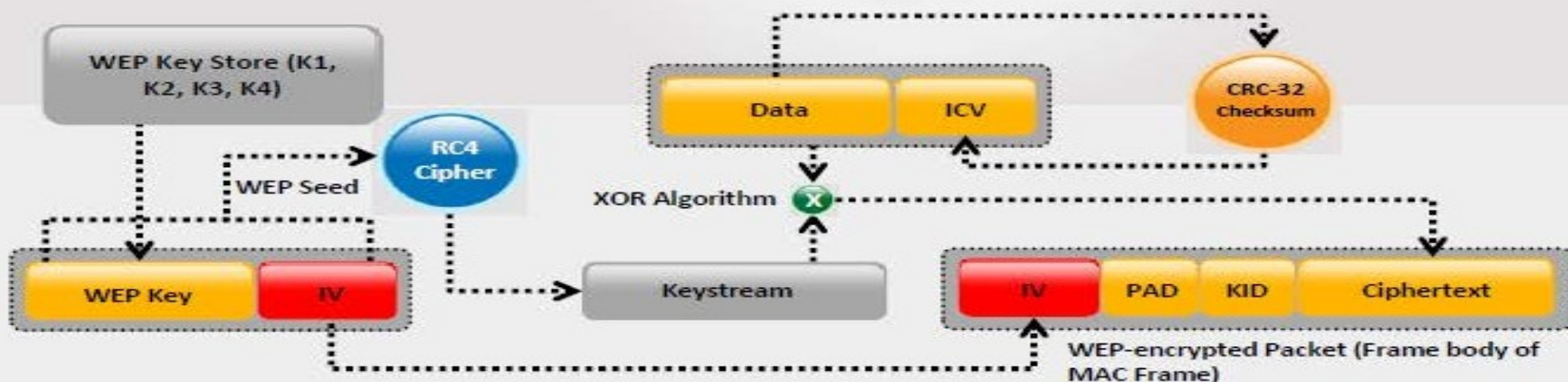
What is WPA?

- Wi-Fi Protected Access (WPA) is a **data encryption method** for WLANs based on 802.11 standards

- It is a snapshot of 802.11i (under development) providing **stronger encryption**, and enabling PSK or EAP authentication

TKIP (Temporal Key Integrity Protocol)

- TKIP utilizes the RC4 stream cipher encryption with **128-bit** keys and **64-bit** MIC integrity check

- TKIP mitigated vulnerability by **increasing the size of the IV** and using mixing functions

128-bit Temporal Key

- Under TKIP, the client starts with a 128-bit "temporal key" (TK) that is then **combined with the client's MAC address** and with an IV to create a keystream that is used to encrypt data via the RC4

- It implements a sequence counter to protect against **replay attacks**

WPA Enhances WEP

- TKIP enhances WEP by adding a **rekeying mechanism** to provide fresh encryption and integrity keys

- Temporal keys are changed for every **10,000 packets**. This makes TKIP protected networks more resistant to cryptanalytic attacks involving key reuse

How WPA Works

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

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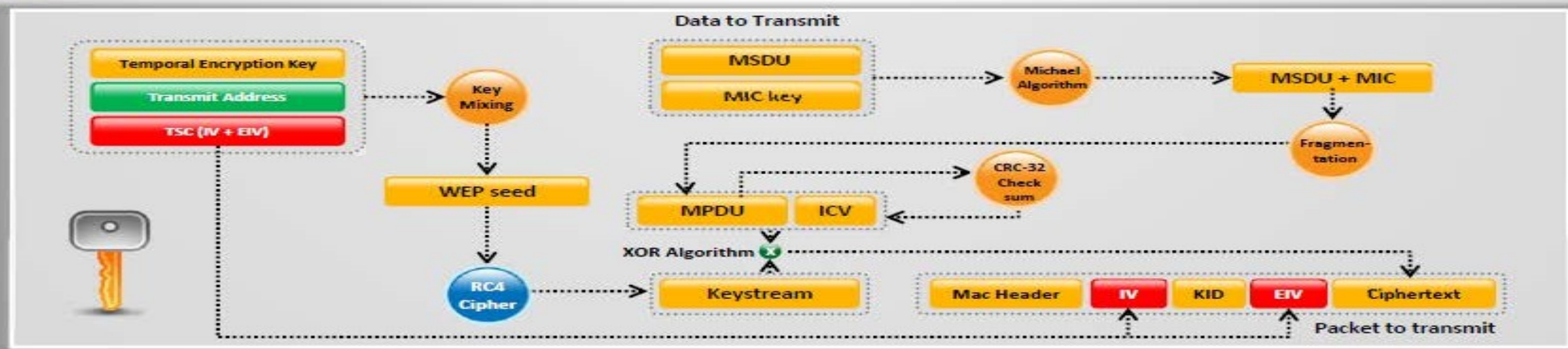
Temporal Keys

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

01 AP sends an ANonce to client which uses it to construct the **Pairwise Transient Key (PTK**

02 Client respond with its own nonce-value (SNonce) to the AP together with a **Message Integrity Code (MIC)**

03 AP sends the **GTK and a sequence number** together with another MIC which is used in the next broadcast frames

04 Client confirm that the temporal keys are installed
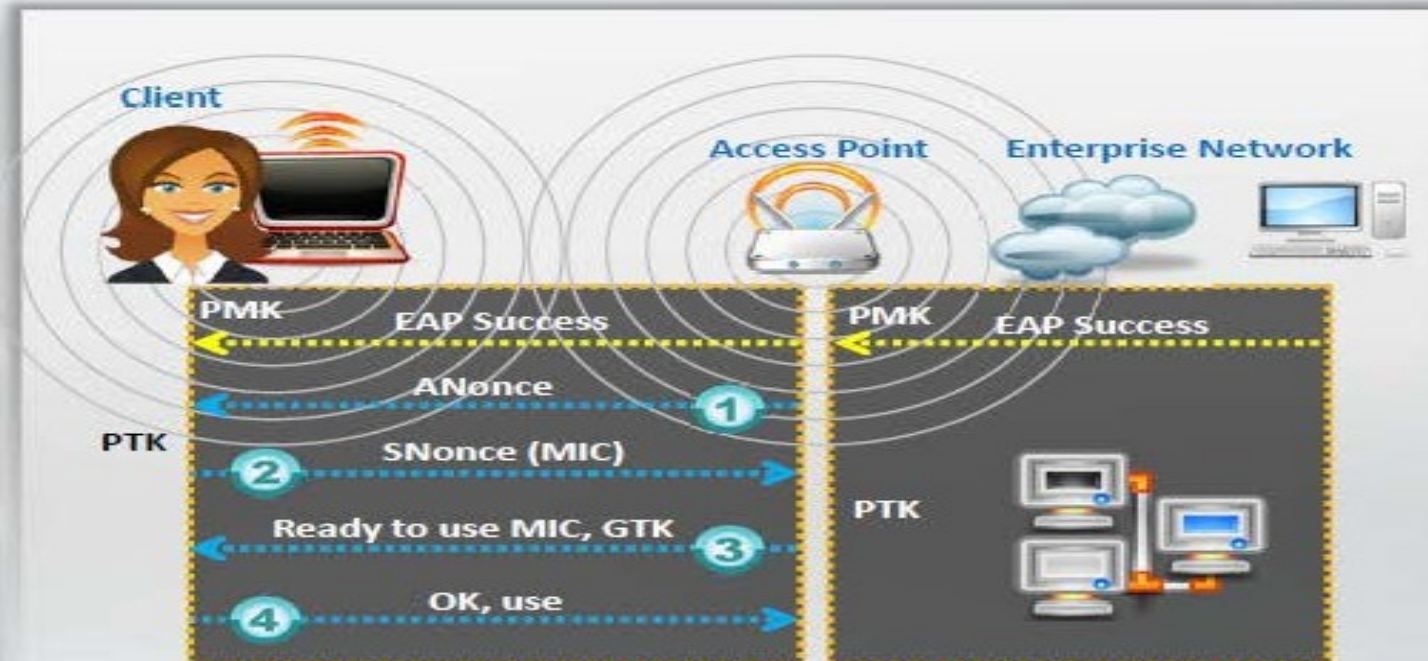
What is WPA2?

- WPA2 provides enterprise and Wi-Fi users with **stronger data protection** and **network access control**

- Provides government grade security by implementing the **National Institute of Standards and Technology** (NIST) **FIPS 140-2 compliant AES encryption** algorithm

WPA2-Personal

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

- In PSK mode each wireless network device encrypts the network traffic using a 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, certificates etc.

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

How WPA2 Works

In the CCMP implementation of WPA2, **MAC header data** is used to build additional authentication data (AAD)

A sequenced **packet number (PN)** is used to build nonce

AAD, temporal key and nonce along with CCMP are used for **data encryption**

A **WPA2 MAC Frame** is build using MAC header, CCMP header, encrypted data and encrypted MIC

MAC header

Priority destination address

PN   Temporal key   Plaintext data

Build AAD

Build Nonce

AAD

Nonce

Build CCMP header

AES CCMP

MAC header   CCMP header   Encrypted data   Encrypted MIC

WPA2 MAC Frame
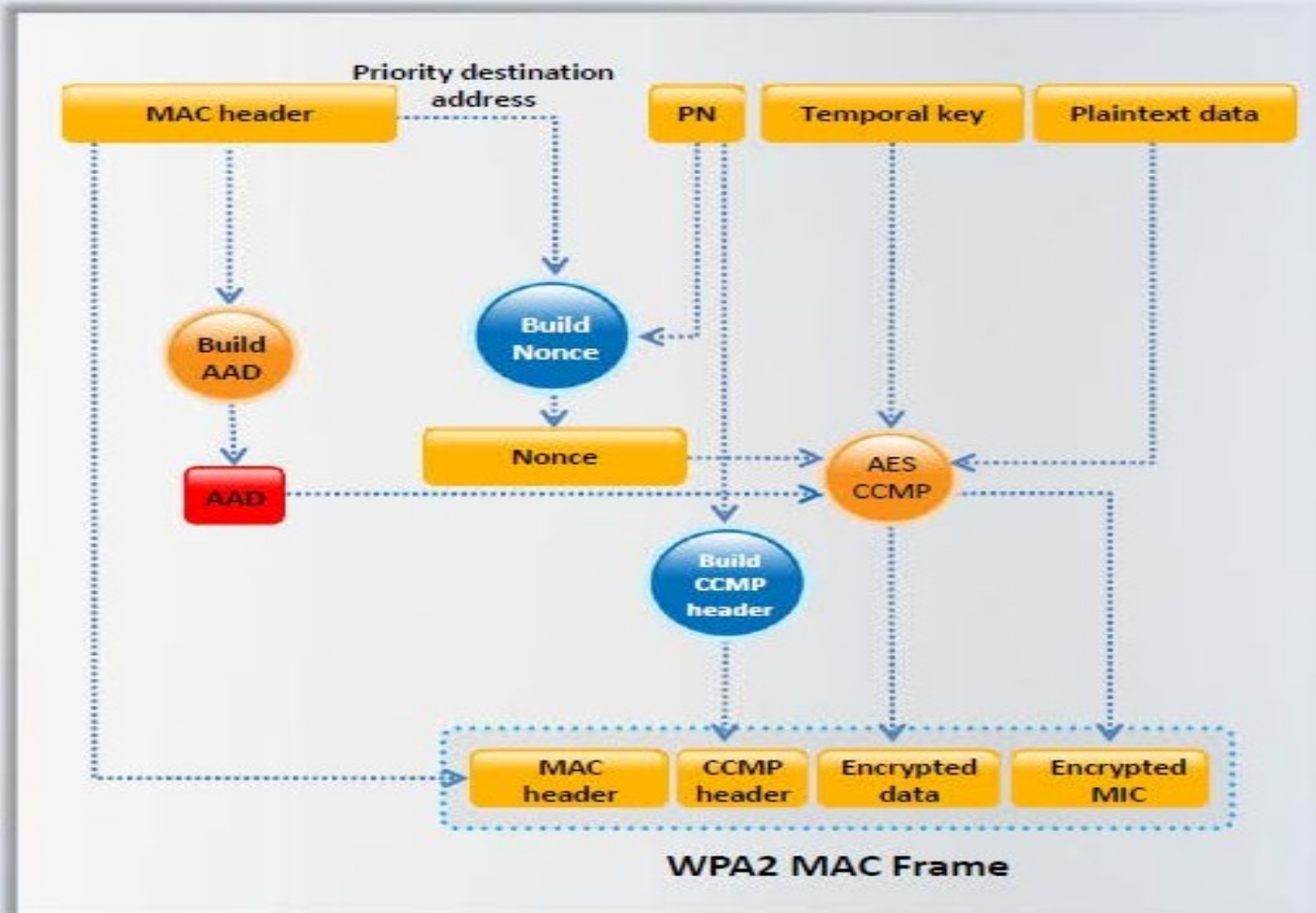
WEP vs. WPA vs. WPA2

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 is too small and is sent in the **cleartext** portion of a message	**7**	No defined method for **encryption key distribution**
2	**Identical key streams** are produced with the reuse of the same IV for data protection, as the IV is short key streams are repeated within short time	**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
3	**Lack of centralized key management** makes it difficult to change the WEP keys with any regularity	**9**	Associate and disassociate messages are **not authenticated**
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	**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
5	IV is a part of the RC4 encryption key, leads to a **analytical attack** that recovers the key after intercepting and analyzing a relatively small amount of traffic	**11**	WEP is based on a password, prone to **password cracking attacks**
6	Use of RC4 was designed to be a **one-time cipher** and not intended for multiple message use	**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

