ISSN 2229-5518

A Comprehensive Study of Wi-Fi Security – Challenges and solutions

Smita Parte[1], Smriti Pandya[2]

Abstract:-A wireless local area Network (LAN) is being widely recognized as a viable cost effective general purpose solution in providing high speed real time access to information. With a WLAN, users can gain access to shared information without being bound to fixed plug-in-point. WLAN transmit and receive data over the Air (OTA) and thus collectively combine data connectivity with ease of mobility. It is a radio frequency data communication. WLAN provides wireless access to multi location enterprises, small and medium enterprises. It can replace wired LAN or simply be used as extension of wired infrastructure so WLAN continue to gain market momentum. Besides all these advantages WLAN are also facing major problems of security. So security is the aspect where most of the researchers are working.

In this we are discussing major security challenges, issues, attacks and solutions to those problems and objectives of this study. Added to the convenience and cost advantages over traditional wired network some of the benefits include scalability, mobility, simplicity, reduced cost and installation speed. Therefore it is necessary to provide the security of WLAN equals to wired LAN

Keywords: WLAN, OTA, IEEE 802.11, Security threats, MAC, OFDM, BSS, ESS, AP

1. Introduction

Now days WLANs is more and more famous due to their reduced price of components, easy to deploy at anytime and anywhere in the world. End client are in a position to send big files through the communication medium that is air and free to move in the boundary of WLAN, able to access the internet and large bandwidth activities without the need of any cable or connectivity with a switch or a hub. Besides all of these advantage WLANs are facing the problem of security because many companies are transferring their sensible data across the WLANs so lots of people are doing research on the WLAN security.

In 1997, IEEE (institute of electrical & electronics engineers) released the 802.11 wireless local area network (WLAN) standard [1] as the name suggests, it belong to the group of popular IEEE 802.x standards ,e.g., IEEE 802.3 Ethernet[2] & IEEE 802.5 token ring[3]. IEEE802.11defines media access control (MAC) and physical layer specification for wireless LANs. In 1999, IEEE introduced two enhanced physical layer specifications 802.11a [4] and 802.11b [5] with data transmission rates of up to 11 and 54 Mbps, respectively. 802.11b is also based on DSSS and operates in the 2.4 GHz band and 802.11a is based on OFDM (orthogonal frequency division multiplexing) and operates in 5GHz band. In 2003, IEEE released 802.11b physical layer to support data transmission rates of up to 54mbps in the 2.4GHz band.

Wi-Fi allows user to surf internet at broadband speed when connected to access point (AP) or in ad hoc mode. The IEEE 802.11 architecture consists of several components that interact to provide a wireless LAN that support station mobility transparency to upper layers. The basic cell of an IEEE 802.11 LAN is called a basic service set (BSS), which is a set of mobile or fixed stations. If a station moves out of its

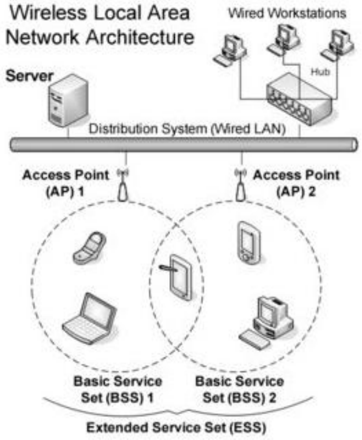

Figure1: Architecture of WLAN

2. Related works

A lot of research has been done in exploring threats, vulnerabilities, attacks and a variety of counter measures to overcome the same has been proposed .To protect the wormhole, each node shares a secret key with every other node and maintains an updated list of its neighbors. Neighbor list are built in a secure manner by using the direction in which a signal is heard from a neighbor with the assumption that the antennas on all the nodes are aligned. To provide the security to WLANs, it requires five main security requirements to be achieved which are data integrity, confidentiality, authentication, access control & non repudiation. The Attack in Wireless Network is introduced by S. Capkun,L.Buttyan [6], Deng,,W. Li,Agrawal [7], J. P. HuBaux ,L.Buttyam and S. Capkun [8], H. Hsieh and R Sivakumar [9], in IEEE Std. 802.11 i/D30 [14], in book Stalling, W., Cryptography and Network Security [16].

