Wireless LAN Security Issues (I). Types of Attacks

Cătălina GHERGHINA[1], Gabriel PETRICĂ[2]
[1] Faculty of Electronics, Telecommunications and Information Technology, University POLITEHNICA of Bucharest
katalina.gherghina@gmail.com
[2] EUROQUALROM Laboratory, Faculty of Electronics, Telecommunications and Information Technology, University POLITEHNICA of Bucharest
gabi@euroqual.pub.ro

Abstract

Wireless communication is a very important part of our lives. Using mobile networks (GSM, UMTS or LTE standards), satellites connections, Wi-Fi local networks or terrestrial microwave, the telecommunication and data transfer between people or companies are assured. This paper presents an overview of wireless networks with their advantages and drawbacks and highlights some of the most common types of attacks whereby an intruder can intercept data.

Index terms: wireless, network, attack, security, WLAN

1. About Wi-Fi technology

We live in a dynamic world, permanently moving and changing, and the time is a critical variable that contribute to success and to maximizing the profitability. The exponential growth in the last five years made Internet network an essential element both in the business field and the personal, individual use. The need to be in a continuous contact with the company or business partners, mobility and portability are the criteria that made Wi-Fi an indispensable technology today. Wi-Fi networks allow connection any time, regardless of physical position (fixed or in motion) in coverage range, can serve several simultaneous connections and ensure good data transfer rates.

Wi-Fi is the trademark of technologies used for products that are based on the IEEE 802.11 set of standards which ensure interoperability between different wireless devices (wireless) - computer systems, laptops, tablets, PDAs (Personal Digital Assistant), smartphones, game consoles, multimedia equipment (TVs, digital audio players) and other peripheral devices.

A Wi-Fi connection requires both hardware support (network interface cards, access points, routers) and software - through the operating system and other programs used for data transfer and processing (dedicated drivers or applications).

The devices used for communication in a Wi-Fi network are:

- Network interfaces integrated in equipment (onboard), connected as PCI cards, PCMCIA cards or USB devices
- WAP (Wireless Access Point) is a device that allows wireless devices to connect to a communication network, usually wired. Depending on his destination, a WAP can be:
  - Private - usually used in small wireless networks, at office, SOHO (Small Office / Home Office) or even at home. The private WAPs are used to

connect laptops or other mobile equipment to the Internet. These devices may incorporate a router (for further distribution and sending the signal), a switch (for connecting multiple network segments) or a modem for connecting to the ISP (Internet Service Provider), offering multiple and complex functions.

- Public (Hotspot) - allow free or commercial (paid) use of Internet and are located in public places (parks, libraries, cafes, airports, hotels, universities). There are ongoing projects in universities for providing campus-wide Internet coverage or for the transformation of an entire city into a wireless access area (known as Municipal Wireless Network).

Some uses for wireless networks are:

- Fast data transfer and sharing of information;
- Access to Internet network in geographical areas with a poor infrastructure or lack of resources.

2. WLAN (Wireless Local Area Network)

A LAN (Local Area Network) is a type of computer network spread over an area up to about 100 meters where the linkage is done using copper wires (usually). In a "wireless LAN" the communication between nodes is implemented using radio waves (without the use of wires). The nodes may consist in computers or other equipment (printers, laptops, smartphones, tablets, etc.).

The world's first wireless computer network was developed in 1970 at the American University of Hawaii, under the leadership of Prof. Norman Abramson. It consisted of seven computers - arranged in a bi-directional star topology - and connected four islands; it was called ALOHAnet, and it was created with the usage of low-cost radios. In 1979, F. R. Gfeller and U. Bapst reported an experimental wireless local area network created using diffused infrared communications. One year later, P. Ferrert reported on an experimental application of a single code spread spectrum for wireless terminal communications.

2.1. Short history

The first generation of wireless data modems was developed in the early 1980's; the available data rates were below 9600 bits/second. The second generation appeared in 1985, and it provided data rates on the order of hundreds of kbits/second. The third generation of wireless modems aimed at compatibility with the existing LANs with data rates on the order of Mbits/second.

In 1996, the technology was relatively mature, with a lot of applications in everyday-life; wireless LANs were being used in hospitals, stock exchanges, building and university campuses or even large applications through internetworking. In July 21 1999, the wireless LAN became publicly available for home use with a decreased pricing.

