Proceedings of
National Conference on Innovative Trends in Computer Science Engineering (ITCSE-2015)
held at BRCMCET , Bahal on 4th April 2015

Analysis of Security Issues and Their Solutions in Wireless LAN

[1]Shenam Chugh, [2]Dr.Kamal
[1,2] Department of CSE
[1,2,3]BRCM Bahal, Bhiwani
[1]shenam91@gmail.com, [2] dkamal@brcm.edu.in

A*bstract*— **This paper begins by introducing the concept of wireless LAN (WLAN). The introductory section gives brief information on the WLAN components and its architecture. In order to examine the WLAN security threats, this paper will look at both active & passive attacks. The paper will then explain the security & flaws of legacy IEEE802.11 WLAN standards. This situation leads to further research regarding practical solutions in implementing a more secured WLAN. This paper will also cover the new standards to improve the security of WLAN such as the IEEE 802.1x standard, which comprises of three separated sections: Point-to-Point Protocol (PPP), Extensible Authentication Protocol (EAP) and 802.1x itself. Then the paper look for a newly proposed standard i.e. 802.11i for key distribution and encryption that will play a big role in improving the overall security capabilities of current and future WLAN networks. Finally, this paper ends with the conclusion of highlighted issues and solutions.**

***Index Terms*— Legacy WLAN Standards, Security Issues, Security Measures, Wireless LAN**

I.INTRODUCTION TO WLAN

WIRELESS local area network (WLAN) is a group of wireless networking nodes within a limited geographic area, such as an office building or building campus, that are capable of radio communication. WLANs are usually implemented as extensions to existing wired local area networks (LAN) to provide enhanced user mobility and network access. In 1997, the IEEE802.11 was implemented as the first WLAN standard. It is based on radio technology operating in the 2.4 GHz frequency and has a maximum throughput of 1 to 2 Mbps. In the recent years, several technologies derived from the 802.11 and these are 802.11a, 802.11b, 802.11g & 802.11n. The currently most spread and deployed standard, IEEE 802.11b, was introduced in late 1999. It still operates in the same frequency range, but with a maximum speed of 11 Mbps.

The network using the IEEE 802.11 family of standards for creating WLAN with internet facility is generally called *Wi-Fi Network*, and the devices used in that network are called Wi-Fi Devices. Wi-Fi is a trademark of the Wi-Fi Alliance and the brand name for products using the IEEE 802.11 family of standards.

This paper is outlined as follows. *Section I* provides the introduction to WLAN and also covers the basic components and architecture of WLAN. *Section II* describes various security threats of WLAN. This section covers both the active and the passive attacks. *Section III* describes the security features provided in legacy IEEE802.11 WLAN Standards and their limitations. This section covers Wireless Equivalent Privacy (WEP) which was originally implemented in legacy IEEE 802.11 WLAN and also covers Wi-Fi Protected Access (WPA) which is proved as a replacement to WEP. *Section IV* provides some of the practical solutions for securing WLAN. This section addresses some important guidelines for the users (WLAN administrators) to secure their Wi-Fi connection (WLAN) manually. *Section V* describes some new Standards to improve the security of today's as well as future WLAN.

Study of securely using external WLAN, such as public wireless access points, is outside the scope of this paper.

1.1 WLAN COMPONENTS

One important advantage of WLAN is the simplicity of its installation. Installing a wireless LAN system is easy and can eliminate the needs to pull cable through walls and ceilings. The physical architecture of WLAN is quite simple. Basic components of a WLAN are Access Points (APs) and Network Interface Cards (NICs)/client adapters.

1.1.1 Access Points

Access Point (AP) is essentially the wireless equivalent of a LAN hub. It is typically connected with the wired backbone through a standard Ethernet cable, and communicates with wireless devices by means of an antenna. An AP operates within a specific frequency spectrum and uses 802.11 standard specified modulation techniques. It also informs the wireless clients of its availability, and authenticates and associates wireless clients to the wireless network.