Organization of this paper is as follows: security goals is in section 3, Types of attacks in section 4, solutions in section 5, and section 6 described the objective of study, finally section 6 and 7 are conclusion and references respectively

3. Security Goals

1) **Authentication:** This means that before sending and receiving data using the system the receiver and sender identify should be verified.
2) **Confidentiality:** Usually this function is how much people identify a secure system it means that only the authenticated people are able to interpret the message content and one else.
3) **Helvetica:** Integrity means that the content of the communicated data is be free from any type of modification between the end points (sender and receiver). The basic form of integrity is packet check sum in IPv4 packets.
4) **Non–Repudiation:** This function implies that neither the sender nor the receiver can falsely deny that they have sent a certain message.
5) **Service reliability and availability:** Since secure systems usually get attached by intruders, which may affect their availability and type of service to their users. Such system should provide a way to grant their users the quality of service they expect.

4. Types of attacks on WLAN Security

Before examining the security solutions available today, it is important to define some of the security risks faced by WLANs. All LANs, wired or wireless, are vulnerable to two types of attack:

1) **Active attack:** Hackers gain access to the LAN to destroy data.
2) **Passive attack:** Hackers gain access to the LAN, but can only eavesdrop to transmitted data. Wireless LANs are more susceptible to both types of attack because hackers do not require a physical connection to the premises.

4.1 Active Attacks

A direct attack by intruder, with specific intent to disrupt network operations or access data.

1) **Denial of service:** A denial of service attack disrupts a network by flooding the bandwidth with meaningless data to bring to halt. To initiate a DoS attack, the intruder discovers an access point on the wireless network and then sent it a continuous stream of meaningless information, the data stream overwhelms the access point, causing it become unusable. DoS attacks may be sophisticated as spoofing 802.11 disassociation management frames to the wireless terminals, or as simple as using an RF generator in the 2.4 GHz band to jam the RF channel.
2) **Malicious association:** Malicious association is when wireless device can be actively made by crackers to connect to a company network through their cracking, laptop instead of company access point (AP). The idea behind this type of attack may not be to break into VPN or other security measures.
3) **Spooling:** One of the most basic type of active attacks where by the intruder configure their wireless terminal to appear to have the same MAC address as an authorized access point or wireless terminal. When spoofing an access point, the intruder's terminal appears as the authorized access point, with the intent to associate with an authorized wireless terminal and access the data on that device.
4) **Accidental association:** Unauthorized access to company wireless network can come from a number of different methods .one of these methods is referred to as "Accidental association". When a user turns on a computer and it latches on to a wireless access point from neighboring companies overlapping network. The user may not even know that this has occurred.
5) **Replay attacks:** The intruder monitors and captures transmitted packets between a wireless terminal and access point. This can be achieved via a passive monitoring utility called a 'sniffer'; such as air snort, which is readily available on the internet as freeware. once the packet is captured ,the hacker can do on the two things: Initiate a DoS attack by repeatedly transmitting through the access point, because the packet contain valid data, The access point forwards it to the host server to process and respond with a data receipt message. The host server overloads if the packets is transmitted with enough frequency.

4.2 Passive attacks

One of the two types A) collect data in transit, without the interruption of communication between authorized devices. B) Penetrate a wireless network through a security hole. A passive attack does not require sophisticated methods or tools in order to eavesdrop and collect data.

1) **Ad Hoc Networks:** Ad hoc network can posses a security threat. These are defined as peer to peer networks between wireless computer that do not have access point in between them.

2) **Man–in–the middle:** An attack that requires sophisticated software and can cause significant disruption or data loss. The hacker inserts themselves between an access point and a wireless terminal to capture packets in transmission. The wireless terminal sees the hacker as authorized devices fails to detect the intruder and continue transmitting information .the intruder captures legitimate information and is also able to inject false data into the network, or initiate a DoS attack.

