**Wireless Hacking Tools**

Ahmed AlaaEl-Din Abd-ElWahab – Ahmed Magdy Mohamed Zaki – Ahmed Abd-ElLatif Mhana – Abd-ElGhani – Abd-Allah Ramadan

*University of Ainshames*

[ahmedalaahagag@gmail.com](mailto:ahmedalaahagag@gmail.com) / [ahmed\_hagag@cis.asu.edu.eg](mailto:ahmed_hagag@cis.asu.edu.eg)

**Abstract**

Wireless local-area networks – also called Wi-Fi networks or WLANs – are very popular. They are installed in offices, hotels, coffee shops, and homes. *Wireless networks* provide convenience, mobility, and are cheaper to realize than wired networks in many cases. The convenience, productivity gains, and cost savings of wireless networks are accompanied with a new set of vulnerabilities.

There are about 10 million Wi-Fi networks around the world, most are unsecured and open to unauthorized use because many individuals’ and businesses don't understand how to secure a wireless network and also because many Wi-Fi products come ready-to-use right out of the box.

**1. Introduction**

Having strong network security does not mean one can prevent the network from being attacked. It simply means that the security mechanisms implemented are just that secure and have not been broken yet. Computer and network security is constantly evolving. Strong security mechanisms must also evolve. As older mechanisms are broken or cracked, new ones must be developed.

Focusing on IEEE 802.11. [1] and Bluetooth connection [2]

**2. Types of attacks on wireless technology** [3]

* Confidentiality
* Integrity
* Availability
* Bluetooth

Confidentiality attack tools focus on the content of the data and are best known for encryption cracking.

Integrity attacks tools focus on the data in transmission and include frame insertion, man in the middle, and replay attacks

Availability attack tools focus on Denial of Service (DoS).

**3. Attacks Types Details**

* Confidentiality:

Is assuring that sensitive information will be kept secret and access limited to the appropriate persons.

Confidentiality can be achieved with: data encryption.

* Integrity:

Is that the message has not been tampered. No portion of the message has been removed, rearranged, or changed. The basic security measure to ensure

Integrity can be achieved with: generate a cryptographic checksum of some sort to guarantee the message is unaltered.

* Availability:

Is that data should be accessible and usable upon demand by an authorized user or process.

An availability attack consists of some sort ofDenial of Service (DoS) attack. A DoS attack prevents the user or device from accessing a particular service or application.

**4. Wireless Attack Tools**

Many of the wireless attack tools are developed to compromise 802.11 networks. The popularity and widespread Use of Wi-Fi gives the attacker a platform in which they can cause the most disruption. As other technologies gain

Popularity and usefulness, the more attack tools are developed for those technologies.

**5. Confidentiality Attacks**

**5.1.1. Definition**

The confidentiality attacks attempt to gather private information by intercepting it over the wireless link. This is true whether the data is encrypted or sent in the clear. If the data is encrypted, these attacks would include breaking the encryption and finding the key. Additionally, eavesdropping, key cracking, access point phishing (Evil Twin Attack), and man in the middle (MIMT) attacks are including in this category.

**5.1.2. Confidentiality Attacks Types**

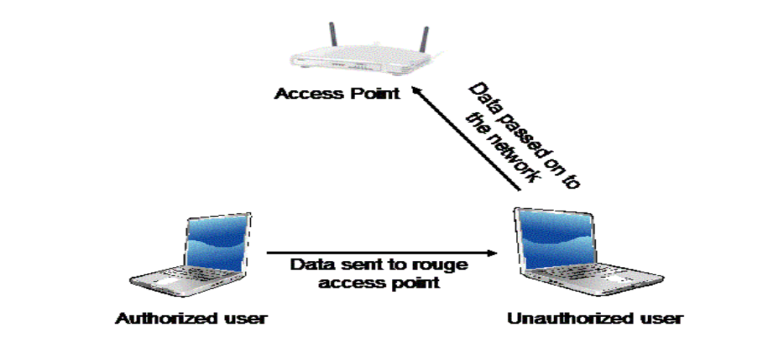
1- Eavesdropping [4]: is gathering information from a network by snooping on transmitted data. And to eavesdrop is to secretly overhear a private conversation over a confidential communication in a not legally authorized way. The information remains intact, but its privacy is compromised.