At the end of the 1990s, wireless standards appeared, the first being the various versions of IEEE 802.11 (using the "Wi-Fi" brand name).

The first version 802.11a (October 1999) operates in 5 GHz band with a maximum raw data rate of 54 Mbit/s. 802.11b version (October 1999) and 802.11g (June 2003) operates in 2.4 GHz band and has a maximum raw data rate of 11 Mbit/s and 54 Mbit/s respectively. These versions suffer temporarily interferences from other products operating in the 2.4 GHz band like cordless telephones, microwave ovens or Bluetooth devices. 802.11n, a new wireless networking standard publicly released in 2009, uses multiple antennas to increase data rates up to 600 Mbit/s. An approximate range for 802.11 standard is 35-38 meters indoors and 120-140 meters outdoors (for a, b, g versions) and 70 / 250 meters (for n version).

2.2. WLAN advantages

An important reason why wireless networks are becoming more and more popular is the mobile devices (laptops, tablets, and smartphones) pre-equipped with necessary wireless technology, which dominate the global market. But there are other benefits of wireless networks.

They are very **convenient**; their nature allows users to access information from any place within their main networking environment, whether it is a home or an office. Wireless networks offer **increased mobility**, as the user is not constrained to this environment; he can access the information he desires outside his normal work environment, having a multitude of choices. **Free or low-cost hotspots** are available in many public places: libraries, restaurants, shopping centers, airports or train stations.

In many job types, the **productivity** is increased by using wireless networks; employees can maintain a permanent connection to the network as they are moving from place to place, fact that contributes to their output.

From the point of view of **efficiency**, it is much easier to create a deployment plan for a single wireless network, as the main thing one needs is one AP (Access Point) for many potential clients. The expandability of wireless networks is much easily attainable, as a highly increased number of clients can be supported without the inconvenience of installing additional wires.

Other benefits of wireless networks are:

- The cost itself; wireless equipment have an affordable price even for end-users;
- Ease of installation and configuration.

2.3. WLAN drawbacks

However, wireless networks present a lot of disadvantages, most of them generated by the technology limitations.

The range aspect (see chapter 2.1) is on the order of tens of meters (indoors), which is highly undesirable for networks with a large structure and has to be solved by using repeaters or additional access points (this leads to an increased price for that wireless network).

Reliability becomes an important issue because the information is transmitted by radio waves, a known fragile environment. A wide variety of interferences may affect data transmission; consequently, wireless networks are unreliable for important network resources (for example, a network server usually has wired connection).

Another issue which could decrease wireless networks usability is **data speed,** especially in specialized environments, where high-speed networks are used.

But the most important issue when evaluating the performance of a WLAN is the **security**. As these networks are subject to numerous types of attacks, a careful security preparation and maintenance is required.

3. Types of attacks in Wireless LANs

Usually, security can be seen as a sum of different measures taken for certain items - computers, peripherals, and data - to be protected from unauthorized access by other people or software applications.

In a normal flow, information is sent from Source to Destination as shown in next figure.

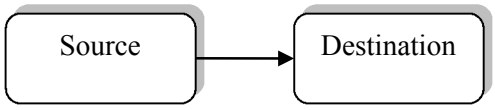

Fig. 1. Normal flow of information

The security of wireless networks is threatened by four major types of attack: interception, fabrication, modification, and interruption. Another type of attacks - repudiation - is an attack against the accountability of information.

Type of attack	On
Interception	Confidentiality Privacy
Fabrication	Authenticity

Type of attack	On
Modification Replay Reaction	Integrity
Interruption	Availability
Repudiation	Non-repudiation

3.1. Interception

Interception is a passive attack (without modification of information) where an intruder is able to read the information sent from the source to destination; it jeopardizes the confidentiality and the privacy of the users.

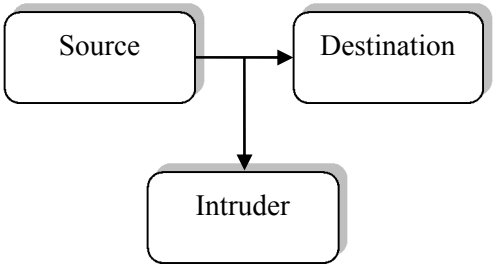

Fig. 2. Interception attack

The main characteristic of this attack is that the intruder intercepts the signal, but does not affect system resources. The purposes of an interception attack could be:

- Obtain sensitive information from message body (usernames, passwords, and credit card numbers);
- Identity interception of the source and subsequent initiation of a masquerade attack type;
- Traffic monitoring and obtaining information about the source profile (usual activities, most visited websites).