3) **Helvetica:** In a network injection attack ,a cracker can make use of access point that are exposed to non-filtered network traffic, the cracker injects bogus networking re-configuring commands that affect router ,switches and hubs.

4) **War-driving:** The most common form of passive attack. The RF signal of 802.11 networks may extend beyond the confines of a building. With a wireless laptop or terminal, a hacker simply drives through business districts passively listening for a strong RF signal. Without good security, little efforts are then required to penetrate the network.

5. Security Solutions

The nature of wireless communication creates three basic threats: Interception, Alteration and Disruption. Followings are some security solution to overcome the above mentioned security attacks and threats.

5.1 Securing Wireless Network

If we can secure the wireless networks then the probability of security threats and attacks may be decreased, below are some ideas to secure your wireless network.

1) **Use of firewall technology:** Computer on wireless network need some protection as any computer connected to the internet, if your firewall was shipped in the off mode, turn it on.

2) **Use of encryption and decryption technology:** One of the most effective way to secure wireless network is to use of encryption and decryption technology, most of the wireless devices have a built in encryption and decryption mechanism. in this technique the plain text is encrypted by using encryption technology and is again decrypt at the destination ,so your message may transmit securely from source to destination.

3) **Make sure that identifier broadcasting is OFF:** Many wireless devices have a mechanism called as identifier broadcasting ,it sends out a signal to any devices in the vicinity announcing its presence .you don’t need to broadcast this information. Hackers can use the identifier broadcasting to home in on vulnerable wireless networks. So make sure that the identifier broadcasting is OFF.

4) **Don’t access public hot spots:** Many cafes, hotel, airports and other public spots offer you to access wireless networks for their customers but there are some networks to hack your system and access the information which you are sending.

5.2 Encryption

The best method for protecting that confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic. This is especially important for organizations subjects to regulations

5.3 Preventing Alteration of Intercepted Communication

Interception and alteration of wireless transmissions represents a form of “man-in-middle” attack two types of counter measures can significantly reduce the risk of such attack :strong encryption and strong authentication of both devices and users.

5.4 Protecting the Confidentiality

Two types of counter measures exist for reducing the risk of eavesdropping on wireless transmissions. The first involves methods for making it more difficult to locate and intercept the wireless signals. The second involves the use of encryption to preserve confidentiality even if the wireless signal is intercepted.

5.5 Securing wireless access point

Insecure, poorly configured wireless access points can compromise confidentiality by allowing unauthorized access to the network.

Organization can reduce risk of unauthorized access to wireless networks by taking these three steps. Countermeasures to secure wireless access points are as follows-

1) **Eliminating rough access points:** Properly configuring all authorized access points, using 802.1x to authenticate all device. Authenticate all devices that are plugged into the network.802.1x

will authenticate all devices connected to the network

2) **Secure configuration of authorized access points:** It is ensure that all authorized wireless access point are securely configured .all default setting need to changed since known to all and can be used by attacker to perform illegal operations.

5.6 Countermeasures to reduce the risk of denial–of-service attacks

Wireless communication are also vulnerable to denial-of service(DoS)attacks. Organizations can take several steps to reduce the risk of such unintentional DoS attacks. Regular periodic audits of wireless networking activity and performance can identify problem areas; appropriate remedial actions may include removal of the offending devices or measures to increase signal strength and coverage within the problem area.

5.7 Signal hiding techniques

In order to intercept wireless transmissions, attackers first need to identify and locate wireless networks. There are, however, a number of steps that organizations can take to make it more difficult to locate their wireless access points. the easiest and least costly including the following :turning off the service set identifier(SSID)broadcasting by wireless access points, assign cryptic names to SSIDs, reducing signal strength to the lowest level than still provides requisite coverage or locating wireless access point in the interior of the building ,away from windows and exterior walls.

