Wireless LAN Security: Addressing Challenges, Attacks and Solutions

Gurpreet Kaur[#1], Kirandeep Kaur*[2]

[#]*Department Of Computer Science And Technology*
Dr. B.R. Ambedkar National Institute Of Technology, Jalandhar, India
** Department Of Computer Science And Technology*
D.A.V. College, Jalandhar, India

***Abstract*— With tremendous growth and advancement in wireless technology and excessive use of internet in all the applications, security has become one of the most crucial and most demanding factor in wireless LAN, no matter if it is an individual, home or a business network. Regardless of different benefits of wireless LANs like mobility, flexibility, reduced cost of ownership and scalability, WLAN also have security issues that must be properly dealt with. Security involves protection of data and nodes from different types of attacks, unauthorized access and misuse of data and systems. Security basically is an overall strategy rather than a technology. It is all about the level of effort one can put into the network for securing it or the level of risk one is willing to tolerate . All the components exist in order to secure the wireless network. This paper will discuss different challenges in a wireless LAN, different types of attacks and different security considerations and strategies which will help an individual user and enterprises in securing their wireless LAN. It also emphasizes on the importance of training and knowledge of safe and reliable wireless network usage.**

***Keywords*— Authentication, EAP, Encryption, IDS, IPS, IEEE 802.11i, IEEE 802.11x, IPSec, WEP, Wireless Attacks, Wireless LAN, Wireless Security, WPA.**

I. INTRODUCTION

Wireless LAN is a network which enables a mobile user to connect to a local area network with the help of a wireless connection. Wireless technologies can erase the physical limitations of wired communications to increase user flexibility, boost employee productivity, and lower cost of network ownership also expose network-based assets to considerable risks. The configuration and reconfiguration of a wireless network is easier, faster and less expensive. Wireless enables a real-time enterprise responsive, collaborative, flexible, connected and informed in a connected society. At the same time wireless technology creates new threats and changes the existing information security risk profile because wireless communications takes place through the air using radio frequencies, hence the risk of interception is greater than with wired networks. Due to this, it suffers from various threats like snooping, unauthorized access, signal interference, loss of confidentiality, integrity and availability [1]. In order to protect WLAN from different threats, many wireless security standards have been developed like 802.11, 802.11b, 802.11g,WPA, VPN etc and different solutions, tools and techniques are devised to ensure the authenticity, integrity and confidentiality of data. In addition to this, different security measures can be taken by an individual or an enterprise in order to have an error free and secure wireless network. The real security for a wireless comes from the selection of a proven security technique which provides strongest authentication and encryption with the protection from different kinds of threats. The choice depends upon various factors like type of users, type of access by an individual or an enterprise and the kind of environment in which security has to be implemented.

This paper is organized in sections. In Section II, we describe different challenges and threats of WLAN. Section III includes different types of attacks in WLAN. Section IV will focus on different security standard and techniques for WLAN security. Section V includes practical solutions to secure a WLAN. At last we will include conclusion in Section V1.

II. CHALLENGES IN WLAN

As productivity and use of WLAN has increased, new challenges to security have come into picture. WLAN provides a unique set of challenges to IT and security professionals including incompatibility, support issues and insecure wireless LANs. A WLAN environment encounter following challenges:

A. Unreliable and Unpredictable Links

Wireless networks use the air, an uncontrollable medium for the transmission. Wireless LAN signals can travel through the walls, ceilings, and windows of buildings up to thousands of feet outside of the building walls. Additionally, since the WLAN medium is airwaves, it is a shared medium that allows any one in proximity to “sniff” the traffic. The risks of using a shared medium is increasing with the advent of readily-available “hacker’s tools. Wireless links are less reliable since there is no dedicated connection and signals are sent through air. Moreover they may vary over time and space.

B. Interference

A wireless network requires packets of data to travel through the air, making them prone to interception. Such breaches lead

to theft of sensitive corporate data and can also result in a loss of trust in the safety of the corporate network and are likely to attract unwanted and damaging attention.