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

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

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

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

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

4 The way the keystream is constructed from the IV makes it susceptible to **weak key attacks** (FMS attack)

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

How to Break WEP Encryption
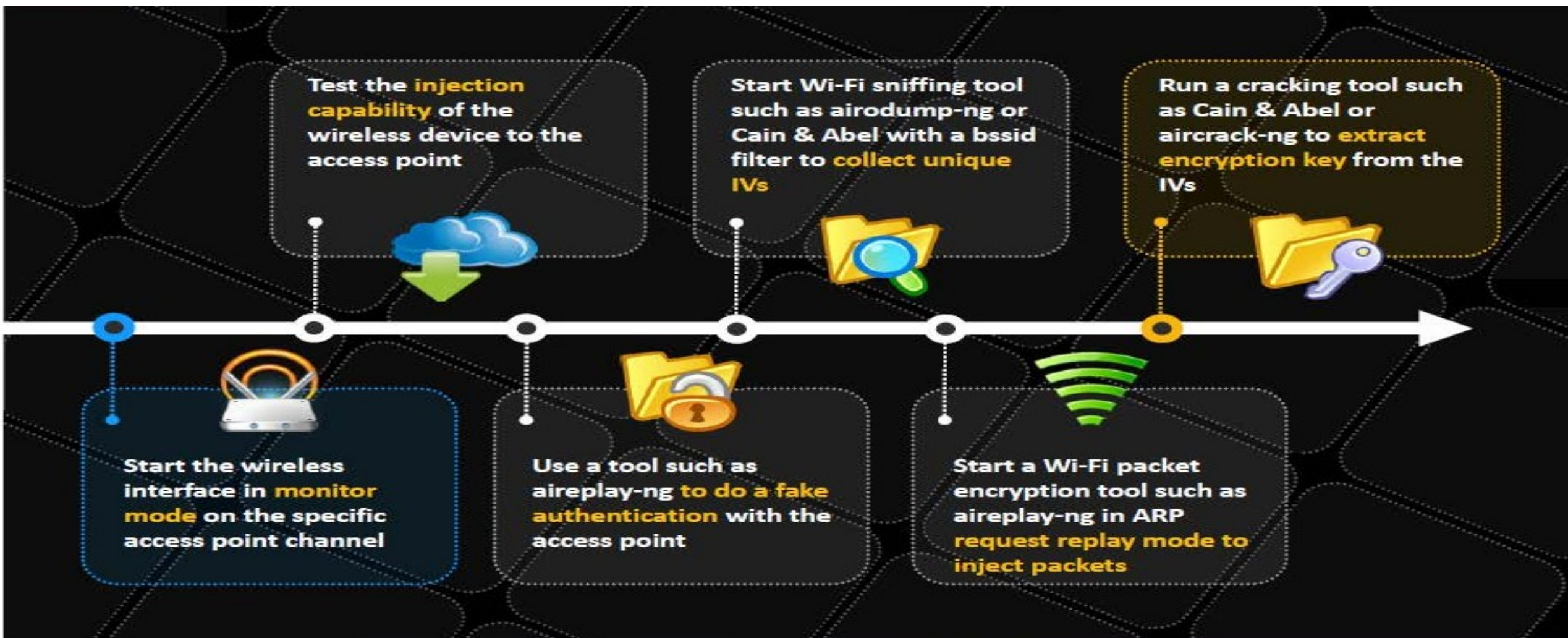
How to Break EPA Encryption

01 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

02 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**

03 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

04 Brute-Force WPA Keys

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

How to Defend Against WPA Cracking

Passphrases

- The only way to crack WPA is to sniff the **password PMK** associated with the "handshake" authentication process, and if this password is extremely complicated, it will be **almost impossible to crack**

Passphrase Complexity

- Select a **random passphrase** that is not made up of dictionary words
- Select a complex passphrase of a **minimum of 20 characters** in length and change it at regular intervals

Client Settings

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

Additional Controls

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

Module Flow

Wireless Threats: Access Control Attacks

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

1 War Driving

2 Rogue Access Points

3 MAC Spoofing

4 AP Misconfiguration

5 Ad Hoc Associations

6 Promiscuous Client

7 Client Mis-association

8 Unauthorized Association

Wireless Threats: Integrity Attacks

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

1 Data Frame Injection

2 WEP Injection

3 Bit-Flipping Attacks

4 Extensible AP Replay

5 Data Replay

6 Initialization Vector Replay Attacks

7 RADIUS Replay

8 Wireless Network Viruses

Wireless Threats: Confidentiality Attacks

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

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

Wireless Threats: Availability Attacks

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

Availability Attacks

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

Wireless Threats: Authentication Attacks

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

PSK Cracking	**Identity Theft**
LEAP Cracking	**Shared Key Guessing**
VPN Login Cracking	**Password Speculation**
Domain Login Cracking	**Application Login Theft**

Rogue Access Point Attack

Legit Company Wi-Fi Network
SSID: juggyboy
Wi-Fi Channel: 6

User Connecting to Rogue Access Point

My SSID is juggyboy Connect to me

Attacker

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

Control Room

Maintenance

Departure

Storage

Air Traffic Controller

Client Mis-association
SSID: juggyboy

Here is the Access Point

Attacker in the Neighboring Network

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

- Once associated, employees may **bypass** the enterprise security policies

Misconfigured Access Point Attack

Access Point Misconfigured
SSID: juggyboy
Wi-Fi password not configured

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

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

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

Connecting to juggyboy No password, Lucky Me!

Attacker

Unauthorized Association

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

Ad Hoc Connection Attack

Hotel Wi-Fi Network

Data Processing Room

Testing Room

User Enabled Wi-Fi ad Hoc Connection

Lounge

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

Attacker

HoneySpot Access Point Attack

SSID Verizon   SSID Vodafone   SSID McDonald's   SSID Starbucks Coffee   SSID at&t

Attacker traps victims by using fake hotspots
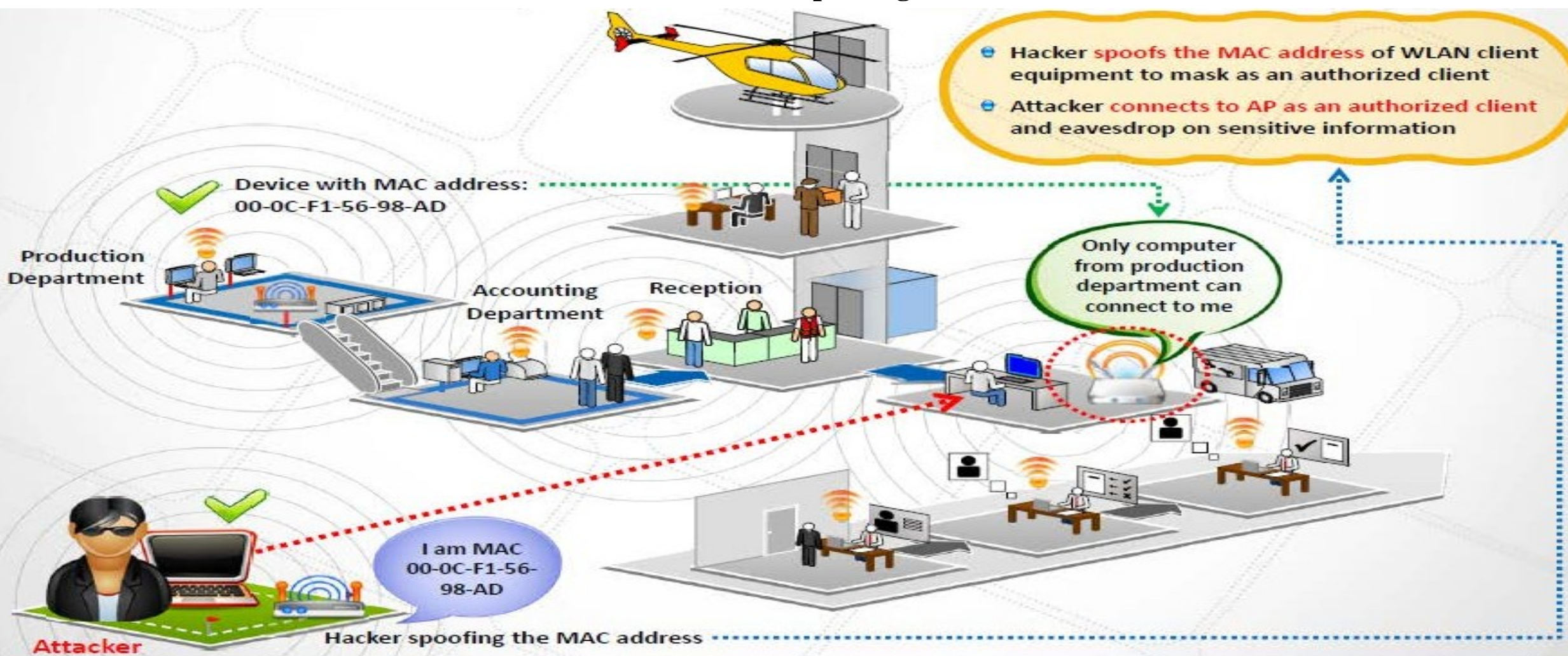
Attacker

Denial-of-Service Attack

Jamming Signal Attack

Attacker sending 2.4 GHz jamming signals

Attacker Jamming Device

- 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

- 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

Wi-Fi Jamming Devices

MGT- P6 GPS Jammer

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

MGT- MP200 Jammer

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

MGT- 03 Jammer

Range : 0 ~ 40 meters
4 antennas
Jammed:
- CDMA: 869 ~ 894 MHz
- GSM: 925 ~ 960 MHz
- DCS: 1805 1880 MHz
- 3G: 2110 ~ 2170 MHz

MGT- P6 Wi-Fi Jammer

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

MGT- P3x13 Jammer

Range : 50 ~ 200 meters
3 frequency bands
jammed:
- GSM: 925 ~ 960 Mhz
- DCS: 1805 ~ 1880 Mhz
- 3G: 2110 ~ 2170 Mhz

MGT- 04 WiFi Jammer

Range : 0 ~ 80 meters
4 Frequency bands
jammed:
- GSM: 925 ~ 960 Mhz
- DCS: 1805 ~ 1880 Mhz
- 3G: 2110 ~ 2170 Mhz
- WiFi / Bluetooth: 2400 ~ 2485 MHz
4 antennas

http://www.magnumtelecom.com

Module Flow

Wireless Concepts

Wireless Encryption

Wireless Threats

Wireless Hacking Methodology

Wireless Hacking Tools

Bluetooth Hacking

Countermeasures

Wireless Security Tools

Wi-Fi Pen Testing

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**

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

Attacker sniffs Wi-Fi traffic

Attacker sends a probe request

AP sends probe response
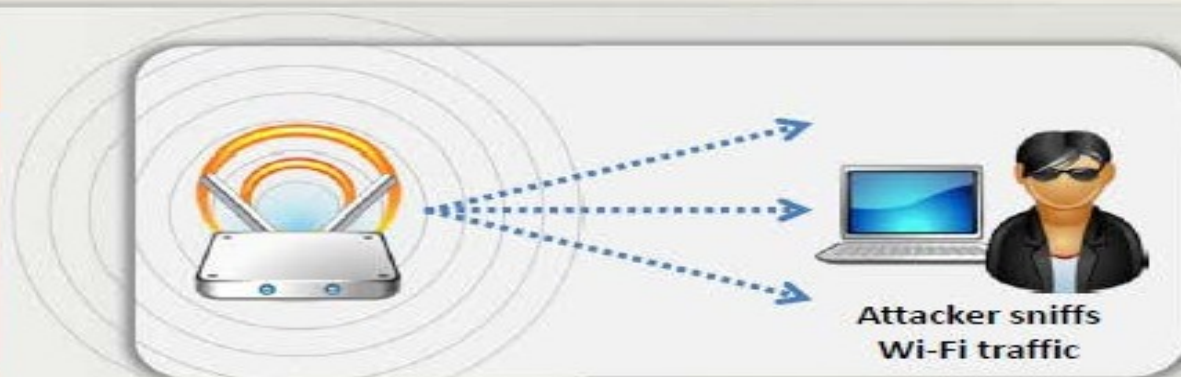
Active Footprinting Method

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
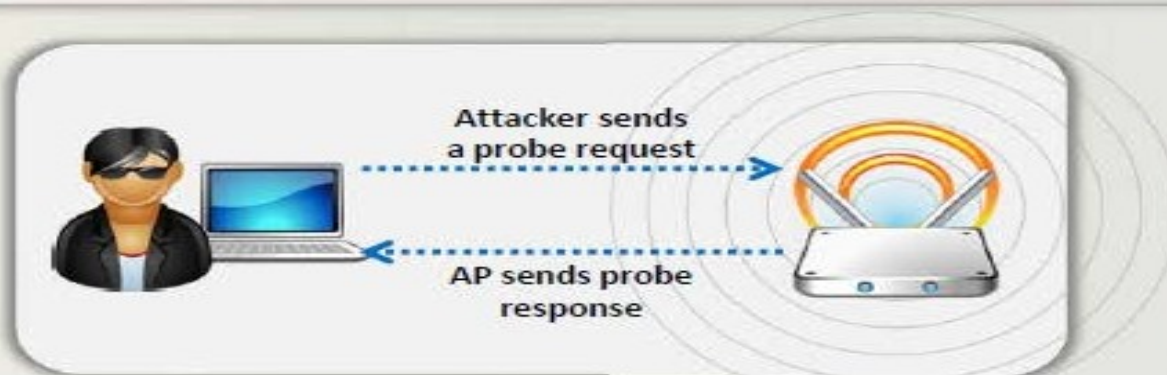
Find Wi-Fi Networks to Attack

Steps

1. 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
2. Drive around with **Wi-Fi enabled laptop** installed with a wireless discovery tool and map out active wireless networks