6. Objective of Study

Following are the major objective of our study-

1) To study the various Vulnerabilities and attacks on WLAN and their solutions.
2) To study the some of the exiting security methods used for securing WLAN and explore the possibility of improvements in the same.
3) To analyze the various techniques based on misuse detection or anomaly detection for securing WLAN.
4) To develop new efficient security measures.
5) To study number of commercial available security solutions.

7. Conclusion

WLAN security is neither straightforward nor easy, and it is constantly changing. Even WLANs increase client's productivity; they expose the network to a new group of hackers because WLAN works on OTA. Given the inherent security weakness of the 802.11 standard, all businesses, regardless of size, need to determine their security requirements based on the application using the WLAN. In this we have discussed all security issues and solution to those issues so that a WLAN is as protected as Wired LAN.

REFERENCES

[1] Prasad , N. R., and A. R. Prasad (eds.), WLAN Systems and Wireless Ip for Next Gereration Communications, Norwood, MA: Artech House. January 2002

[2] IEEE Std. 802.3, part 3:Carrier Sense Multiple Access with Collision detection(CSMA/CD) Access Method and Physical Layer Specification.1985

[3] IEEE std. 802.5,Token Ring Access method and Physical Layer Specification. 1985

[4] IEEE Std. 802.11a, Supplement to part 11: Wireless LAn Medium Access Control(MAC) and Physical Layer (PHY) Specification: Higher Speed Physical Layer Extension in the 5 GHz band. 1999

[5] IEEE Std. 802.11b, Supplement to part 11: Wireless LAn Medium Accesss Control(MAC) and Physical Layer (PHY) Specification: Higher Speed Physical Layer Extension in the 2.4 GHz band. 1999

[6] S. Capkun,L.Buttyan, and J. HUBAUX,"Sector: secure Tracking of Node Encounters in Multi-hop Wireless Networks.proc.of Acm Workshop on Security of Ad Hoc and Sensor Networks," 2003

[7] Deng,,W. Li,Agrawal,D P.,"Routing Security in Wireless Ad Hoc Networks," Cincimmati Uni.,OH,USA;IEEE Communication Magazine,Oct. 2002, vol. 40,pp.70-75,ISSn :0163-6804

[8] J. P. HuBaux ,L.Buttyam and S. Capkun., "The Quest for Security Immobile Ad Hoc Network, " In Proc. ACM MOBICOM, Oct.2001

[9] H. Hsieh and R Sivakumar, "Transport over Wireless networks, " Handbook of wireless Networks and mobile computing

[10] Y. Hu, A. Perrig, and D Johnson "packet Leashes: A defence Against WormHole Attacks in Wireless Ad Hoc networks,"Proc. Of IEEE INFORCOM. 2002

[11] J. Kong et al.,"Providing Robust and Ubiquitous Security Support for Mobile AdHoc Networks,"Prentice Hall PTR, A Division of Pearson Education Inc 2002

[12] Kyasanur , and N. Vaidya, "Detaction and handling of MAC layer Misbehaviour in Wireless Networks," DCC,2003

[13] P. Michiardi. R. Molva, 'Ad Hoc Netwoks Security," IEEE press Wiley, New York, 2003

[14] IEEE Std. 802.11 i/D30, "Wireless Medium Access Control(MAC) and physical Layer(PHY)Specification for enhanced Security," 2002

[15] Black, U., Internet Security Protocol: Protecting Traffic, Upper Saddle River, NJ: Prentice Hall 2000

[16] Stalling, W., Cryptography and Network Security: Principles and Practice ,Upper Saddle River, NJ: Prentice Hall 2000

[17] E. Ferro and F. Potorti, "Blutooth and Wi-fi Wireless protocol: A survey and a Comparision ", IEEE Wireless Commmun., Vol 12, No 1, pp, 12-16, Feb 2005

Mrs Smita Parte , Assistant Professor , TIT College Bhopal, 462026 , MP, India, MNo.-9907525480, E-Mail-smita.athanere@gmail.com

Ms Smriti Pandya,M Tech (CSE) Student ,TIT Science,Bhopal, 402026, MP,India