C. Regulations and Spectrum

802.11 networks basically operate in the unlicensed frequencies of 2.4 GHz and 5 GHz. The unlicensed frequencies are open for use by anyone in contrast to cellular frequencies which require licenses. Despite of the fact that FCC has established certain rules of engagement which are mandatory to be following and which prohibit aggressive or malicious use, there is a difficulty in enforcing such rules in practical scenarios. So, frequencies have to be used and coordinated properly because the portion of usable frequencies is very limited.

D. Performance Issues

WLAN suffers from different performance issues like low bandwidth, high delays and large delay variation. Applications must use robust protocols and must tolerate these issues in order to have high performance [2].

E. Wireless Network Security

There are a number of wireless security threats: rogue access points masquerading as part of the network, the use of unauthorized devices, denial of service attacks, eavesdropping, masquerading, traffic analysis, modification [3]. These threats are due to authentication and encryption weaknesses and unauthenticated management frames. Wireless access must always include encryption, authentication and other security mechanisms that must be efficient and simple to use and provides the best security.

F. Misconfiguration of Wireless Devices and Clients

According to research from analyst firm Gartner, up to 70% and 90% of WLAN attacks were from misconfiguration of WLAN access points in 2006 and 2010 respectively. In recent news given by pcworld on April 19, 2013, a malfunctioning log-in system affected millions of people's ability to access a variety of Google applications on April 15, including Gmail and Drive. The misconfiguration of client devices usually occurs when users mess around with the client supplicant settings on their own without having any experience and knowledge. This usually happens while trying to set up their home WLAN or connecting to a public WLAN hotspot. Different wireless network devices, like access points, can get misconfigured too due to faulty misconfiguration and wrong settings.

G. Unawareness and Lack of Education

Last, but not the least, one reason for WLAN security breaches are a lack of awareness from end-users be it an individual or staff member. The old truth remains: most of the security threats to an organization come from the inside. Whether wired or wireless, the biggest challenge is still making sure that employees' environments are secure.

H. Other Risks and threats

1) BYOD – Increased network density
2) Rogue users – Security exposure
3) Access Point poor signal strength – Interruption of service
4) Access point oversubscription - Decreased availability
5) Honeypot APs – Mis-association of the network
6) Bandwidth abuse – Usage policy violations

III. DIFFERENT TYPES OF ATTACKS

Due to its open and wireless nature, WLAN is vulnerable to different types of attacks which can destroy an entire network, causes unavailability and subject the organization to legal liabilities. The description of various attacks is given as follows:

A. Denial of service attacks

This is an attack which poses a threat to the availability of data. This denial of service (DOS) attacks effectively shut down or severely slow down the wireless network in a similar way that DOS attacks affect wired networks. One common method of DOS attack is to saturate the target machine with excessive external communications requests due to which the machine stops responding to traffic which is legitimate or responds so slowly just like it is not responding at all making the services unavailable. A mischievous person can use a wireless client to insert bogus packets into the wireless LAN with the intent of keeping users from getting access to services. Other more eloquent methods for denying service include fooling valid radio NICs with fake 802.11 frames. Other mechanisms of DOS attacks include disruption in the working of physical network components, state and configuration information, computation of resources like hard disk, bandwidth or processor etc. These types of attacks result in number of problems like slow performance of the network, unavailability of resources like memory, processor , problems in accessing data and website, permanent disconnection of the connection and e-mail bombing. Various DOS attacks are ping of death, smurf attack, ICMP echo attack, tear drop attacks and many more.

B. Guessing passwords

This is one of the ways by which an attacker or a hacker gain access to your computer by obtaining your password somehow. If you are using an easy password that uses common English, common words like names of places, persons etc, then you are at risk. Hackers have various tools and software programs which enables to connect to services using many possible passwords and trying with different sequences of the passwords. Those software programs try to guess passwords using different forms of permutations of common words used in english and other foreign language words. An attacker or a hacker may also be successful in intercepting your password while logging into an insecure network like ftp or telnet.