2- Key cracking: is having the wireless protection key.

3- Access point phishing (Evil Twin Attack): is the wireless version of the phishing scam. An attacker fools wireless users into connecting a laptop or mobile phone to a tainted hotspot by posing as a legitimate provider.

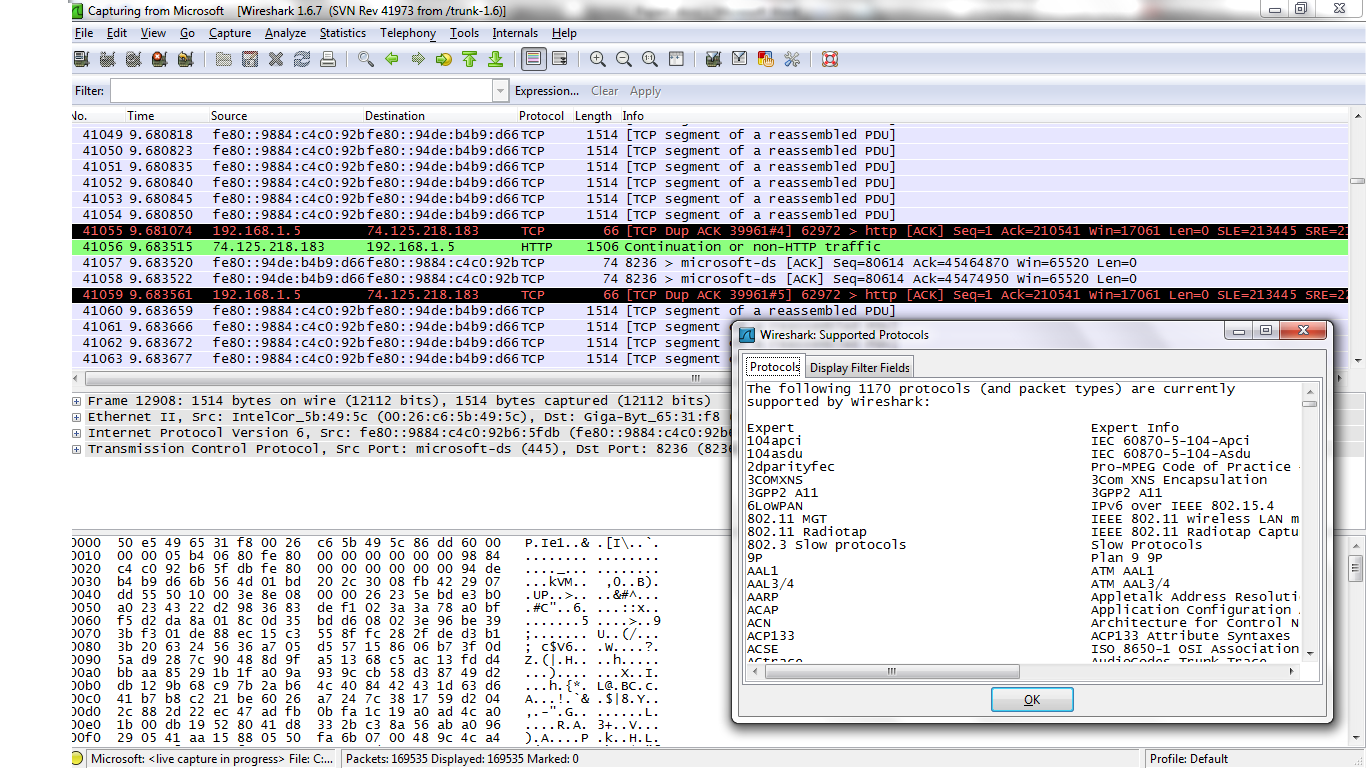
4- Man in the middle (MIMT): is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker.