You will need these to discover Wi-Fi networks

Laptop with Wi-Fi Card

External Wi-Fi Antenna

Network Discovery Programs

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

Wi-Fi Discovery Tools: insider and NetSurveyor
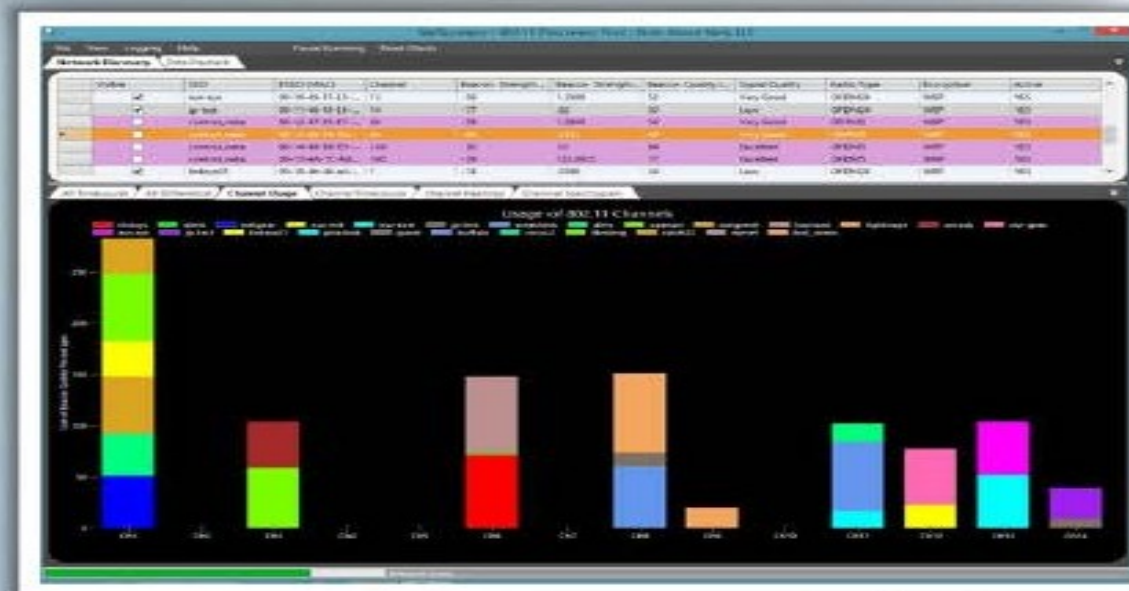
Wi-Fi Discovery Tools: Vistumbler and NetStumbler

Vistumbler

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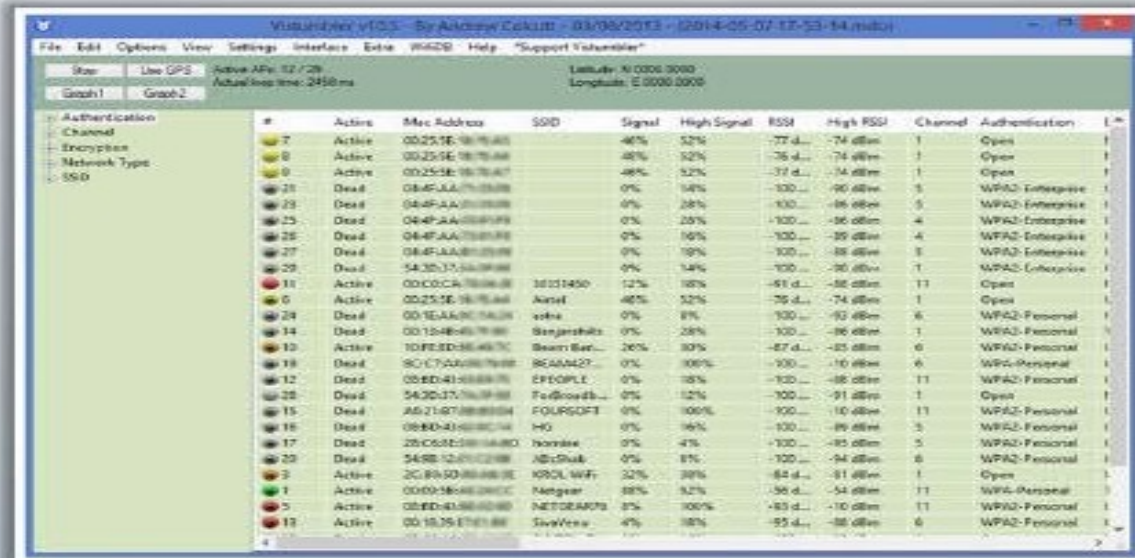
NetStumbler

- Facilitates detection of Wireless LANs using the **802.11b**, **802.11a**, and **802.11g** WLAN standards
- It is commonly used for **wardriving**, **verifying network configurations**, finding locations with poor coverage in one's WLAN, etc.

http://www.vistumbler.net

http://www.netstumbler.com
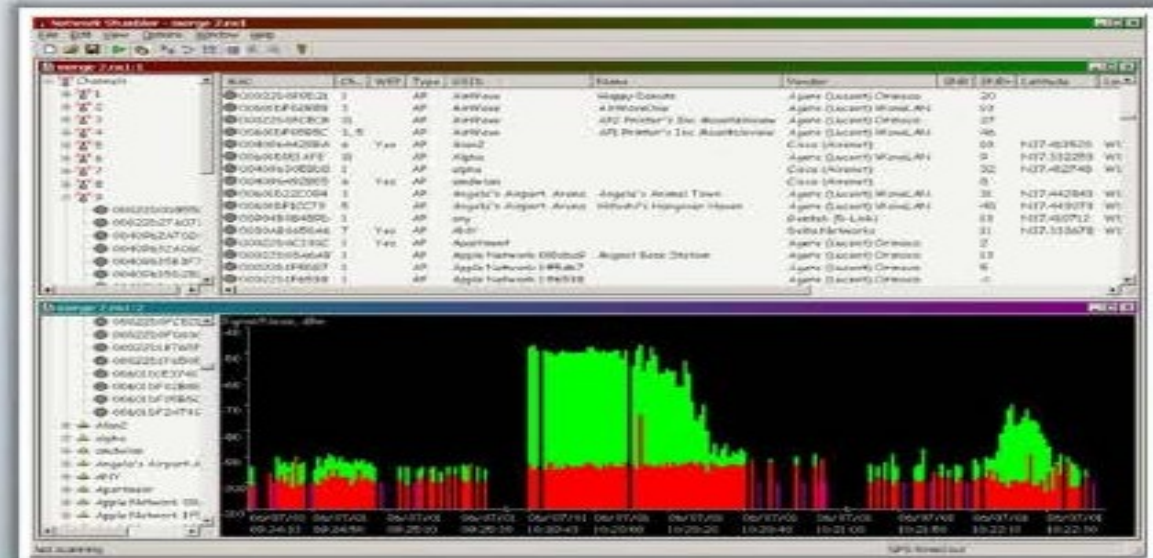
Wi-Fi Discovery Tools

WirelessMon
http://www.passmark.com

WiFinder
http://www.pgmsoft.com

Kismet
http://www.kismetwireless.net

Wellenreiter
http://wellenreiter.sourceforge.net

WiFi Hopper
http://www.wifihopper.com

AirCheck Wi-Fi Tester
http://www.flukenetworks.com

Wavestumbler
http://www.cqure.net

AirRadar 2
http://www.koingosw.com

iStumbler
http://www.istumbler.net

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

Mobile-based Wi-Fi Discovery Tools

WiFiFoFum -
WiFi
Scanner

http://www.wififofum.net

Network
Signal Info

http://www.kaibits-software.com

WiFi
Manager

http://kmansoft.com

OpenSignal
Maps

http://opensignal.com

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	

GPS Mapping

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

- GPS is used to **track the location** of the discovered Wi-Fi networks and the **coordinates are uploaded to sites** like WIGLE
- Attackers can **share this information** with the hacking community or sell it to make money

Attacker → **Discovery of Wi-Fi networks** → **Post the GPS locations to WIGLE**

GPS Mapping Tool: WiGLE

- **WiGLE consolidates location and information of wireless networks** world-wide to a central database, and provides user-friendly Java, Windows, and web applications that can map, query and update the database via the web

- You can **add a wireless network** to WiGLE from a stumble file or by hand and add remarks to an existing network

http://wigle.net
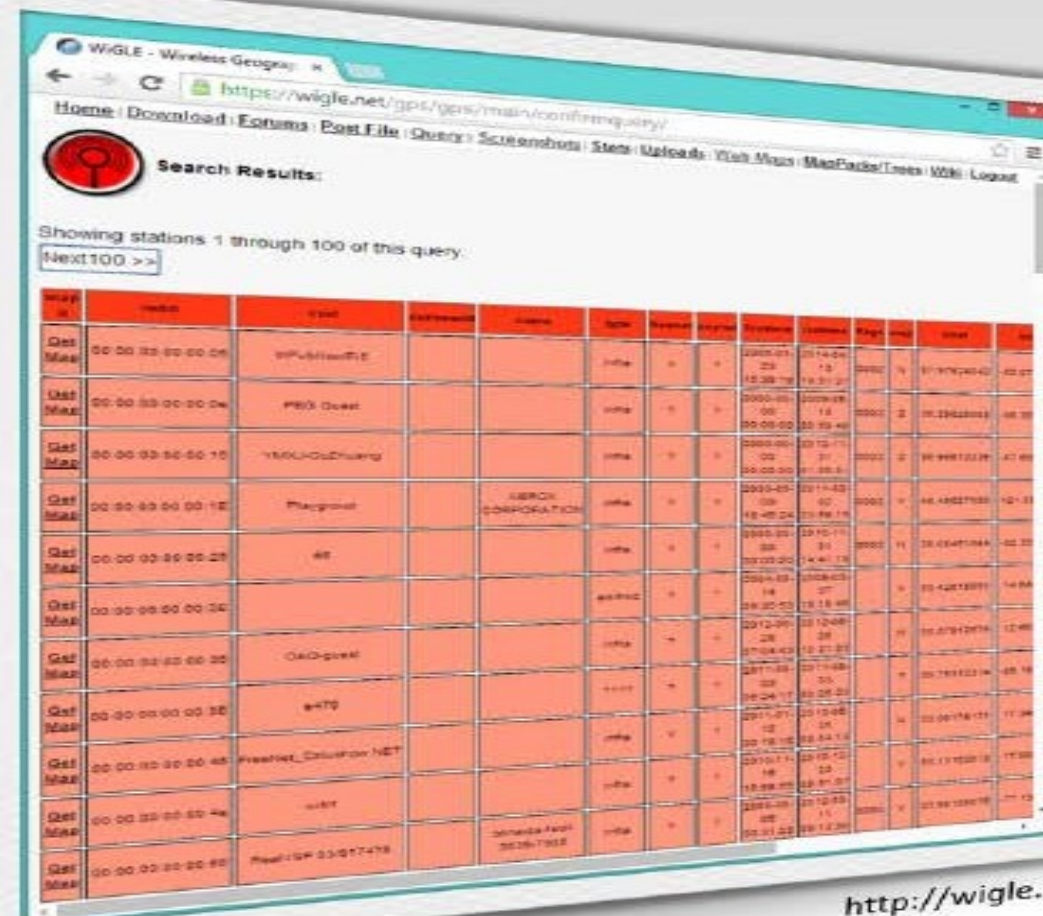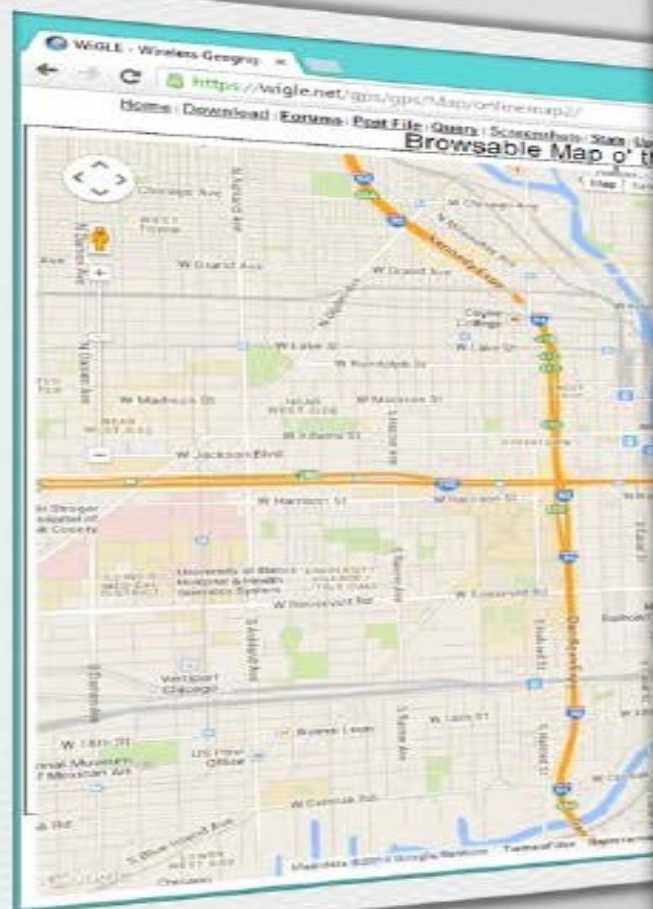
GPS Mapping Tool: Skyhook

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

http://www.skyhookwireless.com

Wi-Fi Hostpot Finder: Wi-Fi Finder

Wi-Fi Hostpot Finder: WeFi

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**

Wireless Traffic Analysis

Identify Vulnerabilities

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

Wi-Fi Reconnaissance

Attackers analyze a wireless network to determine:

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

Tools

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

- Wireshark/Pilot Tool
- OmniPeek Tool
- CommView Tool
- AirMagnet Wi-Fi Analyzer