C. Network Scans

Network Scanning is the process of examining the activity on a network, which can include monitoring data flow as well as monitoring the functioning of network devices. The hacker gets into the network by exploiting different security holes or bugs in the software providing the network service. Hackers usually search for these holes by doing a scan of the network. Then a hacker can connect to almost every possible IP address within range either by using his own computer or someone else computer of which he has taken control illegally. In order to know if a computer has a known bug, the connection attempts have to be carefully crafted. If this is carefully crafted, the scanning software identifies the hacker, who can then take control of the computer by exploiting the bug. Scanning can include war dialing, war driving, ping sweeps, and port scanning.

D. Injection Attacks

These types of attacks allow an attacker to insert code into a program or a query or insert malware or virus onto a computer to execute remote commands that can read or modify a database, or change data on a website and that can even destroy a database.[4]. A successful attack requires three elements:

1) Identifying the technology that the web application is running by simply trying all types of injection attacks and looking into web page footers, error pages, page source etc.
2) Identifying all possible user inputs by interacting with web pages in many ways like by using a web proxy such as Paros or Burp.
3) Finding the user input that is susceptible to the attack.

Attackers use different types of injection attacks like blind SQL Injection which enables him to use an error page that is returned by the database server to ask a series of True and False questions and it basically uses SQL statements to gain complete control of the database or even execute commands on the system, buffer overflow, LDAP injection etc. For example attackers use SQL injection to do anything from circumvent authentication to gain complete control of databases on a remote server.

E. IP address spoofing

It is a technique that involves replacing the IP address of an IP packet's sender with another machine's IP address. This technique lets a pirate send packets anonymously. It is not a question of changing the IP address, but rather of *impersonating* the IP address when packets are sent. It is a common misconception of using IP spoofing to hide your IP address while browsing the Internet, working with e-mails and online chatting etc. This is generally not true. Responses are misdirected due to the forging of the source IP address stating that you cannot create a normal network connection.

F. Eavesdropping

Eavesdropping is the unauthorized real-time interception of a private communication, such as a phone call, instant message, Video-conference or fax transmission. Any protocol analyzer can pick and record the calls without any information to the callers. The attacker uses various tools like network sniffers for this purpose. These tools basically collect packets or information on the network. Then depending on the quality of the tool used, they analyze the collected data in the form of protocol decoders or in the form of stream reassembling. With eavesdropping, following things could occur:

1) The speakerphone function can be turned on remotely, with the caller on mute so that there is no sound coming from the phone. This has happened with some IP phones in executives' offices. Their offices can be listened to without their knowledge.
2) PCs and laptops that have microphones attached or integrated into them can be enabled as listening devices without the user's knowledge. There is a rootkit available for this purpose.

Example: The process of eavesdropping is illustrated in Fig. 1.

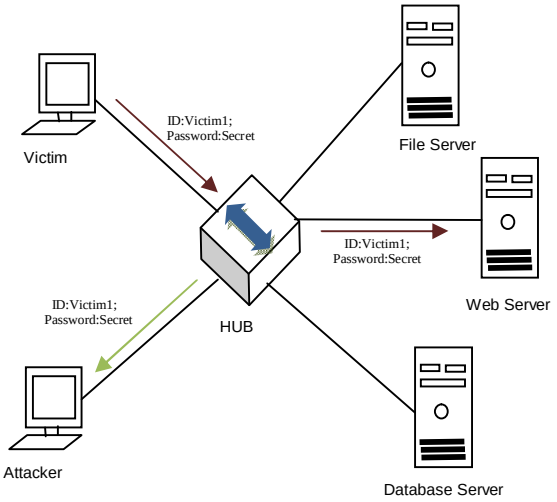

Fig. 1 Example of eavesdropping

In a Local Area Network where all the nodes are connected to HUB, the Network Eavesdropping becomes very easier because HUB redirects the complete traffic received on one node or port to all other nodes or ports. The attacker may capture all the traffic and sensitive information using a protocol analyzer opening a path for unauthorized access.