1.1.2 Network Interface Cards (NIC)/Client Adapter

Wireless client adapters connect PC or workstation to a wireless network either in ad-hoc peer-to-peer mode or in infrastructure mode (will be discussed in the following section) with APs. It connects desktop and mobile computing devices wirelessly to all network resources. The NIC scans the available frequency spectrum for connectivity and associates it to an Access Point (AP) or another wireless client. It is coupled to the PC/workstation operating system using a software driver. The NIC enables new employees to be connected instantly to the network and enable Internet access in conference rooms.

1.2 WLAN ARCHITECTURE

The WLAN components mentioned above are connected in certain configurations. There are two main types of WLAN architecture: Ad-hoc Network and Infrastructure Network.

1.2.1 Ad-hoc Network

This mode of operation, also known as *peer-to-peer mode*, is possible when two or more stations are able to communicate directly to one another. This is called *ad-hoc* Wi-Fi transmission. It is called ad-hoc because the network is set up only when mobile devices want to talk to each other, normally for specific purpose and for a short duration. One of the key advantages of ad-hoc WLANs is that theoretically

they can be formed anytime and anywhere, allowing multiple users to create wireless connections cheaply, quickly, and easily with minimal hardware and user maintenance. With ad-hoc network there is no connection to the other networks. The disadvantage of this method is that vendors must not implement speeds greater than 11 Mbit/s(802.11b) and only WEP encryption is available, not WPA(2).

A more enhanced version of Wi-Fi ad-hoc network called *Wi-Fi Direct* is launched in October 2010 for file transfers and media sharing through a new discovery and security-methodology. In this type of ad-hoc network, some devices can share their Internet connection, becoming hotspots or "virtual routers". The ad-hoc mode is depicted conceptually

in Figure 1-1.

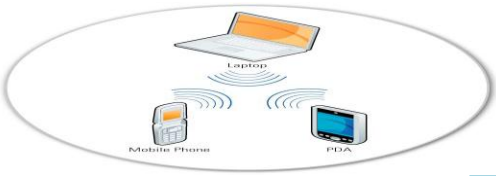

Figure1-1: Ad-hoc Network

1.2.2 Infrastructure Network

Infrastructure WLAN consists of wireless stations and access points. In infrastructure network, the mobile stations communicate with each other by having an access point. Access point is the device that acts as a bridge from the wireless network to the wired or fixed network. Access Points combined with a distribution system (such as Ethernet) support the creation of multiple radio cells that enable roaming throughout a facility. A combination of an AP & one or more station is called Basic Service Set (BSS). The access points not only provide communications with the wired network but also mediate wireless network traffic in the immediate neighborhood. The use of multiple APs connected to a single DS allows for the creation of wireless networks of arbitrary size and complexity. In the IEEE 802.11 specification, a multi-BSS network is referred to as an *extended service set* (ESS). Figure 1-2 shows the architecture of Infrastructure WLAN.

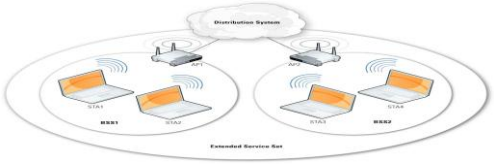

Figure 1-2: Infrastructure LAN

II.SECURITY THREATS OF WLAN

Despite the productivity, convenience and cost advantage that WLAN offers, the radio waves used in wireless networks create a risk where the network can be hacked. Most threats against wireless networks involve an attacker with access to the radio link between wireless devices. Network security attacks against WLANs are typically divided into two broad categories *active attacks* and *passive attacks*. These two broad classes are then subdivided into other types of attacks.

a)Active attacks

In this attack an unauthorized party makes modifications to a message, data stream, or file. It is possible to detect this type of attack, but it may not be preventable. Active attacks may take the form of one of four types (or a combination thereof):

b)Masquerading:

This is where the attacker could gain access to privileged data and resources in the network by assuming the identity of a valid user. This happens because 802.11 networks do not authenticate the source address, which is Medium Access Control (MAC) address of the frames. Attackers may therefore spoof MAC addresses and hijack sessions. Moreover, 802.11 does not require an Access Point to prove

it is actually an AP. This facilitates attackers who may masquerade as AP's. In eliminating spoofing, proper authentication and access control mechanisms need to be placed in the WLAN. It is also called Spoofing or Session Hijacking.

c)Denial of Service:

In this kind of attack, the intruder floods the network with either valid or invalid messages affecting the availability of the network resources. Due to the nature of the radio transmission, the WLAN are very vulnerable against denial of service attacks. The relatively low bit rates of WLAN can easily be overwhelmed and leave them open to denial of service attacks. By using a powerful enough transceiver, radio interference can easily be generated that would unable WLAN to communicate using radio path.