Figure 1 - man in the middle attack

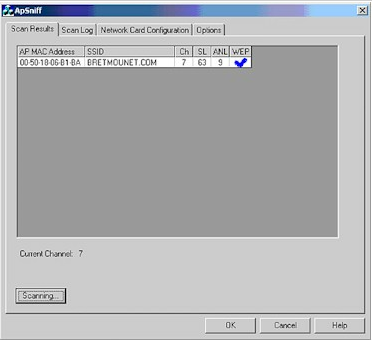


**5.1.3. Tools**

1. Wireshark: It is a basic sniffing program that will display all network traffic both wired and wireless. It is a multi-platform, multi-protocol analyzer [2] with hundreds of protocols supported. Display the captured data in an easy to read and easy to follow form. It also has many built in filters and the ability for the user to design their own filters. These filters can be used to only capture specific data such as a certain IP address, protocol, port number, etc.



1. Ettercap and dsniff: Are two Linux based programs popular man in the middle attack tools. They both provide sniffing capabilities similar to Wireshark, but go beyond that with the ability to modify the data in transmission.
2. Hottspotter [5]: passively monitors the network for probe request frames to identify the preferred networks of Windows XP clients, and will compare it to a supplied list of common hotspot network names.  If the probed network name matches a common hotspot name, Hotspotter will act as an access point to allow the client to authenticate and associate.
3. APsniff[6] : is a wireless (802.11) access point sniffer. It enables you to list all access points broadcasting beacon signals at your location. To help you set new access points making sure you do not have interfering APs. To help you set-up wireless clients by providing you with the client configuration information.

 Figure 3 - APsniff

1. APhunter [7]
2. KNSGEM[8]

All previous four programs will scan for wireless AP beacon signals. Although they are not necessarily attack tools, they can be used to find the wireless APs. KNSGEM will even place the APs on a Google Earth map. Attackers will then setup their evil twin AP near these legitimate ones.

1. HermesAP[9]
2. OpenAP[10]

Are two Linux based tools that allow the user to setup phony Aps.

1. OpenWRT[11]

10- HyperWRT[12]

Are two open source projects that replace the factory firmware for Linksys's popular WRT Line of APs. Attackers can use these distributions to create fake APs.

**5.2. Integrity Attacks**

**5.2.1. Definition**

The idea of an integrity attack is to alter the data while in transmission, the integrity of the data means that it has not been altered in any way. This includes data deletion or addition, frame deletion or addition, or replay attacks.

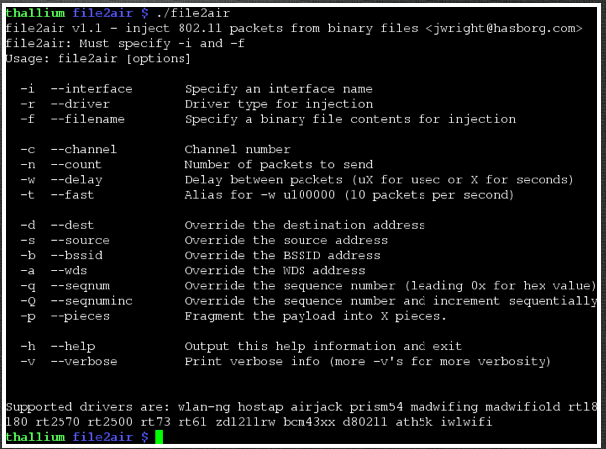
**5.2.2. Integrity Attacks Details**

Frame injection:   is an attack on Internet Explorer 5, Internet Explorer 6 and Internet Explorer 7 to load arbitrary code in the browser. This attack is caused by Internet Explorer not checking the destination of the resulting frame, therefore allowing arbitrary code such as JavaScript or VBScript. This also happens when code gets injected through frames due to scripts not validating their input. This other type of frame injection affects all browsers and scripts that do not validate untrusted input. When an attacker will inject their own Ethernet frames in the middle Of the transmission. This can be used in a variety of ways to attack the user. The user can be misled into accepting frames that it did not intend.