G. Hijacking

Hijacking is a situation in which an unauthorized and a malicious user takes control of an authorized user's WLAN connection. In a Wireless Local Area Network, hijacking is performed at Layer 2 for DOS attack and at Layer 3 for other attacking purposes posing a threat to availability and unnecessary modification of data. The process of hijacking Layer 2 which is MAC layer is outlined here:

1) With the help of software running on his computer, the attacker starts his own Access Point.
2) The attacker configures his AP in view of using the same SSID of the WLAN with which the victim is associated currently.
3) The attacker then sends a de-authentication frame which is equivalent to turning on a high−powered RF signal generator causing some interference which forces the victim to re-associate with the network and also forcing the victim to find out a new AP with which the victim has to associate.

Now, since the attacker's AP is closer to the victim and provides a stronger signal, the victim associates with the attacker's AP without even knowing if he is connected to a valid AP or a hacker's AP. This way attacker gains the access of the victim's computer and network.

H. Authentication and encryption cracking

With the adoption of poor authentication and encryption methods in WLAN, hacker finds a way for unauthorized access, data modification, masquerading and destruction of the data with the unavailability of data and systems posing a threat to confidentiality, integrity and availability.

I. MAC spoofing

MAC addresses can be spoofed which means faked or stolen. If an attacker can discover a valid MAC address, he can easily change the MAC address of his NIC to match.

J. Phishing attacks

Phishing is the act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing email messages, websites, and phone calls are basically designed to steal money. Phishing is typically carried out by e-mail spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users and exploits the poor usability of current web security technologies. Cybercriminals like hackers can do this by installing malicious softwares on your computer or even stealing the information from your computer.

IV. SAFEGAURDING WLAN: DIFFERENT SECURITY TECHNIQUES

To free a WLAN from different challenges, threats and attacks, it is essential to adopt different security techniques and methods. The choice of security technique depends upon the type of enterprise or an individual's network. Different security techniques are discussed here.

A. Adoption of Security Techniques Employing Strongest Encryption and Authentication

A wide variety of techniques are available for encryption and decryption to provide confidentiality and security of data. But the choice of most suitable technique makes a system free from different attacks and it depends on the type of environment and level of risk. To improve the performance, the security mechanisms developed should use relatively low complexity cryptographic algorithms [1]. Different security techniques which provide encryption are WEP, WPA, IPSec, TKIP and 802.11i. These techniques are briefly discussed here.

1) *WEP*: WEP i.e. Wired Equivalent Privacy was basically developed to provide confidentiality and privacy through the use of RC4 encryption and to provide authentication using basic pre-shared key authentication [5]. Relying only on WEP to provide security is not a good option since this method does not provide complete security against all attacks since WEP uses RC4 which is weak and the key can be found by analyzing sufficient data using tools like AirSnort and some of the initialization vectors which are used to pad key length are also weak giving a way for attackers.

2) *WPA*: WPA i.e. Wi-Fi Protected Access has been developed to remove the weaknesses of WEP. WPA encrypts the information using TKIP and it also ensures that the network security key has not been tampered. It improved data encryption through the temporal key integrity protocol (TKIP).TKIP scrambles the keys using a hashing algorithm and, by adding an integrity-checking feature, ensures that the keys have not been tampered with. WPA also includes authentication of users ensuring only authorized people to access the network. The most significant enhancement to WPA2 over WPA is the use of the Advanced Encryption Standard (AES) for encryption which provides much stronger security than WEP, addressing all the weaknesses and allowing compatibility and upgrades with older equipment.

3) *IPSec*: Internet Protocol security (IPSec) uses cryptographic security services to protect communications over Internet Protocol networks. IPSec addresses all security services like authentication, integrity and confidentiality. The basic idea of IPsec is to "mark" packets before being injected into the communications network, and use this "mark" at the receiving side in order to decide whether the packet arrived from the correct source, hence providing authentication. It checks whether the packet content is exactly the one generated by the source, without any modifications providing the integrity of data.