*d)***Message modification:**

The attacker alters a legitimate message by deleting, adding to, changing, or reordering the message.

Replay:

The attacker monitors transmissions and retransmits messages posing as the legitimate user.

Passive Attacks

In this attack an unauthorized party gains access to an asset and does not modify its content or actively attack or disrupt a WLAN. There are two types of passive attacks:

Eavesdropping:

This involves attack against the confidentiality of the data that is being transmitted across the network. By their nature, wireless LANs intentionally radiates network traffic into space. This makes it impossible to control who can receive the signals in any wireless LAN installation. In the wireless network, eavesdropping by the third parties is the most significant threat because the attacker can intercept the transmission over the air from a distance, away from the premise of the company. The attacker monitors wireless data transmissions between devices for message content, such as authentication credentials or passwords. An example of this attack is an attacker listening to transmissions on a WLAN between an AP and a client.

Traffic flow analysis:

The attacker gains intelligence by monitoring the transmissions for patterns of communication. A considerable amount of information is contained in the flow of messages

between communicating parties. This is a more subtle method than eavesdropping.

III.SECURITY OF LEGACY IEEE 802.11 WLAN

This section describes the security features provided by legacy IEEE 802.11 WLAN standards and explains their limitations. The section addresses WEP and WPA, which are designed to protect link-level data during wireless transmission between clients and APs.

a)WIRED EQUIVALENT PRIVACY (WEP)

Wired Equivalent Privacy (WEP) is a standard encryption for wireless networking. It is a user authentication and data encryption system from IEEE 802.11 used to overcome the security threats. Basically, WEP provides security to WLAN by encrypting the information transmitted over the air, so that only the receivers who have the correct encryption key can decrypt the information. WEP was designed by the IEEE to provide the following three basic security services:

*Authentication***:** To verify the identity of communicating client stations. This controls access to the network by denying access to client stations that cannot authenticate properly.

*Confidentiality***:** To use encryption to provide wireless networks with the same or similar privacy achieved by an unencrypted wired network. The intent was to prevent information compromise from casual eavesdropping.

*Integrity***:** To ensure that messages were not modified in transit between wireless clients and APs.

Weakness of WEP:

WEP has undergone much scrutiny and criticism that it may be compromised. What makes WEP vulnerable? The major WEP flaws can be summarized into three categories:

No forgery protection:

There is no forgery protection provided by WEP. Even without knowing the encryption key, an adversary can change 802.11 packets in arbitrary, undetectable ways, deliver data to unauthorized parties, and masquerade as an authorized user. Even worse, an adversary can also learn more about the encryption key with forgery attacks than with strictly passive
attacks.

No protection against replays:

WEP does not offer any protection again replays. An adversary can create forgeries without changing any data in an existing packet, simply by recording WEP packets and then retransmitting later. Replay, a special type of forgery attack, can be used to derive information about the encryption key and the data it protects.

Reusing initialization vectors:

By reusing initialization vectors, WEP enables an attacker to decrypt the encrypted data without the need to learn the encryption key or even resorting to high-tech techniques. While often dismissed as too slow, a patient attacker can compromise the encryption of an entire network after only a few hours of data collection.A report done by a team at the University of California's computer science department, presented the insecurity of WEP which expose WLAN to several types of security breaches. The ISAAC (Internet Security, Applications, Authentication and Cryptography) team which released the report quantifies two types of weaknesses in WEP. The first weakness emphasizes on limitations of the Initialization Vector (IV). The value of the IV often depends on how vendor chose to implement it because the original 802.11 protocol did not specify how this value is derived. The second weakness concerns on RC4's Integrity Check Value (ICV), a CRC-32 checksum that is used to verify whether the contents of a frame have been modified in transit. At the time of encryption, this value is added to the end of the frame. As the recipient decrypts the packet, the checksum is used to validate the data. Because the ICV is not encrypted, however, it is theoretically possible to change the data payload as long as you can derive the appropriate bits to change in the ICV as well. This means data can be tampered and falsified.