**5.2.3 Working Method**

When communicating with a web server there is a delay of tens of milliseconds while waiting for a reply. This is plenty of time for spoofed packets to be injected and the legitimate packets to be deleted.

**5.2.4 Frame injection Attacks Types**

1. User would access their banking web page and it would look like their legitimate web page, but the attacker has injected Ethernet frames so that even though the web page looks legitimate it is not. When the user attempts to login all the login information can be recorder by the attacker.
2. Generate a DoS attack Packet injection tools can be used to issue deauthenticate . [6] messages for the IP addresses in the network, that could easily be obtain from sniffing the traffic. This would cause the valid device to be disconnected from the AP.
3. Delete or jam the data being transmitted an attacker could jam the wireless signal from reaching its intended target and also provide acknowledgments (ACKs) back to the source. The data would never reach the intended target, but the sender would have no idea, since it would see the ACKs.
4. Data replay involves the attacker capturing authentication information and saving it for later use Once the attacker has captured and saved the authentication information, it will monitor the traffic for another authentication. Then it will inject those frames instead of the legitimate authentication frames and essentially gaining access to a system.
   * 1. **Tools**
5. Airpwn[13] : Airpwn is a framework for 802.11 (wireless) packet injections. Airpwn listens to incoming wireless packets, and if the data matches a pattern specified in the config files, custom content is injected "spoofed" from the wireless access point. From the perspective of the wireless client, airpwn becomes the server.
6. File2Air[14]: File-Based Wireless Packet Injection tools except it allows the user to specify a file that will be used for the payload of the injected packets. It uses another tool called AirJack to perform the actual frame injection. File2air runs on top of AirJack and reads in a binary file and transmits its contents onto a wireless network. Figure 4- File2Air
7. Simple replay [15]: an attack tool that allows for 802.11 packets that were previously captured to be injected back into the network.
   1. **Availability Attacks**

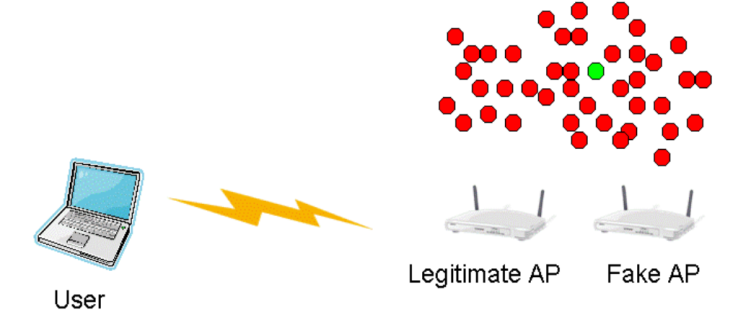
**5.3.1 Definition**

DoS focus on attacking a specific part of the network so that it is unreachable. Network availability means that any point the network is able to provide the requested information to the authorized user. DoS attacks prevent this information from reaching the user.

**5.3.2 Availability Attacks Details**

1. Flooding: is overloading the network with a certain type of packet so that the wireless AP is busy serving all the flooding packets that it cannot serve any legitimate packets.
2. Authentication Flood: where thousands of authentications are sent from random Media Access Control (MAC)addresses filling up the AP's authentication table and making it hard for a legitimate user to gain access.
3. Beacon flood: is where thousands of illegitimate beacons are generate to make it difficult for individual machine to find the legitimate AP.
4. Radio frequency jamming: jams the frequency of the Wireless Local Area Network (WLAN) most likely with a much higher power level allowed by the regulation. This will not allow anyone access to the WLAN.