4) *802.11x Authentication*: It helps in enhancing the security of WLANs by using an authentication server

known as RADIUS to validate users and provide network access with the help of Extensible Authentication Protocol (EAP). EAP supports multiple authentication mechanisms like challenge-response, passwords, digital certificates etc. EAP can use any of its methods namely EAP-TLS, EAP-TTLS, PEAP, EAP-SIM, EAP-EKE etc. The most recommended option is EAP-TLS which is based on Transport Layer Security (TLS) protocol and uses public key cryptography for encryption and security.

5) *802.11i*: IEEE 802.11i enhances the WLAN security in the areas of encryption, authentication and key management. IEEE 802.11i is based on the Wi-Fi Protected Access(WPA), which is a quick fix of the WEB weaknesses. It works in two different authentication modes namely personal mode and enterprise mode. Personal mode provides simple security solution for home and small networks and only requires a pre-shared key for authentication. Enterprise mode is more suitable for large enterprises and uses 802.11x authentication mechanism. It also provides the support for intrusion detection and prevention. Other features provided by 802.11i are key caching, pre-authentication which are essential for advanced mobile applications such as Voice over Wireless LAN. Different enhancements provided by 802.11i finally delivered the level of data confidentiality and user authentication that an individual and enterprises have been demanding.

6) *Deployment of Mutual Authentication*: Mutual authentication between client and the network leads to strong security. This could be provided by the adoption of WPA and IEEE 802.11i which supports the concept of mutual authentication by proving the correct identities of both the parties involved in the communication.

B. Intrusion Detection and Prevention

Wireless detection and prevention systems are basically used to monitor network traffic and analyze the symptoms of possible incidents which violates the security principles and lead to different attacks and malicious access by unauthorized users [6]. An intrusion detection system (IDS) is software that automates the intrusion detection process. An intrusion prevention system (IPS) is software that has all the capabilities of an intrusion detection system and can also attempt to stop possible incidents. All WIDS systems need remote sensors distributed through monitored network and an IDS server often called as management software. The complete information about network is programmed into IDS server. Sensors passively observes network activities and reports the problems to IDS server which in return generates an alarm and take corrective actions for securing the network. WIPS solution has to be chosen with care because sometimes it may report a false detection and may also not detect threats. Unfortunately, WLANs remain vulnerable to denial-of-service (DOS) attacks. While enterprises may not be able to prevent DOS attacks, a wireless IDS can help detect when DOS attacks occur and where they came from. Despite of the fact that intrusion-detection systems have already been deployed by many organizations for wired networks, only have already deployed for their wired networks, but the protection from different attacks will be provided by WLAN-focused IDS before it can arrive the wired network.

C. Secure your Wireless Access Points

Access points like routers may be a direct target for hackers to enter into the network for malicious activities. Securing an access point needs the identification and elimination of rogue access points for which software like HWM HiGuard may be used. It also involves the proper configuration of all the access points with proper authorization and authentication features for which 802.11i may be used.

D. MAC Address Filtering

MAC addresses, which are the hardware addresses of the machines, on wireless clients are fixed, that is, these cannot be altered as they are burnt into the Network Interface Card (NIC). However, sometimes MAC addresses are impersonated or spoofed into the software by the wireless clients. This gives a pathway for the hackers for breaking into the WLAN network by configuring or setting their client to impersonate any of the available MAC addresses. Without the use of MAC address filtering feature, any wireless client, no matter, if he is a legitimate user or a hacker, he can easily get authentication to a Wi-Fi network by knowing the network name and other important security parameters including encryption keys. When this feature is enabled, the access point or router performs an additional step of authorizing the users by performing an additional check using a different parameter. Clearly the more the checks are made at different entry points, more is the likelihood of preventing malicious entry into a network causing different attacks and unauthorized access .