b)Wi-Fi POTECTED ACCESS (WPA)

In early 2003, the Wi-Fi Alliance, in coordination with the IEEE 802.11 Working Group, developed the Wi-Fi Protected Access (WPA) security enhancement to replace WEP. This was implemented as a stopgap measure until a robust IEEE 802.11 security standard could be developed and approved. WPA includes two main features: IEEE 802.1X and the Temporal Key Integrity Protocol (TKIP). The IEEE 802.1X port-based access control provides a framework to allow the use of robust upper-layer authentication protocols. It also facilitates the use of session keys that allow the rotation of cryptographic keys. TKIP includes four new features to enhance the security of IEEE 802.11: TKIP extends the IV space, allows for per-packet key construction, provides cryptographic integrity, and provides key derivation and distribution. Through these features TKIP provides protection against various security attacks discussed earlier, including replay attacks and attacks on data integrity. In addition, it addresses the critical need to periodically change encryption keys. However, WPA also has significant flaws and does not provide the level of security that IEEE 802.11i can.

IV.PRACTICAL SOLUTIONS FOR SECURING WLAN

Despite the risks and vulnerabilities associated with wireless networking, there are certainly circumstances that demand their usage. Even with the WEP flaws, it is still possible for users to secure their WLAN to an acceptable level. This could be done by implementing the following actions to minimize attacks into the main networks:

CHANGING DEFAULT SSID

Service Set Identifier (SSID) is a unique identifier attached to the header of packets sent over a WLAN that acts as a password when a mobile device tries to connect to a particular WLAN. The SSID differentiates one WLAN from another, so all access points and all devices attempting to connect to a specific WLAN must use the same SSID. In fact, it is the onlysecurity mechanism that the access point requires to enable association in the absence of activating optional security features. Not changing the default SSID is one of the most common security mistakes made by WLAN administrators. This is equivalent to leaving a default password in place.

Utilize VPN

A VPN is a much more comprehensive solution in a way that it authenticates users coming from an un-trusted space and encrypts their communication so that someone listening cannot intercept it. Wireless AP is placed behind the corporate firewall within a typical wireless implementation. This type of implementation opens up a big hole within the trusted network space. A secure method of implementing a wireless AP is to place it behind a VPN server. This type of implementation provides high security for the wireless network implementation without adding significant overhead to the users. If there is more than one wireless AP in the organization, it is recommended to run them all into a common switch, then connecting the VPN server to the same switch. Then, the desktop users will not need to have multiple VPN dial-up connections configured on their desktops. They will always be authenticating to the same VPN server no matter which wireless AP they have associated with [10]. Figure 4-1 shows secure method of implementing a wireless AP.

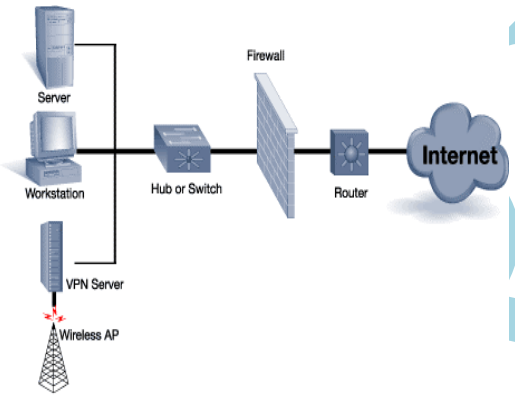

Figure 4-1: Securing a wireless AP using VPN Server

Utilize Static IP

By default, most wireless LANs utilize DHCP (Dynamic Host Configuration Protocol) to more efficiently assign IP addresses automatically to user devices. A problem is that DHCP does not differentiate a legitimate user from a hacker. With a proper SSID, anyone implementing DHCP will obtain an IP address automatically and become a genuine node on the network. By disabling DHCP and assigning static IP addresses to all wireless users, you can minimize the possibility of the hacker obtaining a valid IP address. This limits their ability to access network services. On the other hand, someone can use an 802.11 packet analyzer to sniff the exchange of frames over the network and learn what IP addresses are in use. This helps the intruder in guessing what IP address to use that falls within the range of ones in use. Thus, the use of static IP addresses is not fool proof, but at least it is a deterrent. Also keep in mind that the use of static IP addresses in larger networks is very cumbersome, which may prompt network managers to use DHCP to avoid support issues.