The most common examples of interception are sniffing and eavesdropping.

Sniffing

An *Ethernet sniffer* or *wireless sniffer* can be a hardware device or a computer program that can intercept and log traffic passing over a digital network or part of a network. The sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content. A sniffer (or packet analyzer) can be used by a network administrator (in network monitor purposes) or by an attacker (to intercept illegitimately the data flow). For a network administration, a usual utilization of packet sniffers includes:

- Monitor network usage (bandwidth utilization, internal or external users and systems, verify control system effectiveness for firewalls, proxy, users access control, Web and spam filter);
- Detect and analyze network problems (misuse, isolate exploited systems, traffic congestion, detect network intrusion attempts, filter suspect content);
- Generate different network statistics.

Some common packet sniffers are: tcpdump, Wireshark, ettercap, Microsoft Network Monitor.

Eavesdropping

In network security, *eavesdropping* ("the act of secretly listening to the private conversation of others without their consent", as defined by Black's Law Dictionary) is the passive acquisition of information from a network. Eavesdropping may occur in many methods of private communication (such as e-mail, instant messaging, VoIP or phone lines).

There are available on the market several tools which simplify the eavesdropping attack; NetStumbler, inSSIDer, Kismet or Airopeek (and many more) are programs that enable confidential information acquiring - such as SSID (Service Set Identification), the MAC address (Media Access Control) of the AP and information about whether WEP (Wired Equivalent Privacy) algorithm is enabled.

Another important characteristic of eavesdropping is that, once the attacker caught the weak authentication exchange, such as logging on a Web site using unsecured HTTP (Hypertext Transfer Protocol), it can duplicate later the logon process and gain

access to victim account.

The solution that safeguards the wireless LAN against interception must secure privacy and, also very important, it should solve the associated key distribution problem in order to properly secure the keys.

Security protocols at least as powerful as WPA2 (Wi-Fi Protected Access), ratified in 2004, represent a guaranteed protection against eavesdropping; however, WPA2 protects only the subnetwork, not the entire network. If the entire network protection is targeted, the use of end-to-end security methods (VPN, IPSec) is recommended.

3.2. Fabrication

An active attack on authentication is the *fabrication attack*: the intruder pretends to be the source entity and gather information meant for it.

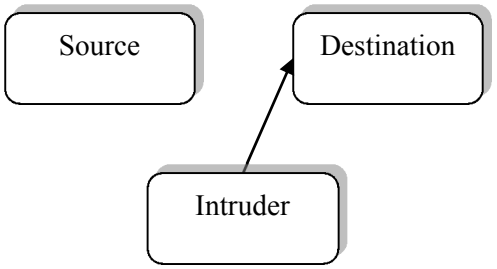

Fig. 3. Fabrication attack

Some examples of fabrication attack are: Man-in-the-Middle attack (the most used), spoofing, insertion attack, and brute-force password attack.

In cryptography and computer security, the *Man-in-the-Middle attack* is a form of active eavesdropping: the attacker makes independent connections with the victims (Sender and Recipient) and relays messages between them, making them believe that they are talking directly to each other over a private connection (both of two parts believe that the part in the middle is the other one) when in fact the entire conversation is controlled by the attacker.

Methods for defense against Man-in-the-Middle attacks include authentication techniques that are based on:

- Strong encryption: instead small key sizes (for symmetric or asymmetric algorithms) or broken ciphers (DES - Data Encryption Standard, 1977, 56 bit keys; WEP - 1999, with flaws in its design; all "classical" - transposition and substitution - ciphers) must be used PGP (Pretty Good Privacy) computer program or AES (Advanced Encryption Standard) algorithm;

- PKI (Public-Key Infrastructure), a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. PKI binds public keys with respective user identities by means of a Certificate Authority (CA) or a web of trust (an alternative to the centralized trust model of a PKI).

- Stronger mutual authentication through secret keys (more secure) or passwords (less secure);

- Other criteria, such as voice or biometrics recognition.