Wi-Fi USB Dongle: AirPcap

Wi-Fi Packet Sniffer: Wireshark with AirPcap

Wi-Fi Packet Sniffer: Steel Central Packet Analyzer
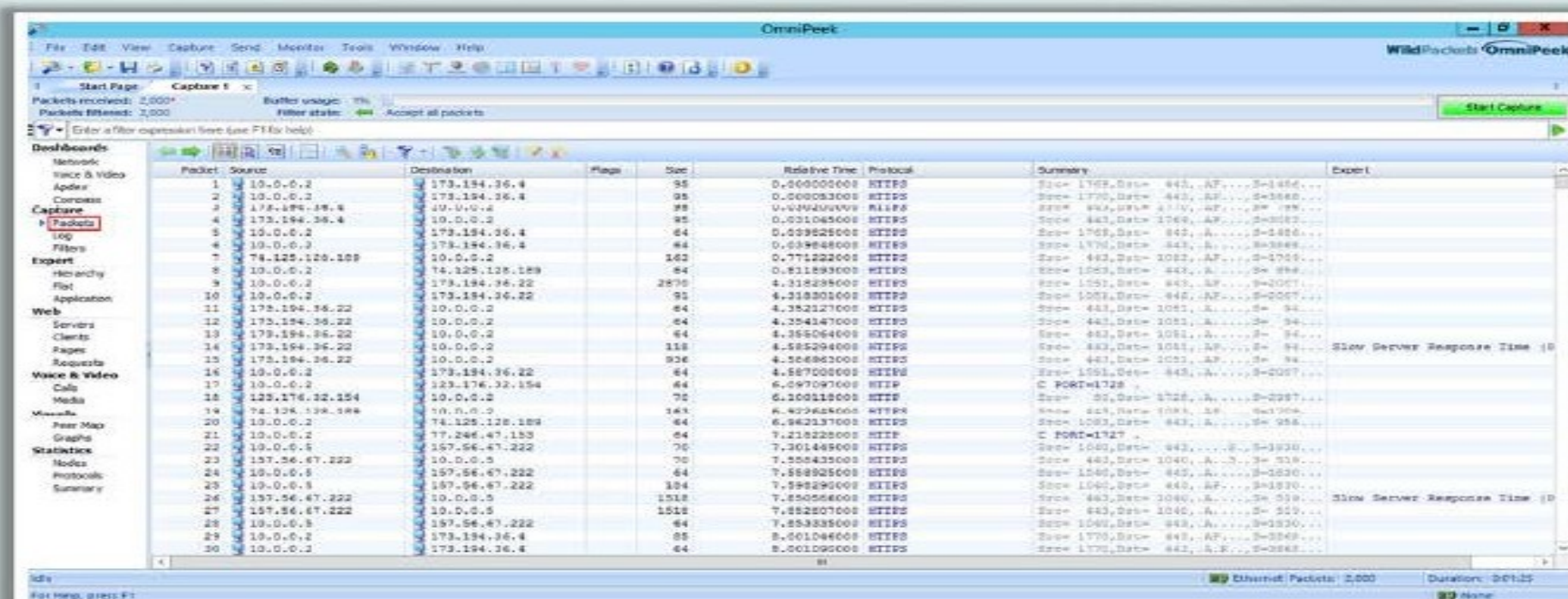
- It measures wireless channel utilization
- It helps in Identifying **rogue wireless networks** and stations
- It isolates specific packets
- It provides an interactive and visually-oriented **user interface**
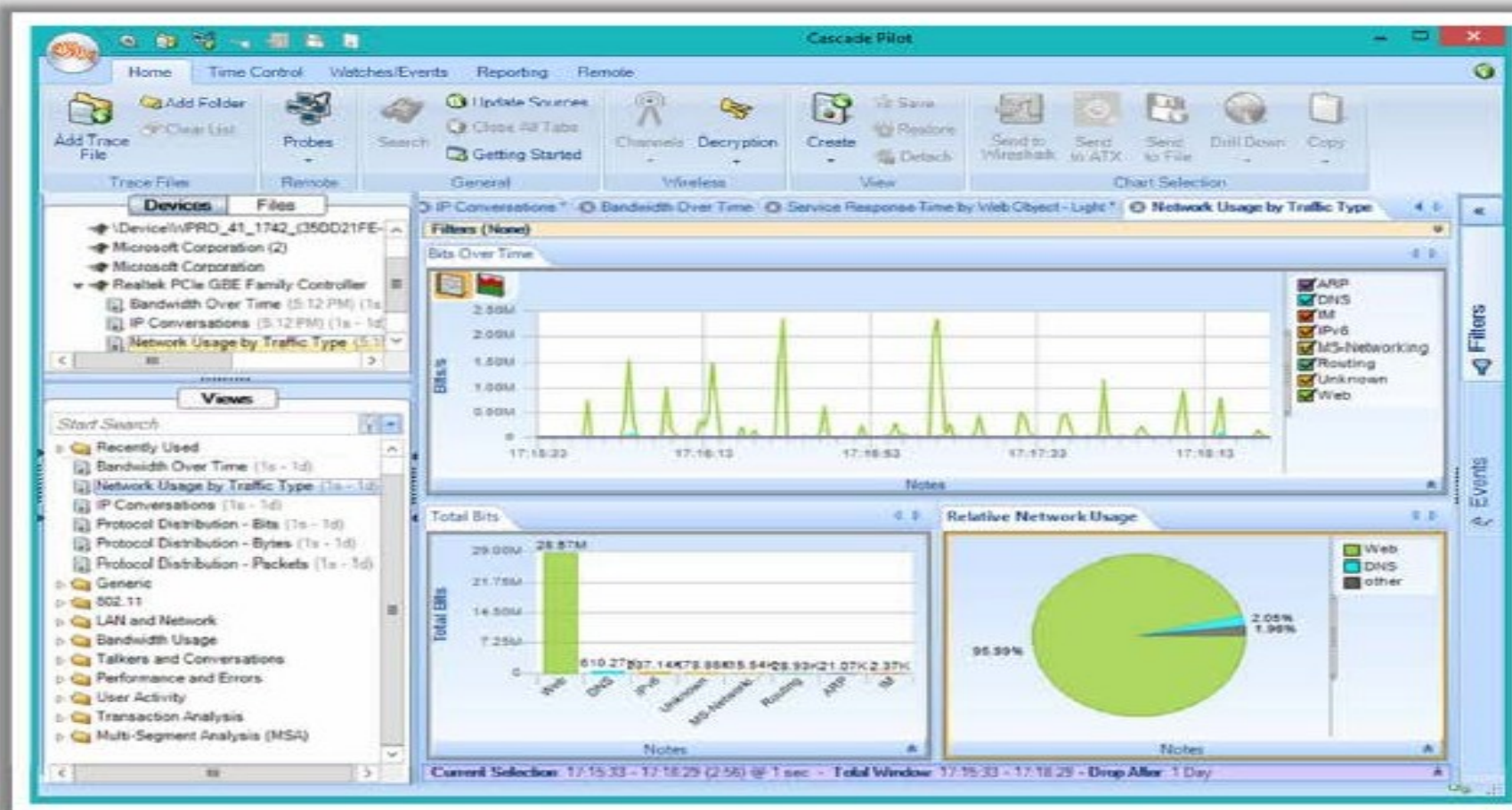
Wi-Fi Packet Sniffer: OmniPeek Network Analyzer

- OmniPeek Network Analyzer offers **real-time visibility and analysis** of the network traffic from a single interface, including Ethernet, 802.11a/b/g/n wireless and VoIP

- It provides a comprehensive view of all **wireless network activity** showing each wireless network, the APs comprising that network, and the users connected to each AP

http://www.wildpackets.com

Wi-Fi Packet Sniffer: CommView for Wi-Fi

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

Features

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

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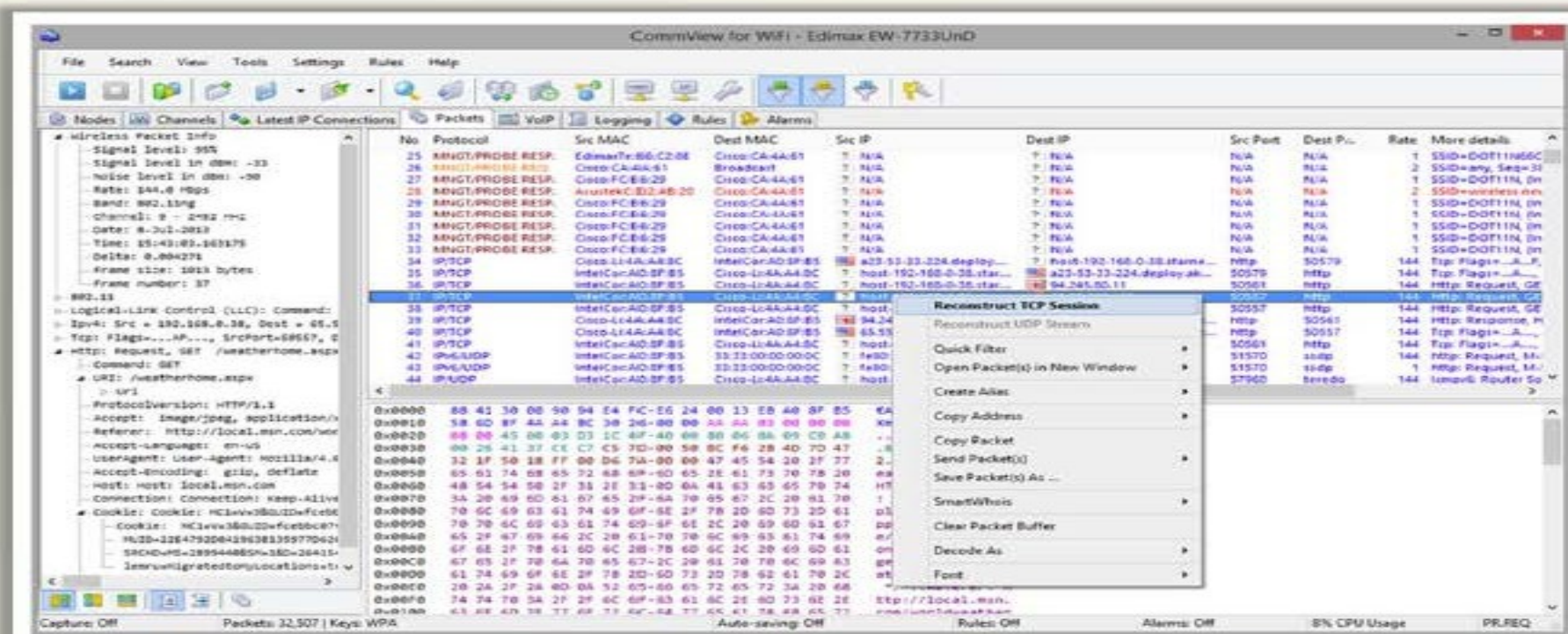
What is Spectrum Analysis?

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

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

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

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

- **Spectrum Analysis Tools**
  - Wi-Spy and Chanalyzer
  - AirMagnet Wi-Fi Analyzer
  - WifiEagle
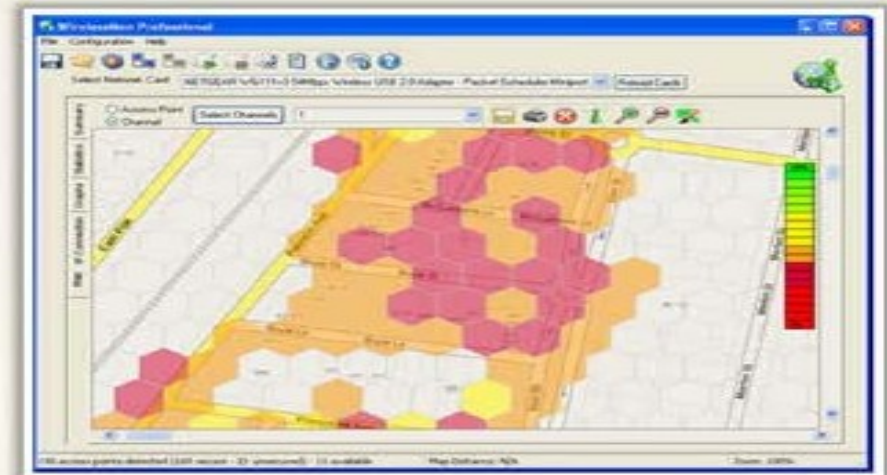
Wi_Fi Packet Sniffers

Sniffer Portable Professional Analyzer
http://www.netscout.com

Airview
http://airview.sourceforge.net

Capsa
http://www.colasoft.com

Observer
http://www.networkinstruments.com

PRTG Network Monitor
http://www.paessler.com

WifiScanner
http://wifiscanner.sourceforge.net

ApSniff
http://www.monolith81.de

Mognet
http://www.monolith81.de

NetworkMiner
http://www.netresec.com

AirTraf
http://www.elixar.com

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**

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

Hoe to Reveal Hidden SSIDs

Fragmentation Attack

A fragmentation attack, when successful, can obtain **1500 bytes of PRGA** (pseudo random generation algorithm)

This attack **does not recover** the WEP key itself, but merely obtains the PRGA

The PRGA can then be used to generate packets with **packetforge-ng** which are in turn used for various injection attacks

It requires at least **one data packet** to be received from the access point in order to initiate the attack

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

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

```
Saving chosen packet in replay_src-0124-161120.cap
Data packet found!
Sending fragmented packet
Got RELAYED packet!!
Thats our ARP packet!          PRGA is stored in the file
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
```