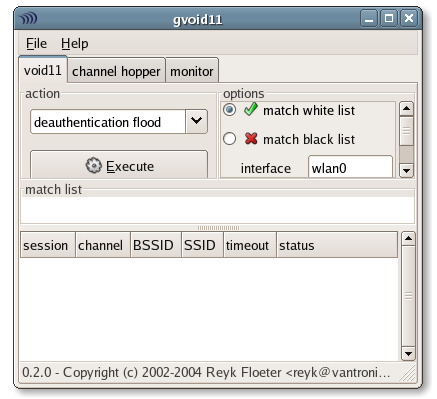
Figure 5- Beacon flood



**5.3.3 Tools**

1. FakeAP[16] : generates thousands of 802.11 APs or more specifically it generates thousands of 802.11 beacon signals that can be used for the beacon signal flooding attack.
2. Void11 [17]: flooding attack tool has the ability to implement three different flooding attacks: deauthenticate clients, deauthentication flood, and association flood. The deauthenticate attack floods the WLAN with deauthenticate packets for random MACs.

Figure 6- Void11



**5.4. Bluetooth Attacks**

**5.4.1 Definition**

Recently more Bluetooth attacks have emerged with Bluetooth technology gaining popularity. The two most well-known attacks are DoS, bluesnarfing, and a key bump attack. The key bump attack involves obtaining the pairing key and then having full access to the victim's system.

**5.4.2 Bluetooth Attacks Details**

1. DoS attack : involves a device that is not part of a piconet disrupting the established piconet of other devices, A Bluetooth piconet is the ad hoc network created with two or more Bluetooth devices that includes one master device and a number of slaves. The attacking device that is not participating in the piconet spoofs a slave out of the piconet and then contacts the master of the piconet. This will confuse the master device and lead to a disruption of the piconet.
2. Buffer overrun: This is when data is copied into a buffer, but the amount of data copied into the buffer exceeds the size of the buffer. This will cause the data to be copied into memory where it is not intended. The resulting status of the system depends on where in memory the data is copied.
3. Bluesnarfing: means obtaining unauthorized information through a Bluetooth connection. The Object Exchange (OBEX) [18] Push Profiler (OPP) has been identified as an easy mechanism for exchange of business cards, calendar entries, and other similar items.
4. Key bump: Gets the victim to accept a connection for some trivial data transfer, such as a picture, calendar notice, or a business card on a PDA. After the data is sent, the attacker keeps the connection open. This allows the attacker to request a key regeneration after the victim has deleted the pairing between the two devices. Once the key regeneration is done, the attacker has full access to any services provided by the victim's device.

**5.4.3. Tools**

1. BlueSmack[19] : Bluetooth attack that knocks out some Bluetooth-enabled devices immediately. This Denial of Service attack can be conducted using standard tools .
2. BlueSnarf : Obtain unauthorized access to files.
3. BluePass: Causes a buffer overflow attack.
4. BlueBump: Obtains the piconet key.

**6. Protection Tips**

1. Change the Administrative Password on your Wireless Routers.
2. Installing a Firewall.
3. Change the Default SSID Name and Turn off SSID Broadcasting.
4. Disable DHCP.
5. Replace WEP with WPA.