E. Security of Management Ports

A secure and authenticated method is provided by the management interface of WLAN system which has protected. Reconfiguring the access point using a management port can open a path for the hacker to use the network which can be controlled and eliminated by the use of different protocols like Secure Shell(SSH) protocol, Secure Socket Layer(SSL) etc.

F. Comprehensive Auditing for Best Practices

This is done by achieving mandated levels of protection and applying best practices including auditing proving that your network is secure and your practices are consistent with security guidelines, visibility giving administrators a global view from a single console and logging by automatically log all threats and actions taken. Continuous auditing of WLAN network would result in achieving confidentiality, integrity and availability.

G. Education and Training of Users

Since users are an integral part of a wireless system, they must be provided with the basic knowledge of different security considerations and associated risks of not following them. At the same time, training users on the usage of security strategies will lead to a safe and secure WLAN. To be effective, user training and education needs to be repeated periodically depending on the type of users and type of environment in which they work.

V. PRACTICAL SOLUTIONS FOR WLAN SECURITY

Following security measures could be taken by an individual or at organizational level:

1) Use anti-virus and anti-spy software.
2) Restrict unnecessary traffic by using a firewall and always turn ON the firewall.
3) Always turn off the SSID broadcasting.
4) Change the SSID and then pick a random SSID that gives no clue about your company or network
5) Change the default password on your router or access points.
6) Always choose strong passwords for access points and internet connection.
7) Allow restricted access. Do not go for open access to everyone.
8) Turn the wireless ON only in case you use it.
9) Limit access point connections.
10) Allow users to connect to the network through VPN.
11) Add MAC address filters.
12) Lock down the access point's configuration interface.
13) Do not depend on WEP only. Use IPSec, VPN, SSH.
14) 24x 7 Real-time Monitoring of Network Traffic.

VI. CONCLUSION

WLANs have created a new level of productivity and freedom for individuals and enterprises because of their numerous benefits. Wireless networks are helping and providing the opportunity to the individuals and business to cut costs, increase productivity, expansibility, mobility and usability. With this growth of WLAN, the importance of information and network security continues to grow because connecting to an unsecure network can leave a computer and complete network susceptible to a plethora of different security attacks and malicious activities. The security strategies and practical solutions discussed above assure a safe, attack free and secure WLAN. The implementation of different techniques discussed above like WPA, IPSec, SSL, 802.11i, TKIP, AES etc. will keep a WLAN protected from different types of attack. Combining a set of above techniques like 802.11 and AES can also ensure greater WLAN security. The best attitude to take towards wireless security has to be constantly vigilant, ensuring that the security used on WLAN is adapted as per the standards leading to high level of security.

VII. REFERENCES

[1] Min-kyu Choi1, Rosslin John Robles, Chang-hwa Hong, Tai-hoon Kim, "*Wireless Network Security: Vulnerabilities, Threats and Countermeasures*", International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No. 3, July, 2008

[2] Se Hyun Park a, Aura Ganz a and Zvi Ganz b," *Security protocol for IEEE 802.11 wireless local area network*", Mobile Networks and Applications 3 (1998) 237–246

[3] Arun Kumar Arigala, Sreeram.Munisankaraiah "*A perspective of Security in wireless networks*" , International Journal of Computer Trends and Technology (IJCTT) - volume4 Issue5–May 2013

[4] White Paper*: "Wireless LAN Security: What Hackers Know That You Don't"*, ©Motorola, Inc. 2008.

[5] Yang Xiao , Chaitanya Bandela , Xiaojiang (James) Du , Yi Pan , Edilbert Kamal Dass, " *Security mechanisms, attacks and security enhancements for the IEEE 802.11 WLANs*", Int. J. Wireless and Mobile Computing, Vol. 1, Nos. 3/4, 2006.

[6] White Paper" *WLAN Security Today: Wireless more Secure than Wired* ", Siemens Enterprise Communications July 2008.