Access Point Placement

WLAN access points should be placed outside the firewall to protect intruders from accessing corporate network resources. Firewall can be configured to enable access only by legitimate users based on MAC and IP addresses. However, this is by no means a final or perfect solution because MAC and IP addresses can be spoofed even though this makes it difficult for a hacker to mimic.

Minimize radio wave propagation in non-user areas

Try orienting antennas to avoid covering areas outside the physically controlled boundaries of the facility. By steering clear of public areas, such as parking lots, lobbies, and adjacent offices, the ability for an intruder to participate on the wireless LAN can be significantly reduced. This will also minimize the impact of someone disabling the wireless LAN with jamming techniques.

V.NEW STANDARDS FOR IMPROVING WLAN SECURITY

Apart from all of the actions in minimizing attacks to WLAN mentioned in the previous section, we will also look at some new standards that intend to improve the security of WLAN. There are two important standards that will be discussed in this paper: IEEE802.1x and IEEE802.11i.

802.1x

One of the standards is 802.1x which was originally designed for wired Ethernet networks. This standard is also a part of the IEEE802.11i standard that will be discussed later in this section. The following discussion of 802.1x is divided into three parts, starting with the concept of Point-to-Point Protocol (PPP), followed by Extensible Authentication Protocol (EAP), and continues with the understanding of 802.1x itself.

PPP:

The Point-to-Point Protocol (PPP) originally emerged as an encapsulation protocol for transporting IP traffic over point-to-point links. PPP also established a standard for the assignment and management of IP addresses, asynchronous (start/stop) and bit-oriented synchronous encapsulation, network protocol multiplexing, link configuration, link quality testing, and error detection. By any measure, PPP is a good protocol. However, as PPP usage grew, people quickly found its limitation in terms of security. Most corporate networks want to do more than simple usernames and passwords for secure access. This leads to the designation of a new authentication protocol, called Extensible Authentication Protocol (EAP).

EAP

The Extensible Authentication Protocol (EAP) is a general authentication protocol defined in IETF (Internet Engineering Task Force) standards. It was originally developed for use with PPP. It is an authentication protocol that provides a generalized framework for several authentication mechanisms. These include Kerberos, public key, smart cards and one-time passwords. With a standardized EAP, interoperability and compatibility across authentication methods become simpler. For example, when user dials a remote access server (RAS) and use EAP as part of the PPP connection, the RAS does not need to know any of the details about the authentication system. Only the user and the authentication server have to be coordinated. By supporting

EAP authentication, RAS server does not actively participate in the authentication dialog. Instead, RAS just re-packages EAP packets to hand off to a RADIUS server to make the actual authentication decision . How does EAP relate to 802.1x? The next section will explain the relation.

802.1x:

IEEE 802.1x relates to EAP in a way that it is a standard for carrying EAP over a wired LAN or WLAN. There are four important entities that explain this standard.

Authenticator:

Authenticator is the entity that requires the entity on the other end of the link to be authenticated. An example is wireless access points.

Supplicant:

Supplicant is the entity being authenticated by the Authenticator and desiring access to the services of the Authenticator.

Port Access Entity (PAE):

It is the protocol entity associated with a port. It may support the functionality of Authenticator, Supplicant or both.

Authentication Server:

Authentication server is an entity that provides authentication service to the Authenticator. It maybe co-located with Authenticator, but it is most likely an external server. It is typically a RADIUS (Remote Access Dial In User Service) server.