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

How to Launch MAC Spoofing Attack

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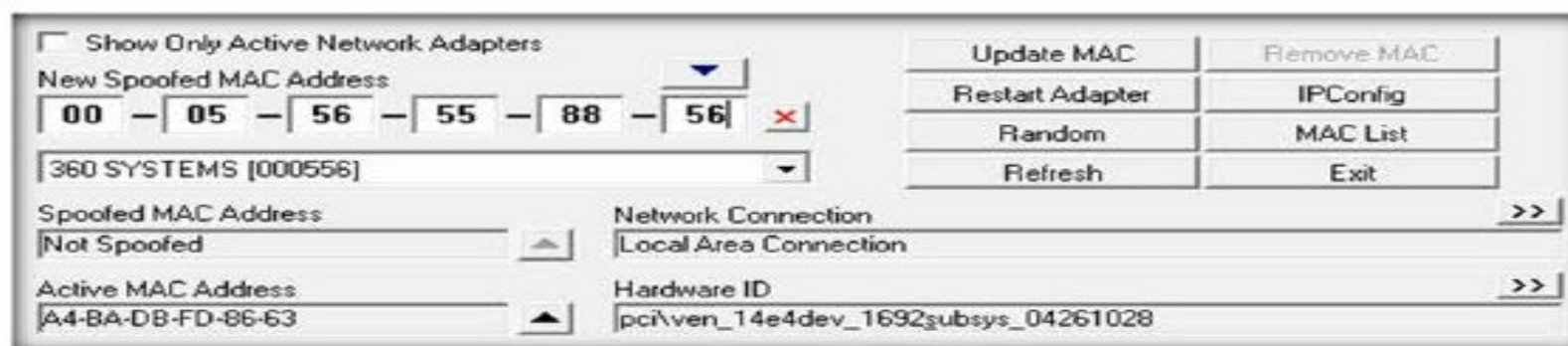
Linux Shell

[root@localhost root]# **ifconfig wlan0 down** ◄·············· 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

☐ Show Only Active Network Adapters

New Spoofed MAC Address

`00` — `05` — `56` — `55` — `88` — `56` ✕

360 SYSTEMS [000556]

Spoofed MAC Address
Not Spoofed

Network Connection
Local Area Connection

Active MAC Address
A4-BA-DB-FD-86-63

Hardware ID
pci\ven_14e4dev_1692subsys_04261028

Update MAC | Remove MAC
Restart Adapter | IPConfig
Random | MAC List
Refresh | Exit

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

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

Denial of Service: Deauthentication and Disassociation Attack

Man-in-the-Middle Attack

MITM Attack Using Aircrack-ng

Wireless ARP Poisoning Attack

Access Point1

Traffic is no longer sent to AP2

Access Point2

MAC Address 04-A4-52-33-61

MAC Address 00-45-B8-74-03

Attacker uses ARP Poisoning tool such as Cain & Abel

Attacker's System

Jessica's Wireless Laptop

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

Rogue Access Point

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

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

- Choose an **appropriate location** to plug in your rogue access point that allows maximum coverage from your connection point

- Disable the **SSID Broadcast** (silent mode) and any management features to avoid detection

- Place the access point behind a **firewall**, if possible, to avoid network scanners

- Deploy a **rogue access point** for short period

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

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

Evil Twin

Authorized Wi-Fi

SSID: STARBUCKS

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

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

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

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

Evil Twin

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

How to Set 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 8 or Internet Sharing in Mac OS X
- Broadcast your Wi-Fi connection and run a **sniffer program** to capture passwords
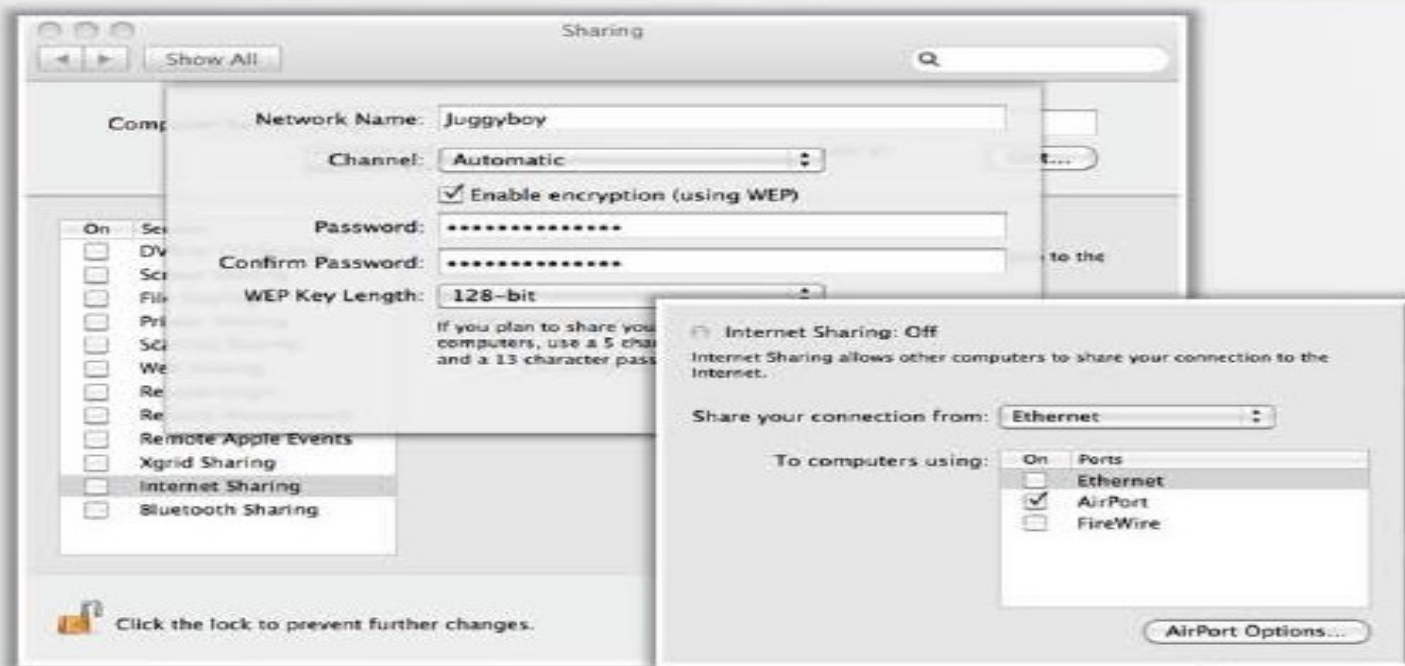
A user tries to log in and finds *two access points*. One is legitimate, while the other is an identical fake (evil twin). Victim picks one, if it's the fake, the hacker gets *login information* and access to the computer. In the meantime, the user goes nowhere. He or she probably thinks it was just a *login attempt* that randomly failed.

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**

How to Crack WEP Using Aircrack

How to Crack WEP Using Aircrack (Cont'd)

Command Prompt

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

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

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

Command Prompt

```
C:\>aircrack-ng -s capture.ivs
Opening capture.ivs
Read  75168 packets.

                        Aircrack-ng 0.7 r130
                [00:00:10] Tested 77 keys (got 684002 IVs)

KB depth byte(vote)
0 0/ 1 AE( 199) 29( 27) 2D( 13) 7C( 12) FE( 12) FF( 6) 39( 5) 2C( 3) 00( 0) 08( 0)
1 0/ 3 66( 41) F1( 33) 4C( 23) 00( 19) 9F( 19) C7( 18) 64( 9) 7A( 9) 7B( 9) F6( 9)
2 0/ 2 5C( 89) 52( 60) E3( 22) 10( 20) F3( 18) 8B( 15) 8E( 15) 14( 13) D2( 11) 47( 10)
3 0/ 1 FD( 375) 81( 40) 1D( 26) 99( 26) D2( 23) 33( 20) 2C( 19) 05( 17) 0B( 17) 35( 17)
                        KEY FOUND! [ AE:66:5C:FD:24 ]
```

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

How to Crack WPA-PSK Using Aircrack

Step 1

Monitor wireless traffic with **airmon-ng**

`C:\>airmon-ng start eth1`

Step 2

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

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

How to Crack WPA-PSK Using Aircrack(Cont'd)
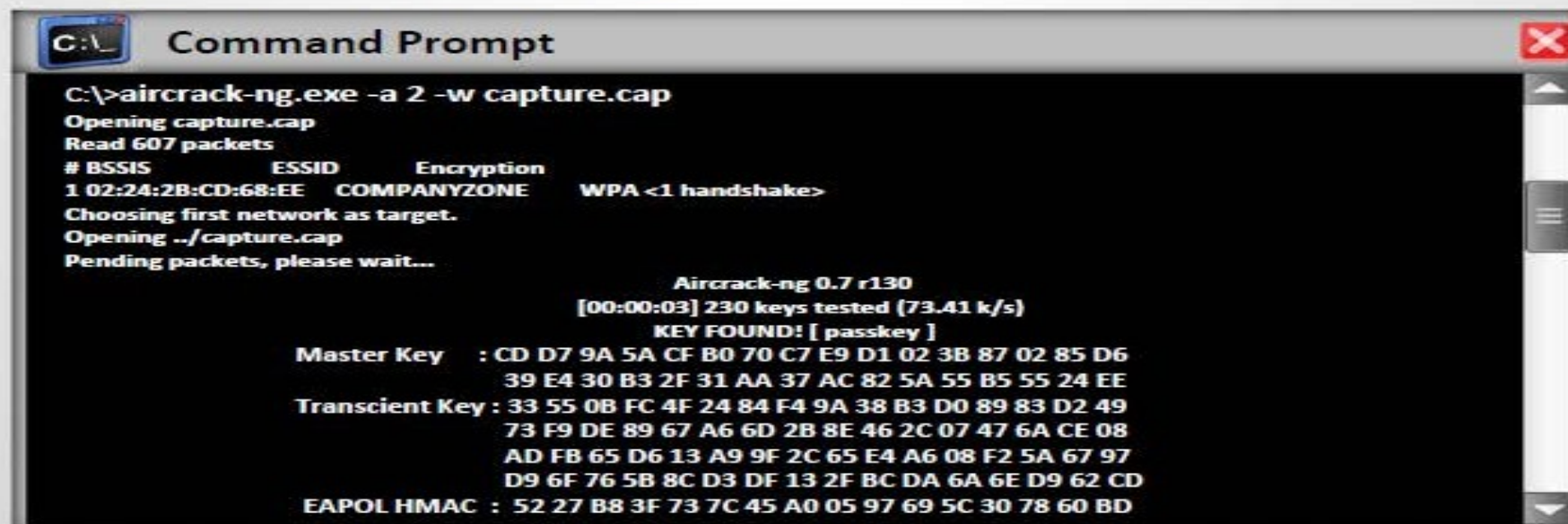
Step 3: De-authenticate (deauth) the client using Aireplay-ng. The client will try to authenticate with AP which will lead to **airodump** capturing an authentication packet (WPA handshake)

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

WPA Cracking Tool: KisMAC

http://trac.kismac-ng.org

WEP Cracking Using Cain & Abel

WEP Brute Forcing Using Cain & Abel

Cain can **recover passwords** by sniffing the wireless network, and **crack WPA-PSK encrypted passwords** using dictionary and brute-force attacks
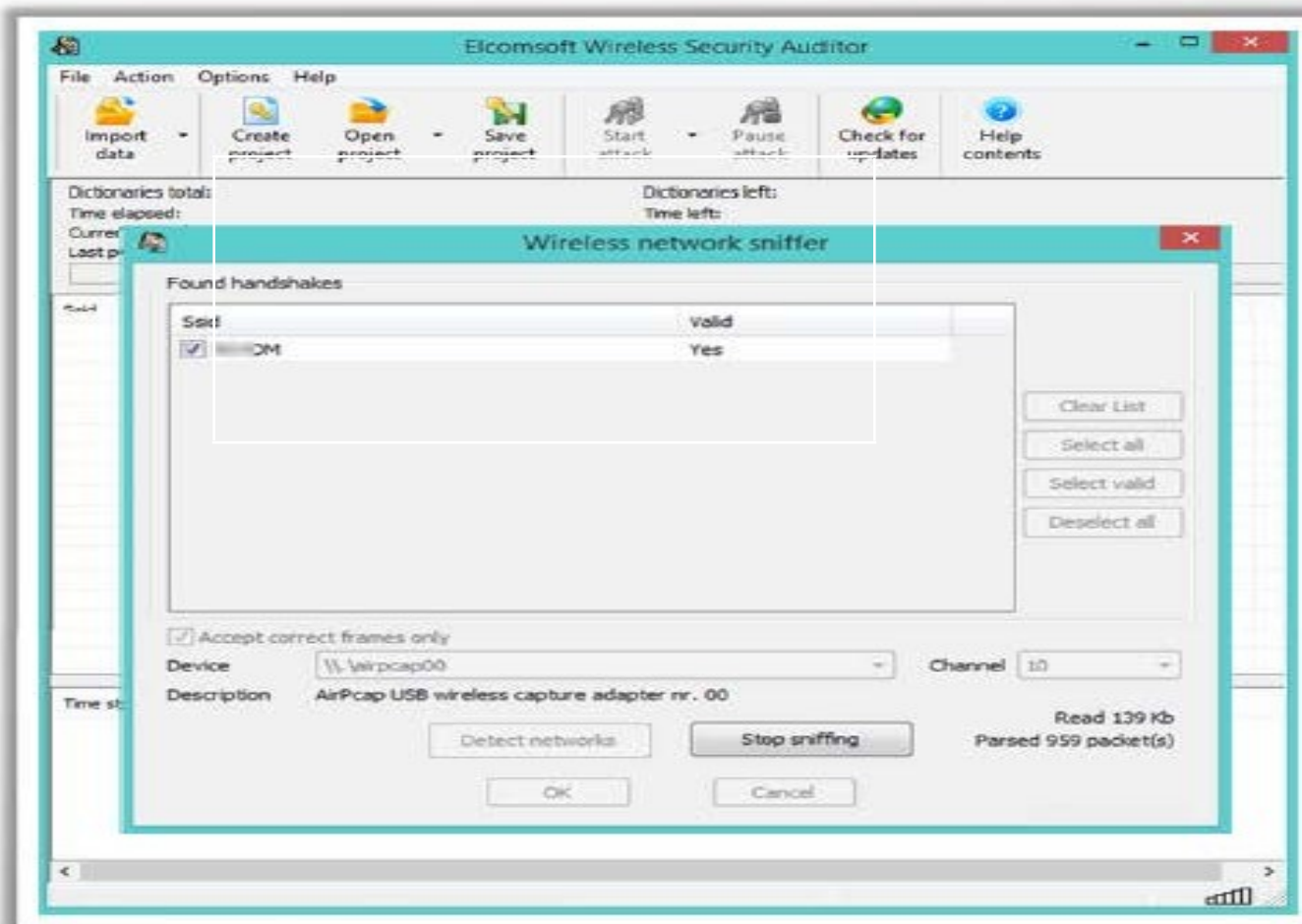
WEP Cracking Tool: Elcomsoft Wireless Security Auditor