**7. References**

[1] IEEE 802.11 Standard <http://standards.ieee.org/findstds/standard/802.11v-2011.html>

[2] Wikipedia 802.11 Standards

<http://en.wikipedia.org/wiki/IEEE_802.11#802.11-1997_.28802.11_legacy.29>

[3] wirelessdefence

<http://wirelessdefence.org/>

[4] Eavesdropping attack over Wi-Fi by Fadi Farhat University of Windsor*.*

<http://www.google.com.eg/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CFQQFjAA&url=http%3A%2F%2Fweb2.uwindsor.ca%2Fcourses%2Fcs%2Faggarwal%2Fcs60564%2FAssignments2Project1%2FFadiFarhatAssignment2.doc&ei=ls2-T9OXMeyY0QXh-JzACg&usg=AFQjCNFS17riX_6K_0QT-vfEMIdhgK4Ebg&sig2=25a3eSaoDQ2NUQJyuao-7A>

[5] Hotspotter

<http://wirelessdefence.org/Contents/hotspotter.htm>

[6] ApSniff

<http://www.monolith81.de/mirrors/index.php?path=apsniff/>

[7] ApHunter

<http://www.hackerscenter.com/index.php?/Downloads/View-document-details/74-APHunter.html>

[8] Knsgem

<http://wirelessdefence.org/Contents/knsgem_main.htm>

[9] HermesAP

<http://linux.softpedia.com/get/System/Networking/HermesAP-13871.shtml>

[10] OpenAP

<http://savannah.nongnu.org/projects/openap/>

[11]OpenWRT

<https://openwrt.org/>

[12]HyperWRT

<http://sourceforge.net/projects/hyperwrt/>

[13]Airpwn

<http://airpwn.sourceforge.net/Airpwn.html>

[14]File2Air

<http://www.willhackforsushi.com/File2air.html>

[15]Simplereply

<http://www.security-freak.net/tools/amit/simple-replay-airbase/simple-replay.html>

[16]FakeAP

<http://www.blackalchemy.to/project/fakeap/>

[17]Void11

<http://www.wirelessdefence.org/Contents/Void11Main.htm>

[18]Object Exchange

<http://en.wikipedia.org/wiki/OBject_EXchange>

[19]BlueSmack

<http://trifinite.org/trifinite_stuff_bluesmack.html>

[20] A Visualization Tool for Wireless Network Attacks

[21] The OpenAP Project2

**8. List of Acronyms**

802.11: is a set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802)

Wireless devices link to the Internet via "hotspots" – nearby connection points that they lock on to. But these hotspots can act like an open door to thieves. Anyone with suitable equipment can locate a hotspot and take its place, substituting their own "evil twin".

Protocol analyzer: is a tool (hardware or software) used to capture and analyze signals and data traffic over a communication channel. Such a channel differs from a local computer bus to a satellite link, that provides a means of communication using a standard communication Protocol (networked or point-to-point). Each type of communication protocol has a different tool to collect and analyze signals and data.

Phony access points (APs) : that use spoofed service set identifiers (SSIDs) to lure wireless users

 WRT:firmware for several wireless routers, most notably the Linksys WRT54G

In 802.11, the AP and wireless device attempting to connect to it will trade associate and authenticate messages. When disconnecting, they will exchange deauthenticate messages.

MAC: is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used for numerous network technologies and most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the Media Access Control protocol sub-layer of the OSI reference model.

OBEX: is a communications protocol that facilitates the exchange of binary objects between devices. It is maintained by the Infrared Data Association but has also been adopted by the Bluetooth Special Interest Group and the SyncML wing of the Open Mobile Alliance (OMA)

Push Profile: is a specification regarding an aspect of Bluetooth-based wireless communication between devices. In order to use Bluetooth technology, a device must be compatible with the subset of Bluetooth profiles necessary to use the desired services.

Terms

ACK: Acknowledgment

AP: Access Point

DoS: Denial of Service

EAP: Extensible Authentication Protocol

ISAKMP: Internet Security Association and Key Management Protocol

MAC Medium Access Control

MSCHAP: Microsoft Challenge-Handshake Authentication Protocol

OBEX: Object Exchange

OPP :Push Profiler

RADIUS: Remote Authentication Dial-In User Service

RF: Radio Frequency

WEP: Wired Equivalent Privacy

WLAN: Wireless Local Area Network

WPA: Wi-Fi Protected Access