802.11i

In addition to 802.1x standard created by IEEE, one recent 802.11 specification, which is 802.11i, provides replacement technology for WEP security. In this paper, the key technical elements that have been defined by the specification will be discussed. The 802.11i specification consists of three main pieces organized into two layers. On the upper layer is the 802.1x, which has been discussed in the previous section. As used in 802.11i, 802.1x provides a framework for robust user authentication and encryption key distribution. On the lower layer are improved encryption algorithms. The encryption algorithms are in the form of the TKIP (Temporal Key Integrity Protocol) and the CCMP (counter mode with CBC-MAC protocol). It is important to understand how all of these three pieces work to form the security mechanisms of 802.11i standard. Since the concept of 802.1x has been discussed in the previous section, the following section of this paper will only look at TKIP and CCMP. Both of these encryption protocols provide enhanced data integrity over WEP, with TKIP being targeted at legacy equipment, while CCMP is being targeted at future WLAN equipments. However, a true 802.11i system uses either the TKIP or CCMP protocol for all equipments.

TKIP:

The temporal key integrity protocol (TKIP) which initially referred to as WEP2, was designed to address all the known attacks and deficiencies in the WEP algorithm. According to 802.11 Planet, the TKIP security process begins with a 128-bit temporal-key, which is shared among clients and access points. TKIP combines the temporal key with the client machine's MAC address and then adds a relatively large 16-octet initialization vector to produce the key that will encrypt the data. Similar to WEP, TKIP also uses RC4 to perform the encryption. However, TKIP changes temporal keys every 10,000 packets. This difference provides a dynamic distribution method that significantly enhances the security of the network. TKIP is seen as a method that can quickly overcome the weaknesses in WEP security, especially the reuse of encryption keys.

CCMP

As explained previously, TKIP was designed to address deficiencies in WEP; however, TKIP is not viewed as a long-term solution for WLAN security. In addition to TKIP encryption, the 802.11i draft defines a new encryption method based on the advanced encryption standard (AES). The AES algorithm is a symmetric block cipher that can encrypt and decrypt information. It is capable of using cryptographic keys of 128, 192, and 256 bits to encrypt and decrypt data in blocks of 128 bits. More robust than TKIP, the AES algorithm would replace WEP and RC4. AES based encryption can be used in many different modes or algorithms. The mode that has been chosen for 802.11 is the counter mode with CBCMAC protocol (CCMP). The counter mode delivers data privacy while the CBC-MAC delivers data integrity and authentication. Unlike TKIP, CCMP is mandatory for anyone implementing 802.11i

VI.CONCLUSION

The general idea of WLAN was basically to provide a wireless network infrastructure comparable to the wired Ethernet networks in use. It has since evolved and is still currently evolving very rapidly towards offering fast connection capabilities within larger areas. However, this extension of physical boundaries provides expanded access to both authorized and unauthorized users that make it inherently less secure than wired networks. WLAN vulnerabilities are mainly caused by WEP as its security protocol. However, these problems can be solved with some new standards, such as 802.11i. For the time being, WLAN users can protect their networks by practicing the suggested actions that are mentioned in this paper based on the cost and the level of security that they wish.

REFERENCES

[1] Karen Scarfone, Derrick Dicoi, Matthew Sexton, Cyrus Tibbs, "Guide to Securing Legacy IEEE 802.11 Wireless Networks" *Recommendations of the National Institute of Standards and Technology, Department of Commerce, U.S.A., July 2008*

[2] "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i " *National Institute of Standards and Technology, Special Publication (NIST SP) 800-97, Available at URL: http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf*

[3] General Introduction to IEEE802.11 is available at URL: *http://www.ieee802.org/11/Tutorial/General.pdf*

[4] Description of IEEE802.11 and its amendments is available at URL: *http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm* and *http://standards.ieee.org/getieee802*

[5] Information about IEEE802.11 2007 Edition is available at URL: *http://standards.ieee.org/getieee802/download/802.11-2007.pdf*

[6] Information about IEEE802.11i 2004 Edition is available at URL: *http://standards.ieee.org/getieee802/download/802.11i-2004.pdf*

[7] Information about IEEE802.11X 2004 Edition is available at URL: *http://standards.ieee.org/getieee802/download/802.1X-2004.pdf*