Elcomsoft Wireless Security Auditor allows network administrators to **audit accessible wireless networks**

It comes with a built-in **wireless network sniffer** (with AirPcap adapters)

It tests the strength of **WPA/WPA2-PSK passwords** protecting your wireless network

http://www.elcomsoft.com

WEP/WPA Cracking Tools

WepAttack
http://wepattack.sourceforge.net

Portable Penetrator
http://www.secpoint.com

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

CloudCracker
https://www.cloudcracker.com

Reaver Pro
https://code.google.com

coWPAtty
http://wirelessdefence.org

WEPCrack
http://wepcrack.sourceforge.net

Wifite
http://code.google.com

WepDecrypt
http://wepdecrypt.sourceforge.net

WepCrackGui
http://wepcrackgui.sourceforge.net

WEP/WPA Cracking Tool for Mobile: Penetrate Pro

- Penetrate Pro android app allows you to **decode and access a secure Wi-Fi network** from Android smartphone and devices

- The app **calculates WEP/WPA keys** for some Wi-Fi routers and lets you to get access by using the password

- Penetrate Pro calculates WEP/WPA keys for various wireless routers such as **Thomson, Discus, Infinitum**, BBox, DMax, Orange, SpeedTouch, DLink, Eircom, BigPond, O2Wireless routers, etc.
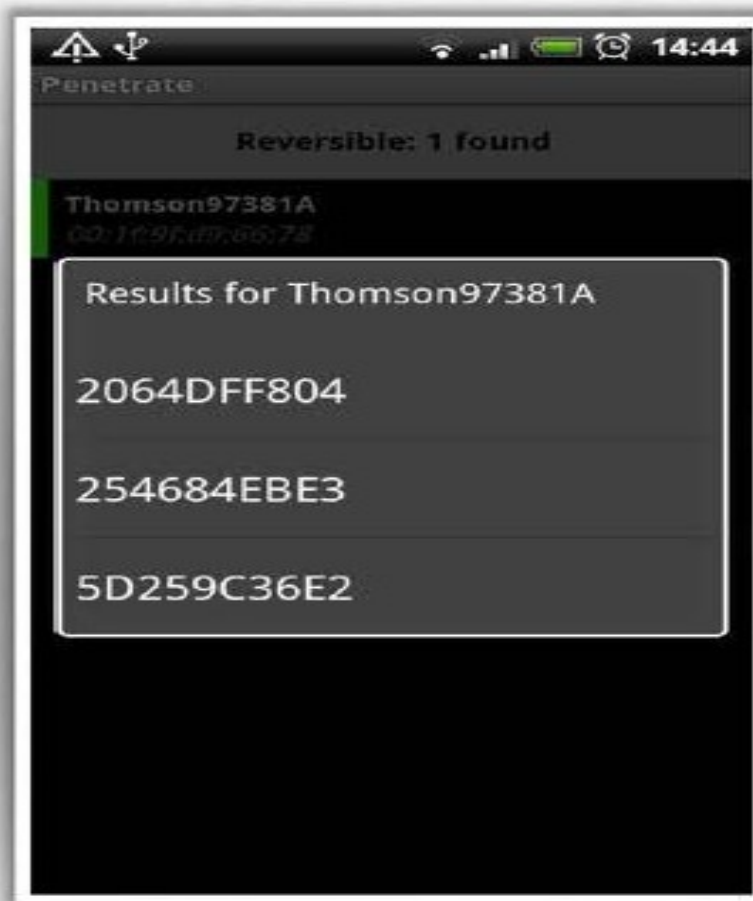
Reversible: 1 found

Thomson97381A
00:1f:9f:d9:66:78

Results for Thomson97381A

2064DFF804

254684EBE3

5D259C36E2

http://getandroidstuff.com

Module Flow

Wi-Fi Sniffer: Kismet

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

2 It **identifies networks** by passively collecting packets and detecting standard named networks

3 It **detects hidden networks** and presence of nonbeaconing networks via data traffic

http://www.kismetwireless.net

Wardriving Tools

Airbase-ng
http://aircrack-ng.org

ApSniff
http://www.monolith81.de

WiFiFoFum
http://www.wififofum.net

MiniStumbler
http://www.netstumbler.com

WarLinux
http://sourceforge.net

MacStumbler
http://www.macstumbler.com

WiFi-Where
http://www.threejacks.com

AirFart
http://airfart.sourceforge.net

AirTraf
http://airtraf.sourceforge.net

802.11 Network Discovery Tools
http://wavelan-tools.sourceforge.net

RF Monitoring Tools

NetworkManager https://wiki.gnome.org		**xosview** http://xosview.sourceforge.net	
KWiFiManager http://kwifimanager.sourceforge.net		**RF Monitor** http://www.newsteo.com	
NetworkControl http://www.arachnoid.com		**DTC-340 RFXpert** http://www.dektec.com	
Sentry Edge II http://www.tek.com		**Home Curfew RF Monitoring System** http://solutions.3m.com	
WaveNode http://www.wavenode.com		**SigMon** http://www.sat.com	

Wi-Fi Traffic Analyzer Tools

AirMagnet WiFi Analyzer *http://www.flukenetworks.com*	**OneTouch™ AT Network Assistant** *http://www.flukenetworks.com*
OptiView® XG Network Analysis Tablet *http://www.flukenetworks.com*	**Capsa Network Analyzer** *http://www.colasoft.com*
Observer *http://www.netinst.com*	**SoftPerfect Network Protocol Analyzer** *http://www.softperfect.com*
Ufasoft Snif *http://ufasoft.com*	**OmniPeek Network Analyzer** *http://www.wildpackets.com*
vxSniffer *http://www.cambridgevx.com*	**CommView for WiFi** *http://www.tamos.com*

Wi-Fi Raw Packet Capturing and Spectrum Analyzing Tools

Raw Packet Capturing Tools

WirelessNetView
http://www.nirsoft.net

Tcpdump
http://www.tcpdump.org

Airview
http://airview.sourceforge.net

RawCap
http://www.netresec.com

Airodump-ng
http://www.aircrack-ng.org

Spectrum Analyzing Tools

Cisco Spectrum Expert
http://www.cisco.com

AirMedic® USB
http://www.flukenetworks.com

AirSleuth-Pro
http://nutsaboutnets.com

BumbleBee-LX Spectrum Analyzer
http://www.bvsystems.com

Wi-Spy
http://www.metageek.net

Wireless Hacking Tools for Mobile: WiHack and Backtrack Simulator

WiHack

- WiHack is a program for hacking Wi-Fi, which is able to crack WPA, WPA2, and WEP keys

Backtrack Simulator

- Backtrack Simulator is simulated with Fern Wi-Fi Cracker, Fern Wi-Fi Cracker can crack WEP, WPA, and WPA2 secured wireless networks

https://wihack.com

https://play.google.com

Module Flow

Wireless Concepts

Wireless Encryption

Wireless Threats

Wireless Hacking Methodology

Wireless Hacking Tools

Bluetooth Hacking

Countermeasures

Wireless Security Tools

Wi-Fi Pen Testing

Bluetooth Hacking

- Bluetooth hacking refers to **exploitation of Bluetooth stack implementation vulnerabilities** to compromise sensitive data in Bluetooth-enabled devices and networks
- Bluetooth enabled devices connect and communicate wirelessly through **ad hoc** networks known as **Piconets**

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 Stack

Middleware Protocol Group

- Application
  - OBEX
  - TCP/IP
  - AT
  - PPP
  - RFCOMM
  - TCS
  - SDP
  - L2CAP

- HCI

Transport Protocol

- Link Manager
- Audio
- Baseband
- Bluetooth Radio
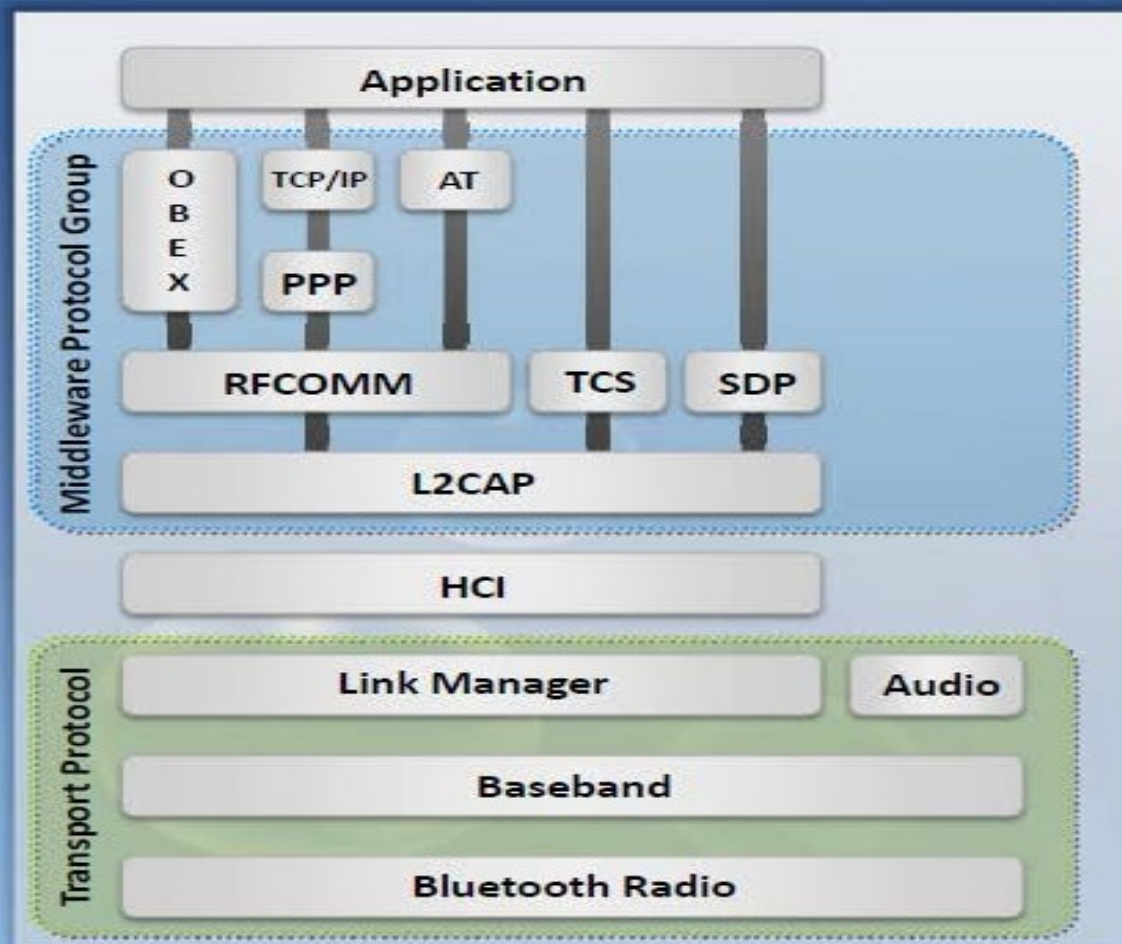
Bluetooth Modes

Discoverable modes

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

Pairing modes

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

Bluetooth Threats

Leaking Calendars and Address Books

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

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

STEP 2

STEP 3

STEP 4

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
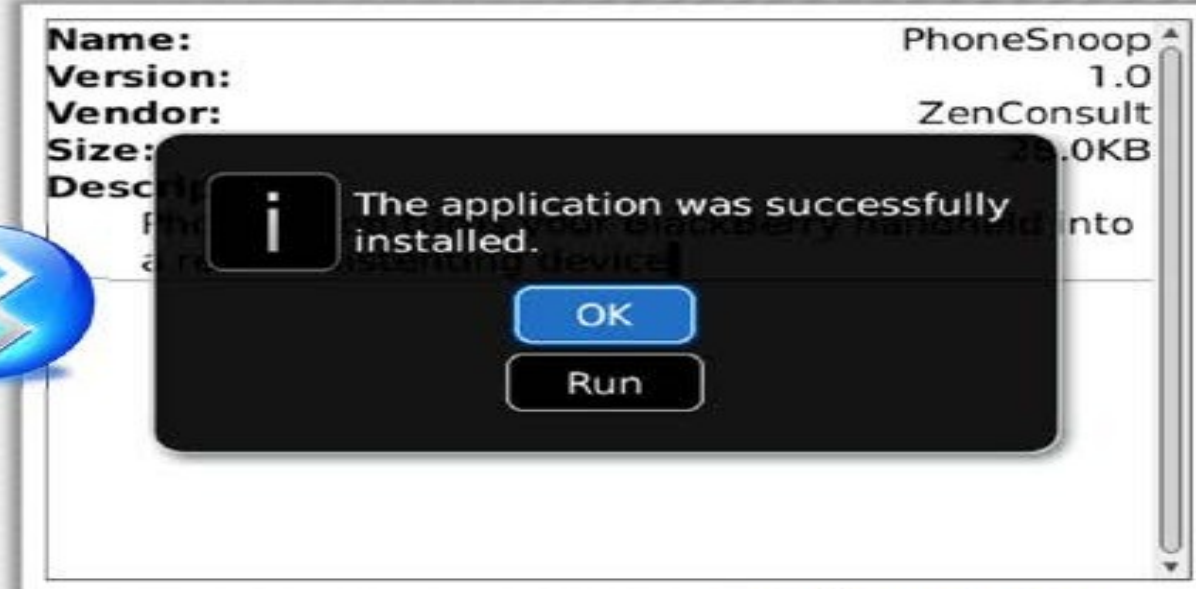- Choose "send via Bluetooth". These searches for any Bluetooth device within range

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 Tool: PhoneSnoop

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

- It exists **solely to demonstrate** the capabilities of a BlackBerry handheld when used to conduct surveillance on an individual

- It is purely a **proof-of-concept application** and does not possess the stealth or spyware features that could make it malicious

Name: PhoneSnoop
Version: 1.0
Vendor: ZenConsult
Size: 29.0KB
Descri

The application was successfully installed.

