Security Of Wi-Fi Networks

Durmuş Ali Avcı, Kemal Hajdarević
International Burch University, Faculty of Engineering and Information Technologies, 71000, Sarajevo, Bosnia and Herzegovina
E-mails: avcidurmusali@gmail.com, khajdarevic@ibu.edu.ba

Abstract: With the rapid increase in use of WLAN technology it is important to provide a secure communication over wireless network. This paper focuses on current security issues in Wi-Fi networks, and gives overview of already available set of security controls which can help organizations to secure their wireless LANs. The goal of this paper is to summarize existing means of securing Wi-Fi networks and to analyze the possible solutions for the Wi-Fi networks. Furthermore, the paper explains how the security mechanisms work and provide security in order to have best communication.

Keywords: wlan, wi-fi, wireless, security, network, wi-fi security, wps

1. INTRODUCTION

Personal computers appeared in the 1970s and they were meant to be placed on a desk. Then Laptop computers were invented in the 1980s and then handheld computers were invented in the 1990s. People began to use the portable devices in airplanes, automobiles, or anywhere outside. People wanted to access to the Internet wherever they were. Radio link is proposed as alternative way for connection to Internet. During World War II, the United States Army first used radio signals for data transmission (Tammie, 2005). In 1971, researchers at the University of Hawaii developed the world’s first WLAN, or wireless local area network which was named ALOHANET which consisted of 7 computers that communicated in a bi-directional star topology (Maury, 2002). Wi-Fi was invented in 1991 by Vic Hayes in Nieuwegein, the Netherlands. At the beginning the name was WaveLAN which has speeds of 1Mbps/2Mbps and it was used for cashier systems (Schilling, 2007). Initially Wi-Fi was thought to have potential in replacing the current cell
phones or devices equipped to use Wi-Fi technologies will work worldwide and allow for easy access to the internet. Current cell phone technologies like GSM or CDMA are spread randomly throughout the world and access is not always available with the equipment.

2. WHAT IS Wi-Fi?

Technology which allows devices to communicate without cords or cables is popularly called Wi-Fi (Wireless fidelity) and network which provides local connection is called wireless local area network (WLAN). It describes all network components that are based on one of the 802.11 standards. Mobile data devices (such as laptops, PDAs or phones) are used to connect to Wi-Fi access points (devices connected with wired network) in short proximity. Wi-Fi provides Internet connection to mobile user by using wired connection with Internet. Wi-Fi is generally much faster than data technologies operating over the cellular network like GPRS, EDGE, HSDPA, and EV-DO. Thanks to the Wi-Fi technology, wireless technology has transformed to an open solution for providing mobility and network services without the requirement of wired connection.

The Wi-Fi is currently the most widespread wireless networking mechanism for personal computers and organizations. Many users have installed Wi-Fi networks at home, and numerous corporations have added Wi-Fi access points to their wired networks. While wireless LAN provides greater mobility and flexibility, it also poses security risks to the organizations. Security in wireless networks is harder to provide than the wired networks because of their inherent broadcast nature. This is due to the fact that every packet transmitted in a wireless network can be intercepted by all nodes within the communication range of the transmitter. This underlying vulnerability not only makes security in wireless networks extremely important but also adds additional requirements like privacy, anonymity and resource optimization. These networks have given hackers new opportunities to gain unauthorized access to corporate computer systems and their data.
3. SECURITY PROBLEMS AND REQUIREMENTS OF Wi-Fi

In the wireless systems, having a secure network has become quite important due to the large number of people dependent on these systems in daily life. One of the most drawbacks of wireless networks is that they are not as secured as wired networks and the data sent through wireless networks can easily be intruded and modified. In wireless networks the security is much more critical and compulsory than the wired networks; because the data is sent over the wireless network is actually broadcast for the neighborhood to hear. When sending a critical data over the airwaves, the wireless networks should not be used unless some countermeasures taken. All the wireless systems must have a specific level of security in order to have privacy when sending data over the network. For example when financial institutions, banks, military networks etc. send their sensitive data through a wireless networks, then some extra measures have to be taken to have privacy and confidentiality, otherwise the important data could end up in wrong hands and you can imagine how useful things become dangerous. Each security solution has to provide the security requirement above to make a secure WLAN. The network administrator must use the specific security mechanism in the WLAN in order to make the network consistent and scalable. Nowadays the wireless internet is growing very fast, so there is a great need to make communication secure; without it, this perfect and fast speed of data flow becomes useless for everybody.

Security is an important issue for wireless networks, especially for those security sensitive applications and data exchanges. Many users of data transmission devices (such as laptops, PCs, phones, etc.) demand for protecting data being transferred between devices, and ensuring proper transfer. One of the goals of current wireless standard was to provide security and privacy that was ‘Wiredequivalent’ and to meet this goal, several security mechanisms were provided for confidentiality, authentication, and access control. Unfortunately all of these can be easily broken (Kush & Kumar, 2005). The main points that are considered as security parameters are:

- **Authentication**: It ensures that communication from one node to other is genuine. Only legitimate users can access the system and services.
- **Access control**: Access control is the constraint that limits those who can utilize system resources. Two approaches are used, one is called ‘access control list (ACL)’ and other as ‘closed network’.
Availability: Availability ensures the service offered by node will be available to its users when expected, in spite of attacks. Also, only legitimate users can access data anytime.