Spoofing is the act of pretending to be something (computer, user or person) you are not (assumption of other identities and fraudulent using IDs, passwords, access rights, etc.). There are multiple versions of spoofing: DNS (Domain Name Service) spoofing, IP (Internet Protocol) address spoofing. MAC address spoofing, etc. E-mail spoofing is the process of creation e-mail messages with a forged sender address (fake e-mails), typically used in spam and phishing e-mails to deceive the recipient about the origin of the message.

An *insertion attack* is the act of configuring a device to gain access to a network or inserting unauthorized devices into a network in order to gain access. For instance, a hacker can install an unauthorized AP (Access Point) in order to get users to connect to it (instead of the legitimate network).

In the *brute-force password attack*, also known as password cracking or dictionary attack, the attacker uses a dictionary (letters, numbers, words, special characters) in repeated attempts to find the password that gives access to the network. Even if a password authentication mechanism is implemented, brute-force attacks can occur.

3.3. Modification, Replay, Reaction

Modification

When an attacker changes the information sent from Source to Destination, this is a *modification attack*. This type of attack is an active attack on integrity of data.

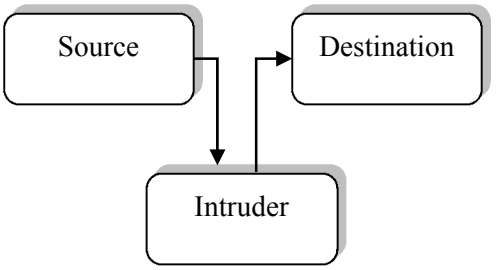

Fig. 4. Modification attack

Some examples of modification attacks are:

- Loss of equipment - data stored in a lost laptop (e.g. passwords) can be used by an attacker to masquerade him as an authorized user and login into a network;
- Insertion of a virus or Trojan program - the virus infection is a very common type of attack, affecting both wired and wireless networks. The malware program can infect a station inside the network and can spread through it all.

Replay

In a *replay attack*, an intruder resends information sent from the Source to the Destination entity.

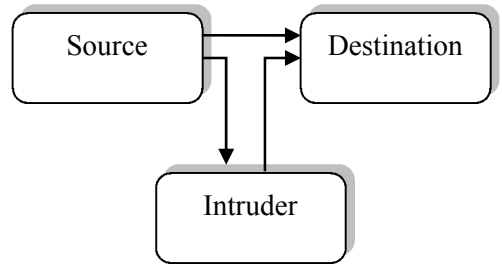

Fig. 5. Replay attack

Replay attack is an active attack on integrity of data, and the most common type of replay attack is traffic redirection: this is done by routing the packets on the network towards the attacking station. The attacker can capture these packets before forwarding them to the attacked systems or can attempt a man-in-the-middle attack.

Reaction

In a *reaction attack*, packets are sent by an intruder to the destination; the intruder monitors the reaction for information or benefits he can get.

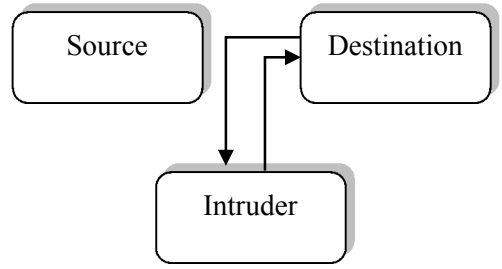

Fig. 6. Reaction attack

3.4. Interruption

Interruption is the attack type in which an intruder blocks data flow sent from the source entity to the destination. Interruption is an active attack on system availability.

Some common examples of interruption attacks are DoS (Denial of Service) attacks. DoS or DDos (Distributed DoS) do not seek attacks on computers or access to information, but are focused on blocking services by overloading a resource with useless traffic to cause a failure.

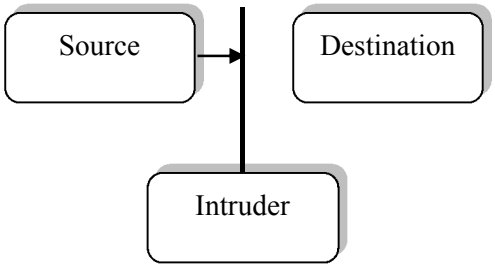

Fig. 7. Interruption attack

Basic types of DoS attacks are:

- Consumption of computational resources - disk space, bandwidth, internal memory, buffers, or processor time;

- Disruption of configuration information, such as routing information (selecting best paths in a network);

- Disruption of state information, such as unsolicited resetting of TCP sessions (a method of tampering with Internet communications where a third computer send a "forged" packet containing a TCP reset to one or both endpoints).

- Disruption of physical network components.

- Obstructing the communication media so the devices (computers, AP) can no longer communicate adequately. The attacker may use some physical mechanism (such as RF interference) to successfully interrupt a wireless network. Because the RF spectrum is shared by other devices (microwave ovens, cordless phones, and baby monitors), an attacker with the proper equipment can flood the airwaves with noise and disrupt service to the network.

- Another related type of attack consists of the degradation of a service; thus, it is not completely stopped, but the quality of service (Q0S) is reduced.

Some common types of DoS are: Teardrop attack (sending invalid IP fragments with over-sized payloads to the target machine), Peer-to-Peer attack (exploits DC++ client used for peer-to-peer file sharing), Nuke (an old DoS attack consisting of repeatedly send invalid ICMP packets to the target) or Floods (to exhaust network bandwidth).

An intruder can use different types of floods:

- ARP Spoofing/Flooding/Poisoning on ARP (Address Resolution Protocol);

- Synk4/Syn Flooding - at connections between two computers over the Internet using a TCP connection;

- SMTP queue flooding - many messages to an open mail relay server or a very large number of spam messages can fill the SMTP (Simple Mail Transfer Protocol) queue;

- Smurf attacks - many ICMP (Internet Control Message Protocol) packets with the victim's spoofed source IP address are broadcast to a network using an IP Broadcast address. Most computers will respond by sending a reply to the source IP address, which will be flooded with traffic.

- Ping broadcasts - the attacker flood the victim with ICMP Echo Request packets.

3.5. Repudiation

In information security, non-repudiation is a service that provides proof of the integrity and origin of data so as to the source entity cannot denies sending a message or the destination entity cannot denies receiving a message.

Repudiation is an active attack on non-repudiation and occurs when a system or application don't track users' actions, thus permitting malicious manipulation or forging the identification of actions. A malicious user can change the authoring information of his actions in order to write wrong data to log files, so the data stored on log files is corrupted.

4. Conclusions

This paper presented an overview of WLAN networks and highlighted the main types of attacks in a computer network (wired or wireless). The main advantages of a WLAN are:

- Easy access to electronic resources (in a local network or on the Internet) without relying on cables;
- Maximum mobility (there are many public wireless networks, but the connection is possible only in a limited area, served by a hotspot);
- Efficiency (a hotspot can serve simultaneously a large number of clients, so it's a low price relative to the number of potential users).

There are some disadvantages of deployment and use of wireless networks, and among them we can mention:

- Some physical limitations (electromagnetic emitted power, frequency spectrum) have made the range of a WLAN to a few tens of meters to 100 meters, and the data transfer rate is lower than wired Ethernet networks;
- Spectrum assignment is not consistent worldwide: channels 1-11 for the 2.4 GHz band in USA, channels 1-13 for Europe and Australia, and 1-14 in Japan;
- Interferences with other devices working in the proximity;
- Operating safety in terms of health (radiation exposure).

One of the major problems encountered in wireless networks is the security of transmitted data. Because unauthorized access in radio networks is much easier to achieve than in wired connections, multiple methods must be adopted to ensure the security of data: a strong encryption algorithm, MAC address filtering, SSID hiding, etc.

References

[1]. P. Roshan and J. Leary, *802.11 Wireless LAN Fundamentals*. Cisco Press, 2010.
[2]. F. Ohrtman, *Voice Over 802.11*. Artech House, 2004.
[3]. F. Baiardi *et al.*, "SEAS, a Secure E-voting Protocol: Design and Implementation," *Comput. Security*, vol. 24, no. 8, pp. 642-652, 2005.
[4]. E. A. Jorswieck *et al*., "Secrecy on the Physical Layer in Wireless Networks," *Trends Telecommun. Technol*., pp. 413-435, 2010.
[5]. B. D. Lewis and P. T. Davis, *Wireless Networks for Dummies*, 2004.
[6]. I.-C. Mihai, *Information Security*. Craiova, Romania: Sitech, 2012.
[7]. R. K. Nichols and P. C. Lekkas, "Wireless Security: Models, Threats, and Solutions," McGraw-Hill Professional, 2001.
[8]. WLAN (2013, Jul. 05) [Online]. Available: http://en.wikipedia.org/wiki/WLAN