OK

Run

http://www.blackberryrc.com

01

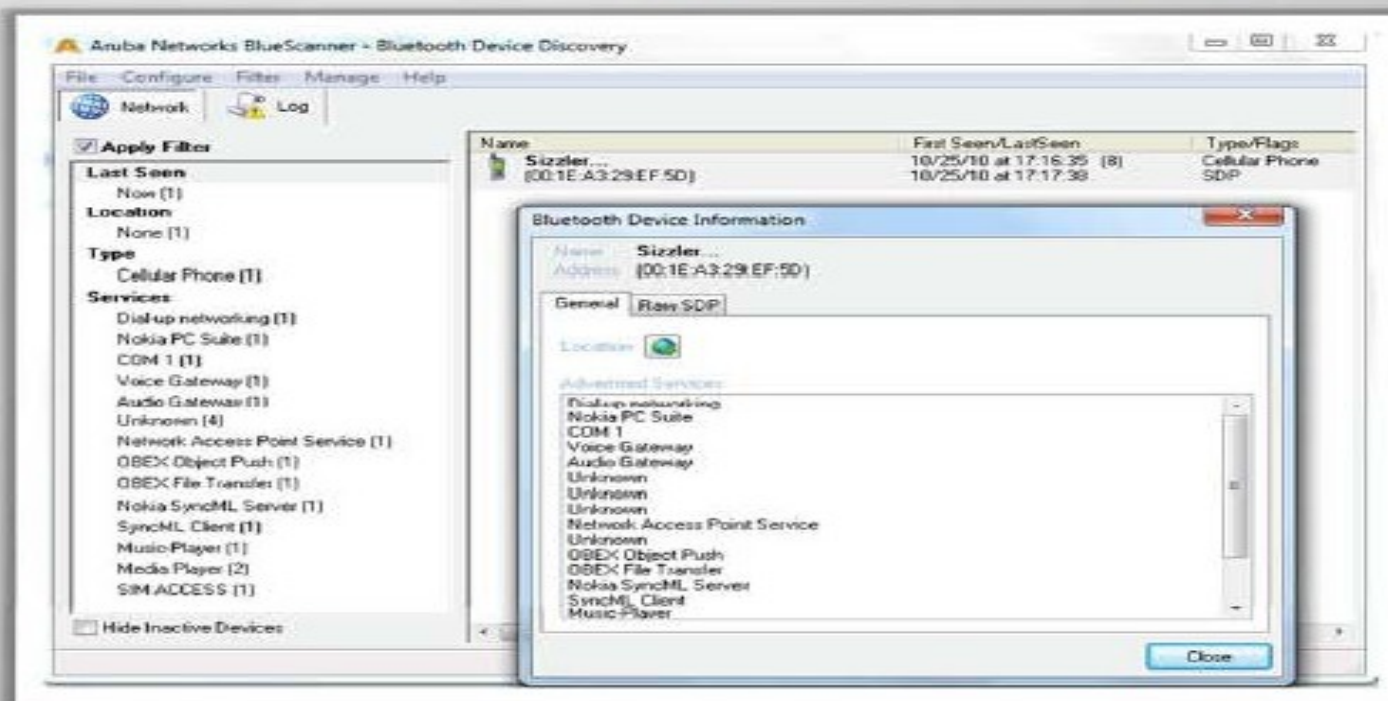A Bluetooth **device discovery** and vulnerability assessment tool for Windows

Discover **Bluetooth devices type** (phone, computer, keyboard, PDA, etc.), and the services that are advertised by the devices

02

03

Records all information that can be gathered from the device, without attempting to authenticating with the remote device

http://www.arubanetworks.com

Bluetooth Hacking Tools

BH BlueJack
http://croozeus.com

btscanner
http://www.pentest.co.uk

Bluesnarfer
http://www.alighieri.org

CIHwBT
http://sourceforge.net

btCrawler
http://www.silentservices.de

BT Audit
http://trifinite.org

Bluediving
http://bluediving.sourceforge.net

Blue Alert
http://www.bluejackingtools.com

Blooover II
http://trifinite.org

Blue Sniff
http://bluesniff.shmoo.com

Module Flow

Wireless Concepts

Wireless Encryption

Wireless Threats

Wireless Hacking Methodology

Wireless Hacking Tools

Bluetooth Hacking

Countermeasures

Wireless Security Tools

Wi-Fi Pen Testing

How to Defend Against Bluetooth Hacking

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

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

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

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

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

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

How to Defend Against Bluetooth Hacking(Cont'd)

1 Set Bluetooth-enabled device **network range to the lowest** and perform pairing only in a **secure area**

2 Install **antivirus** which support host-based security software on Bluetooth-enabled devices

3 Change the default settings of the Bluetooth-enabled device to a **best security standard**

4 Use **Link Encryption** for all Bluetooth connections

5 If multiple wireless communication is being used, make sure that **encryption is empowered** on each link in the communication chain

Detecting Rogue AP

RF Scanning

Re-purposed access points that do only packet capturing and analysis (RF sensors) are plugged in all over the wired network to detect and warn the WLAN administrator about any wireless devices operating in the area

AP Scanning

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

Using Wired Side Inputs

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

Blocking Rogue AP

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

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

Wireless Security Layers

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 Wireless Attacks

Configuration Best Practices

Change the **default SSID** after WLAN configuration

Set the **router access password** and enable firewall protection

Disable **SSID broadcasts**

SSID Settings Best Practices

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

Authentication Best Practices

Configuration Best Practices

SSID Settings Best Practices

Authentication 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

Configuration Best Practices
- Choose Wi-Fi Protected Access (WPA) instead of WEP
- Implement WPA2 Enterprise wherever possible
- Disable the network when not required

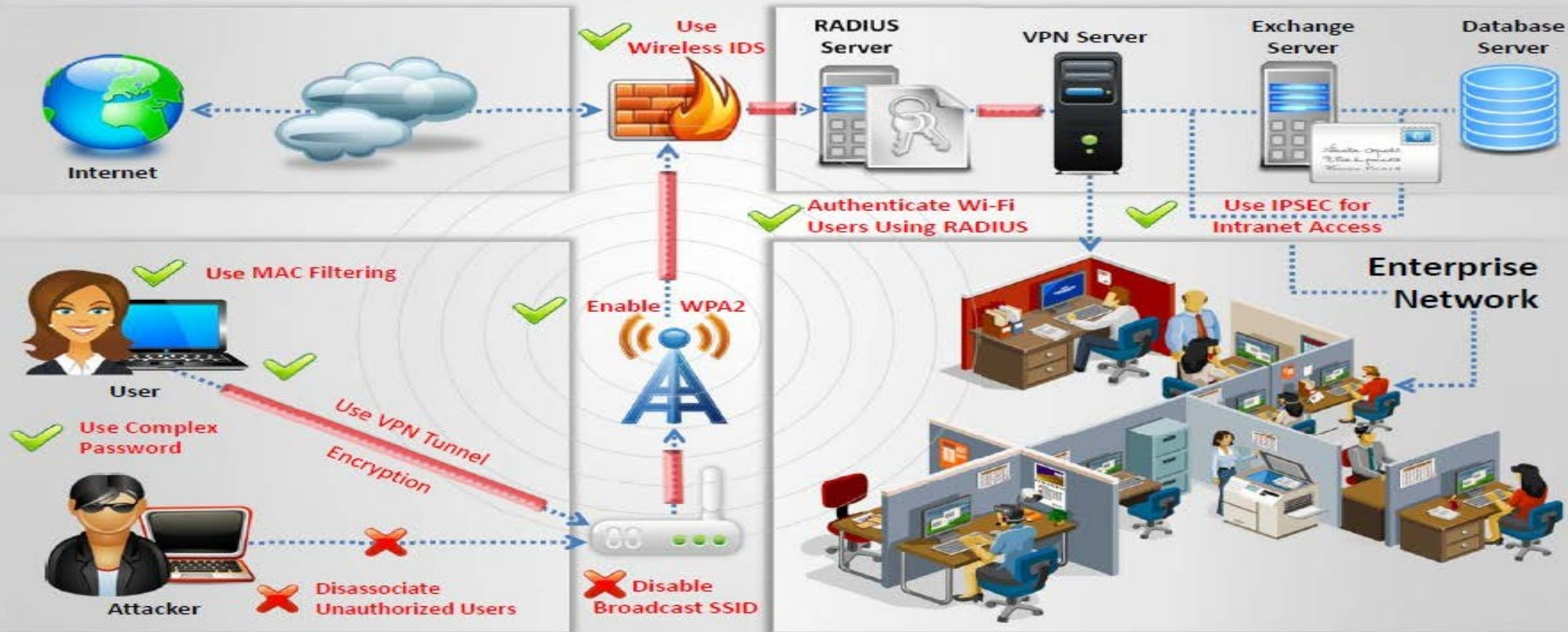SSID Settings Best Practices / Authentication Best Practices
- Place wireless access points in a secured location
- Keep drivers on all wireless equipment updated
- Use a centralized server for authentication

Module Flow
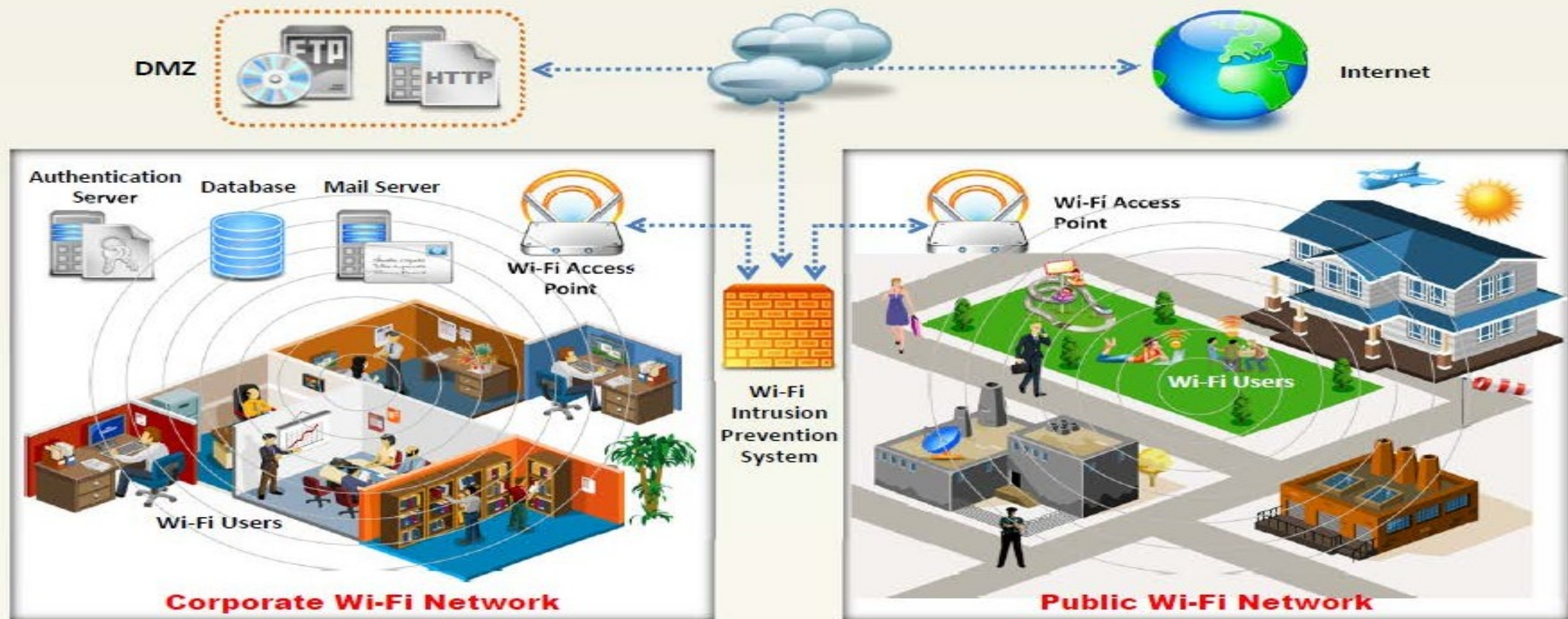
Wireless Intrusion Prevention Systems
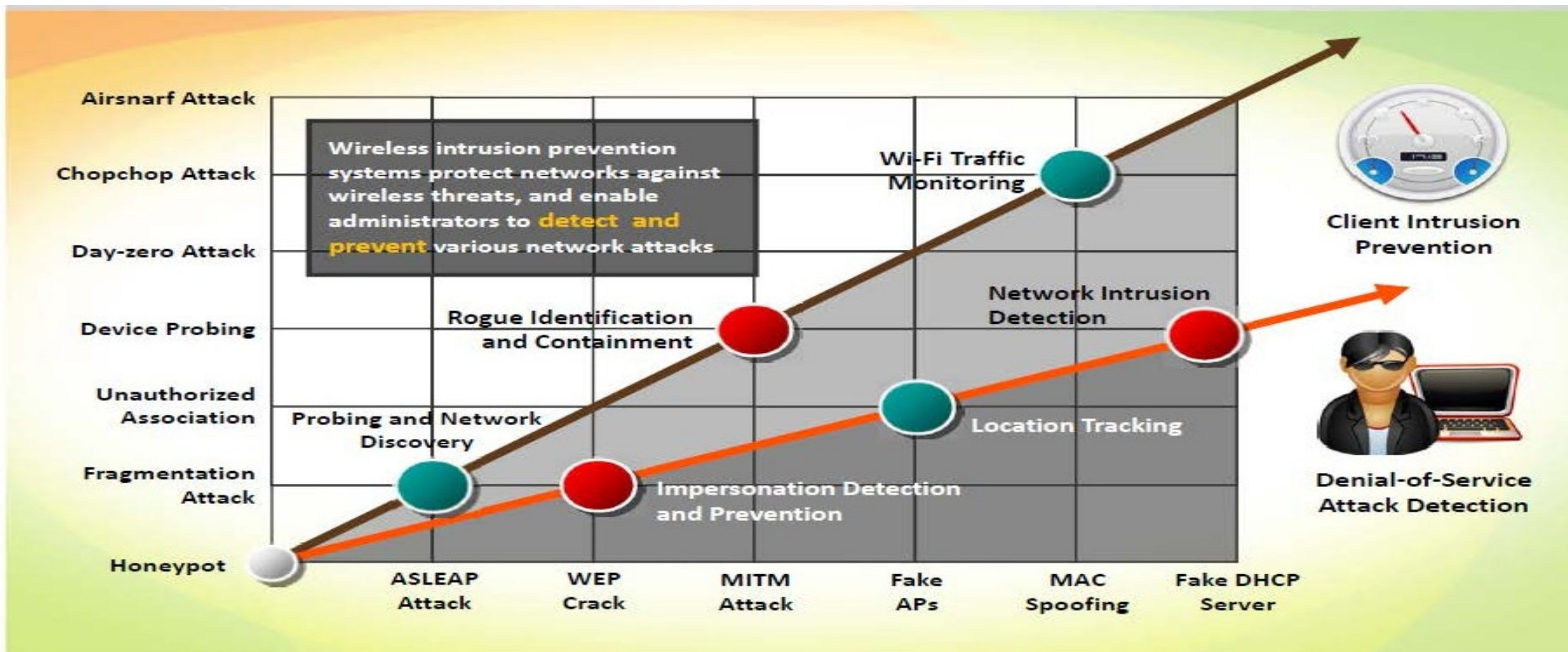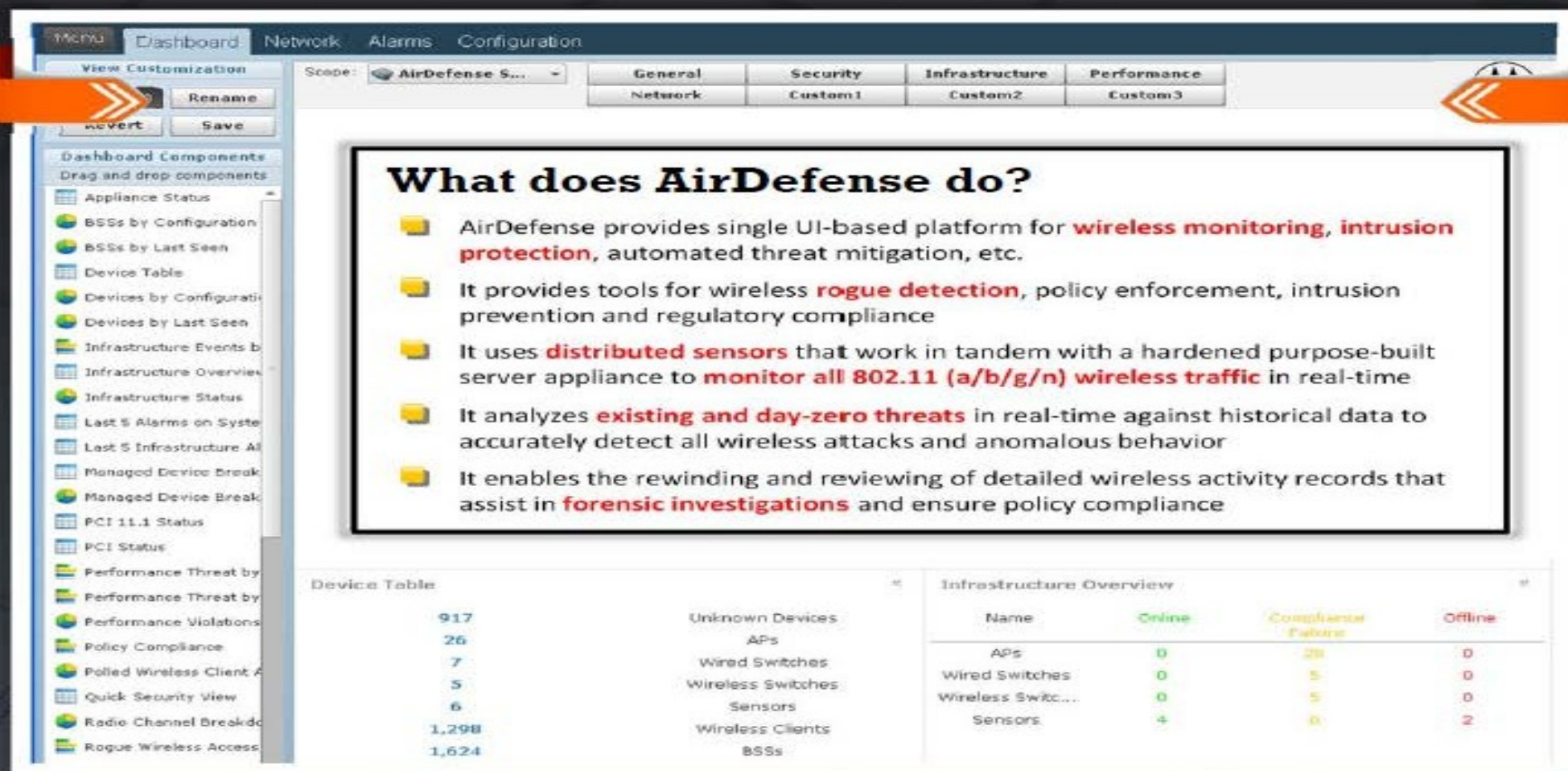
Wireless IPS Development

Wi-Fi Security Auditing Tool: AirMagnet Wi-Fi Analyzer

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

http://www.flukenetworks.com

Wi-Fi Security Auditing Tool: Motorola's Air Defense Services Platform (ADSP)

Wi-Fi Security Auditing Tool: Adaptive Wireless IPS

Wi-Fi Security Auditing Tool: Aruba RF Protect

Wi-Fi Intrusion Prevention System

Extreme Networks Intrusion Prevention System *http://www.extremenetworks.com*	**Network Box IDP** *http://www.network-box.com*
AirMagnet Enterprise *http://www.flukenetworks.com*	**AirMobile Server** *http://www.airmobile.se*
Dell SonicWALL Clean Wireless *http://www.sonicwall.com*	**Wireless Policy Manager (WPM)** *http://www.airpatrolcorp.com*
HP TippingPoint NX Platform NGIPS *http://www8.hp.com*	**ZENworks® Endpoint Security Management** *http://www.novell.com*
AirTight WIPS *http://www.airtightnetworks.com*	**FortiWiFi** *http://www.fortinet.com*

Wi-Fi Predictive Planning Tools

AirMagnet Planner	**Connect EZ Predictive RF CAD Design**
http://www.flukenetworks.com	*http://www.connect802.com*
Cisco Prime Infrastructure	**Ekahau Site Survey (ESS)**
http://www.cisco.com	*http://www.ekahau.com*
AirTight Planner	**ZonePlanner**
http://www.airtightnetworks.com	*http://www.ruckuswireless.com*
LANPlanner	**Wi-Fi Planning Tool**
http://www.motorolasolutions.com	*http://www.aerohive.com*
RingMaster	**TamoGraph Site Survey**
http://www.juniper.net	*http://www.tamos.com*

Wi-Fi Vulnerability Scanning Tools

Zenmap
http://nmap.org

Nessus
http://www.tenable.com

OSWA-Assistant
http://securitystartshere.org

Network Security Toolkit
http://networksecuritytoolkit.org

Nexpose Community Edition
http://www.rapid7.com

WiFish Finder
http://www.airtightnetworks.com

Penetrator Vulnerability Scanning Appliance
http://www.secpoint.com

SILICA
http://www.immunityinc.com

WebSploit
http://sourceforge.net

Airbase-ng
http://www.aircrack-ng.org

Bluetooth Security Tool: 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 takes place
- You can also **scan your device and detect apps** with bluetooth capabilities

http://www.fruitmobile.com

Wi-Fi Security Tools for Mobile: Wi-Fi Protector, Wi-Fi Guard and Wi-Fi Inspector
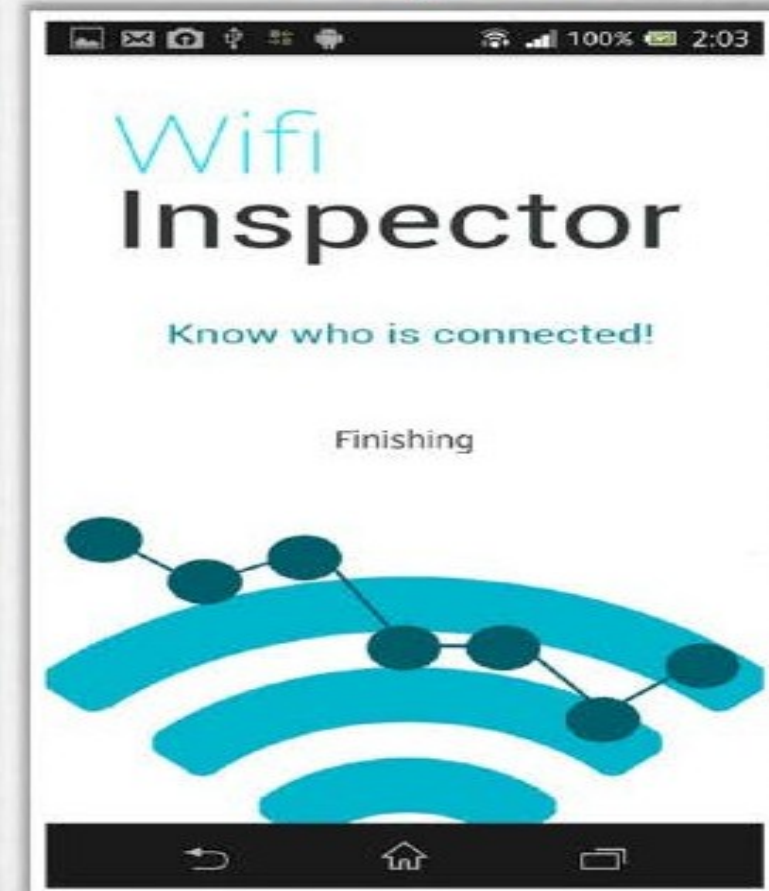
Module Flow

Wireless Penetration Testing

- The process of actively **evaluating information security measures** implemented in a wireless network to analyze design weaknesses, technical flaws and vulnerabilities
- A comprehensive report in **detail about the findings** along with the suite of **recommended countermeasures** is delivered to the executive, management, and technical audiences

Threat Assessment

Identify the wireless threats facing an organization's information assets

Security Control Auditing

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

Upgrading Infrastructure

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

Data Theft Detection

Find streams of sensitive data by sniffing the traffic

Risk Prevention and Response

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

Information System Management

Collect information on security protocols, network strength and connected devices

Wireless Penetration Testing Framework

Wireless Pen 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

Wi-Fi Pen Testing Framework

General penetration steps for all Wireless networks:

1. Create a rogue access point
2. Deauthenticate the client using the tools such as Karma, Hotspotter, Airsnarf, 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 LEAP Encrypted WLAN

START

LEAP Encrypted WLAN

Deauth Client?

Break LEAP

Steal Confidential Information

- Deauthenticate the client using tools such as **Karma**, **Hotspotter**, **Airsnarf**, etc.

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

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

Pen Testing WPA/WPA2 Encrypted WLAN

- Deauthenticate the client using tools such as **Karma**, **Hotspotter**, **Airsnarf**, 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 WEP Encrypted WLAN

Flowchart:

START → WEP Encrypted WLAN → Visible SSID?
- If No (✗): Deauth Client → Associate Client → Sniff the Traffic
- If Yes (✓): Sniff the Traffic

Sniff the Traffic → Captured/Injected Packets?
- If No (✗): back to Sniff the Traffic
- If Yes (✓): Break WEP → Use tools such as Aircrack-ng, Airsnort, WEPcrack, etc. → Launch Replay Attacks

Use tools such as Aireplay-ng, Commview, etc. → Deauth Client

Notes:

- Check if the SSID is visible or hidden

- If SSID is visible, sniff the traffic and then check the status of packet capturing

- If the packets are captured/injected, then break the WEP key using tools such as **Aircrack-ng**, **Airsnort**, **WEPcrack**, etc., or else sniff the traffic again

- If SSID is hidden, then deauthenticate the client using tools such as **Aireplay-ng**, **Commview**, etc., associate the client and then follow the procedure of visible SSID

Pen Testing Unencrypted WLAN

Module Summary

❑ IEEE 802.11 standards based Wi-Fi networks are widely used for communication and data transfer across a radio network

❑ A Wi-Fi infrastructure generally consists of hardware components such as wireless routers and APs, antennas, relay towers and authentication servers, and software components such as encryption algorithms, key management and distribution mechanisms

❑ Most widely used wireless encryption mechanisms include WEP, WPA and WPA2, of which, WPA2 is considered most secure

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

❑ WPA uses TKIP which utilizes the RC4 stream cipher encryption with 128-bit keys and 64-bit keys for authentication whereas WPA2 encrypts the network traffic using a 256 bit key with AES encryption

❑ WEP is vulnerable to various analytical attack that recovers the key due to its weak IVs whereas WPA is vulnerable to password brute forcing attacks

❑ Wi-Fi networks are vulnerable to various access control, integrity, confidentiality, availability and authentication attacks

❑ Wi-Fi attack countermeasures include configuration best practices, SSID settings best practices, authentication best practices and wireless IDS systems