Confidentiality: It ensures that certain information is never disclosed to unauthorized entities. Personal or sensitive data is protected.

Integrity: It protects nodes from maliciously altered messages. It assures the data, system, or platform has not been tampered with.

Identity: An essential element in any security system is reliable, robust non-malleable identity.

Non repudiation: It ensures that the origin of the message cannot deny having sent the message.

Wi-Fi depends on the cryptographic methods to be well secured. In this paper, the WEP and WPA security mechanisms will be shown to provide the security. Privacy is one of the most important needs in network to secure the data from being watched by third party. The transmitted data in the network should not be readable by anyone but those communicating.

4. ATTACKS ON WIRELESS NETWORKS

There are many security threats and attacks that can damage the security of WLANs. Those attacks and threats can be basically classified into two main categories:

Logical Attacks
Physical Attacks

Logical Attacks

Logical attacks always related with the software, system, and the sensitive data flowing through the network. In these types of attacks the main goal of the intruder is to find the code and software that will help the intruder to access the network the sensitive data. Some most common logical attacks are defined below.

• Brute Force Attacks against Access Point Passwords
• Spoofing of MAC address
Security Of Wi-Fi Networks

- Denial of Service Attack
- Man in the Middle Attack
- Eavesdropping
- Dynamic Host Configuration Protocol Attack
- Reconnaissance Attacks

**Brute Force Attacks against Access Point Password**

A brute force attack is a trial-and-error method which is used to obtain information such as a user password or personal identification number. In a brute force attack, intruder uses automated software to generate a large number of guesses as to the value of the desired data.

**Spoofing of MAC address**

MAC spoofing is a technique for changing a Media Access Control (MAC) address of a network interface on a networked device. Normally the MAC address cannot be changed. However, there are some tools which can make an operating system believe that the MAC address the user’s address. The process of masking a MAC address is known as MAC spoofing. MAC spoofing is changing a computer’s identity, for good or for bad reasons, and it is relatively easy process.

**Denial of Service Attack (DoS)**

A DoS attack is an attempt to make one or more computer systems unavailable. They are considered to as the most common type of security attacks. The target of the attack is to make the network inaccessible for the client. DoS attacks can be implemented by using Flood attack, SYN attack and Ping of death attack.

**Man in the Middle Attack**

A man in the middle attack is an unauthorized blocking of network traffic to get the secret information and modify the data packets on the network. A man-in-the-middle attack can be used to block an encrypted message exchange and make the recipient think the message is coming from his partner. The main target of this type of attack is to read and alter the data whenever intruder wants during the
communication session without knowing the hosts which is also known as session hijacking attack.

Eavesdropping

Eavesdropping is an attack in which the attacker passively monitors network communications for data, including authentication credentials. In the wireless network, eavesdropping by is the most indicative threat because the attacker can intercept the transmission over the air from a distance.

Dynamic Host Configuration Protocol Attack (DHCP)

The Dynamic Host Configuration Protocol (DHCP) is a protocol which is used in the TCP/IP networking model to configure hosts attached to a network automatically. Specific attacks can use broadcasted DHCP requests with spoofed MAC addresses. Some of DHCP attacks can be sued as a denial of service (DoS) attacks.

Reconnaissance Attacks

Attacks which are used to collect information about a targeted network and are called reconnaissance and they can information for DoS attacks. The reconnaissance attack consists on the following four processes which are sing sweep, sort scan, packet sniffer, and Internet Information Queries (IIQ).

Physical Attacks

Physical attacks are always related with the hardware and the design of the network. In this type of attack the target of the intruder is to block the network performance rather than searching for a sensitive data and then make some changes with the data. Some of the most popular physical attacks are:

- Rogue Access Points
- Physical placement of Access Points
- Jamming attacks
- Spam Attack
Rogue Access Points

Rogue access points are WLAN APs which are not authorized to connect to a target network which is opening a wireless hole into the network. An attacker can plant a rogue AP, or an employee may accidentally create a security hole by plugging a non-secure access point into the network. In order to get rid of this type of attack, simple technique known as lock down mechanism is used. By installing this application the administrator will get the logs whenever attacker tries to add some application.

Physical placement of Access Points

Physical placement of APs is another security issue because placing APs in an unsecure place will expose it to physical attacks. The AP can be shut down easily by attackers and whole configuration will be lost and AP will come into default configuration. Because of that special care has to be taken in consideration when choosing physical location of the access points.

Jamming attacks

Jamming attack is achieved by transmitting a signal to the receiving antenna at the same frequency band as the original signal. An attacker with the can easily jam the 2.4 GHz frequency in a way that drops the signal to a level where the wireless network can no longer function.

Spam Attack

The purpose of spam is to flood messages over the whole network like traditional emails. The spam attack absorbs bandwidth, which is not scalable for the WLAN network.
5. SECURITY OF Wi-Fi

WEP

WEP is a well-known security protocol which is specified in the IEEE Wi-Fi standard, 802.11b. It is designed to provide a wireless networks with a level of security and privacy as a wired LAN. The aim of the WEP is to give protection to that offered by the wired network’s physical security measures by encrypting data transmitted over the WLAN. WEP has well known security weaknesses and almost 13 years passed since its ratification, it is still widely used as a common option to secure communication on network.

To transfer data through the network WEP uses some encryption and decryption techniques. Encryption is achieved as:

- The secret PSK that is 40 bit long is hashed with Initialization Vector that is 24 bit.
- A PRNG is generated from the result of mixed IV and pre shared key to form a new sequential key.
- The plaintext and the ICV are hashed in the mixer, when a copy of plain text is transferred to integrity Algorithm the ICV is created.
- The sequential key and the result of hashed plaintext and ICV is transferred to RC4 algorithm, where RC4 algorithm performs the XOR operation to give the encrypted result.

In the end encrypted message can be obtained by first adding the IV in front of Cipher text.
Hence the encrypted message is ready to send across the air (Lashkari, Mansoor, & Danish, 2009).

Decryption: There are five steps helps to define how WEP works in order to decrypt the information.

- The pre shared key that is 40 bit long is hashed with IV that is 24 bit long and available in the encrypted information to generate a PRNG to form a sequential key.
- The cipher text that available in encrypted message and the Sequential key that is already generated are transferred into RC4 algorithm, which performs the XOR operation on both of them to form a plain text.
- The ICV is separated from the Plain text.
Plain text is transferred to integrity algorithm to form a new ICV. The new ICV is compared with the original ICV, if the both ICV matched then the data becomes safe otherwise it is altered.

Hence the message is successfully decrypted and the original message is available at the recipient side (Lashkari, Mansoor, & Danish, 2009).

WEP is considered to be very vulnerable to attackers that any attacker close enough to the building can attack the building’s WLAN security. The following known attacks are known to be effective on WEP:

Passive Attacks
- Dictionary based attacks
- Cracking the WEP key

Active attacks
- Authentication Spoofing
- Message Injection
- Message Modification
- Message Decryption
- Man in the Middle Attack

WPA

WPA is a security technology for wireless networks which is stronger on the authentication and encryption than WEP. WPA provides two standard technologies: Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) to achieve better security. It also has built-in authentication support which WEP did not offer.

WPA utilizes its TKIP to improve data encryption which provides important data encryption enhancements including a per-packet key mixing function, a message integrity check (MIC), an extended initialization vector (IV) with sequencing rules, and a re-keying mechanism.

WPA also implements 802.1x and Extensible Authentication Protocol (EAP) provides better user authentication. These implementations provide a framework for strong user authentication.
Wi-Fi Protected Access 2 (WPA2)

WPA2 was introduced in September 2004 which is the second generation of WPA security. WPA2 uses PSK authentication but instead of TKIP encryption it uses enhanced data encryption which is a specific mode of the Advanced Encryption Standard (AES) known as the Counter Mode Cipher Block Chaining-Message Authentication Code (CBC-MAC) protocol (CCMP). WPA2 offers two modes of operation:

- WPA2-PSK (Pre-Shared Key) mode
- WPA2 Enterprise mode

In WPA2-PSK mode the 256-bit key is generated from plain-text passphrase called pre-shared key (PSK). Like WPA, the same input is used to generate the pairwisemaster key (PMK), which is used to initiate the handshake: passphrase, SSID andSSID length.

On the other hand, when WPA2 Enterprise mode is used, much more complex authentication schemes can be supported since authentication is performed with the aid of an Authentication,Authorization and Accounting (AAA) backend server. (Georgopoulos, McCarthy, & Edwards, 2011).

Wi-Fi Protected Setup (WPS)

WPS was introduced and developed by the Wi-Fi Alliance to simplify ways of setting up and configuring security on wireless networks. Users manually create a wireless network name, and then manually enter security key on both the access point and the client to secure their wireless network. However, this process requires the users to have the some knowledge on the Wi-Fi devices to make the configuration. WPS was introduced to remove the guess work of securing a wireless network by typing a short PIN (numeric code) or pushing a button. WPS automatically configures wireless networks with a network name (SSID) and strong WPA data encryption and authentication. WPS is a new standard which offers some alternative ways for clients to authenticate the wireless network which is meant to make wireless encryption easy to setup. WPS defines four new ways of authentication:
• The PIN method
• The Push Button Configuration (PBC) method
• The Near Field Communication (NFC) method
• The USB method

6. CONCLUSION

In this paper, an overview of security scheme in wireless networks is presented. Wireless technology has been changing rapidly and as the time goes and networking technology improves, there is a long way to go for wireless networks to achieve security. The main goal was to show a preview of mechanisms used for securing wireless networks. In general some basic terms about WLANs were discussed with possible attacks on WLANs.

REFERENCES

4. Davies, J., n.d. Wi-Fi protected access 2 data encryption and integrity. [Online]
10. Available at:


