ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.5 , No.1, Pages : 41 -45 (2016)
Special Issue of ICACEC 2016 - Held during 23-24 January, 2016 in Institute of Aeronautical Engineering, Quthbullapur, Telangana-43, India

WIRELESS LOCAL AREA NETWORK SECURITY USING WPA2-PSK

***S .DEEPTHI*[1]** ***G .MARY SWARNALATHA*[2]** ***PAPARAO NALAJALA*[3]**
Assoc. Professor, Dept. of Electronics &Communication Engineering at Institute of Aeronautical Engineering, deepthichowdarys@gmail.com
Assoc. Professor, Dept. of Electronics &Communication Engineering at Institute of Aeronautical Engineering, swarnasuresh.tr@gmail.com
Asst. Professor, Dept. of Electronics &Communication Engineering at Institute of Aeronautical Engineering, nprece@gmail.com

Abstract: The scope of this project is to communication plays prominent role in today's technology. Computer Network is the communication between two computers or within a small area called as LAN (Local Area Network) using wires. As technology is growing day by day to make easy way to access for end user, new technology came into existence by minimizing the need for wired connections called as WIFI (Wireless fidelity).

Wireless local area networks (WLANs) based on the Wi-Fi (wireless fidelity) standards are one of today's fastest growing technologies which is used in Business, Offices, Organizations, and Colleges etc. They provide mobile access to the Internet and to enterprise networks so users can remain connected away from their desks. The popularity gained is due to many reasons, such as ease of installation, installation flexibility, mobility, reduced cost-of-ownership, and scalability. Wireless networks are convenient and popular, but without security are easy to hack and leave your data at risk. Wireless communication medium is, by its nature, vulnerable to variety of threats, including unauthorized access, eavesdropping of communication, modification and repetition of data, denial of service, and fabrication of data. Therefore, it's essential that the security protocol can counter to these issues. In this seminar report, we introduce three commonly used WLAN security protocols algorithms such as WEP, WPA and WPA2 that try to provide protection against threats

Keywords: WLAN Components: LAN Access point, Network interface card, Wi-Fi Device

INTRODUCTION

A wireless local area network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive Information over the air. Wireless LAN (WLAN) is very popular nowadays. Wireless LANs enable users to communicate without the need of cable. Below is an example of a simple WLAN

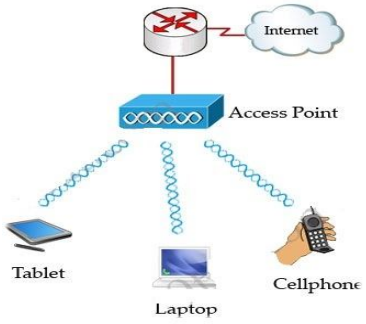

Fig.1 WLAN Architecture

The major difference between wired LAN and WLAN is WLAN transmits data by radiating energy waves, called radio frequency waves, instead of transmitting electrical signals over a cable
IEEE 802.11 is a standard specification for implementing wireless local area network (WLAN) computer communication in the 2.4, and 5GHZ frequency bands. They are created and maintained by the IEEE LAN/MAN Standards Committee (IEEE 802). The base version of the standard was released in 1997, and has had subsequent amendments. The standard and amendments provide the basis for wireless network products using the Wi-Fi brand.

Standard	Description
802.11	This original standard was released in 1997. It supports a 2-Mbps data rate over the 2.4-GHz frequency. A maximum range is undefined.
802.11a	This amendment was released in 1999. It supports a 54-Mbps data rate over the 5-GHz frequency. The maximum range is estimated at about 50 meters.
802.11b	This amendment was released in 1999. It supports an 11-Mbps data rate over the 2.4-GHz frequency. The maximum range is estimated at about 100 meters.
802.11g	This amendment was released in 2003. It supports a 54-Mbps data rate over the 2.4-GHz frequency. The maximum range is estimated at about 100 meters. 802.11g is backward-compatible with 802.11b.
802.11n	This amendment should be released in 2007. It will support a 540-Mbps data rate over the 2.4-GHz and 5-GHz frequencies. The maximum range is estimated at about 250 meters. 802.11n should be backward-compatible with 802.11a, 802.11b, and 802.11g.

Table 1.Wireless IEEE Standards

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.5 , No.1, Pages : 41 -45 (2016)
Special Issue of ICACEC 2016 - Held during 23-24 January, 2016 in Institute of Aeronautical Engineering, Quthbullapur, Telangana-43, India

Apart from the above the latest technologies like 802.11ac and 802.11ad provides upto 7Gbit/s which require Gigabit switches and advanced hardware.

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.

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 802.11standard specified modulation techniques. It also informs the wireless clients of its availability, and authenticates and associates wireless clients to the wireless network.

Fig: 2 Linksys Wireless Access point

Network Interface cards (NICS)/client adapters

Wireless client adapters connect PC or workstation to a wireless network either in ad hoc peer-to-peer mode or in infrastructure mode with APs (will be discussed in the following section). Available in PCMCIA (Personal Computer Memory Card International Association) card and PCI (Peripheral Component Interconnect), 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 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.

Fig: 2.1 D-Link Wireless adapter

WLAN ARCHITECTURE

There are two types of WLAN architecture: Independent or Adhoc mode and infrastructure mode WLAN.

Independent WLAN

The simplest WLAN configuration is an independent (or peer-to-peer) WLAN. It is a group of computers, each equipped with one wireless LANNIC/client adapter. In this type of configuration, no access point is necessary and each computer in the LAN is configured at the same radio channel to enable peer-to-peer networking. Independent networks can beset up whenever two or more wireless adapters are within range of each other.

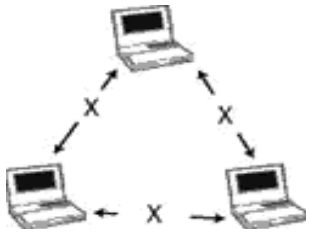

Fig: 3. Independent WLAN or ADHOC Mode WLAN

Infrastructure WLAN

Infrastructure WLAN consists of wireless stations and access points. Access Points combined with a distribution system (such as Ethernet) support the creation of multiple radio cells that enable roaming throughout a facility. The access points not only provide communications with the wired network but also mediate wireless network traffic in the immediate neighborhood. This network configuration satisfies the need of large-scale networks arbitrary coverage size and complexities

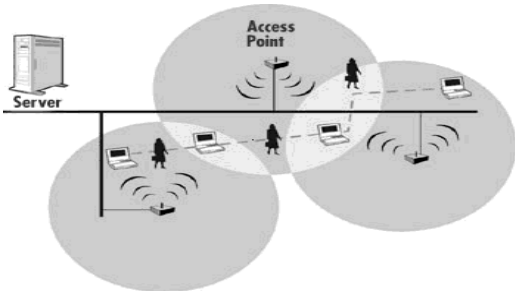

Fig: 3.1 Infrastructure WLAN

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. This section explains three examples of important threats: Denial of Service, Spoofing, and Eavesdropping.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.5 , No.1, Pages : 41 -45 (2016)
Special Issue of ICACEC 2016 - Held during 23-24 January, 2016 in Institute of Aeronautical Engineering, Quthbullapur, Telangana-43, India

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.

Spoofing and Session Hijacking

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.

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

WIRELESS SECURITIES

Wired Equivalent Privacy (WEP)

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. The following section explains the technical functionality of WEP as the main security protocol for WLAN.

How WEP Works

When deploying WLAN, it is important to understand the ability of WEP to improve security. This section describes how WEP functions accomplish the level of privacy as in a wired LAN WEP uses a pre-established shared secret key called the base key, the RC4encryption algorithm and the CRC-32 (Cyclic Redundancy Code) checksum algorithm as its basic building blocks. WEP supports up to four different base keys, identified by Key IDs 0 thorough 3. Each of these base keys is a group key called a default key, meaning that the base keys are shared among all the members of a particular wireless network. However, this is less common in first generation products, because it implies the existence of a key management facility, which WEP does not define. The WEP specification does not permit the use of both key-mapping keys and default keys simultaneously, and most deployments share a single default key across all of the 802.11devices.

WEP tries to achieve its security goal in a very simple way. It operates on MAC protocol Data Units (MPDUs), the 802.11 packet fragments. To protect the data in an MPDU, WEP first computes an integrity check value (ICV) over to the MPDU data. This is the CRC-32 of the data. WEP appends the ICV to the end of the data, growing this field by four bytes. The ICV allows the receiver to detect if data has been corrupted in flight or the packet is an outright forgery. Next, WEP selects a base key and an initialization vector (IV), which is a 24-bitvalue. WEP constructs a per-packet RC4 key by concatenating the IV value and the selected shared base key. WEP then uses the per-packet key to RC4, and encrypt both the data and the ICV. The IV and Key ID identifying the selected key is encoded as a four-byte string and pre-pended to the encrypted data. Figure 4depicts a WEP-encoded MPDU.

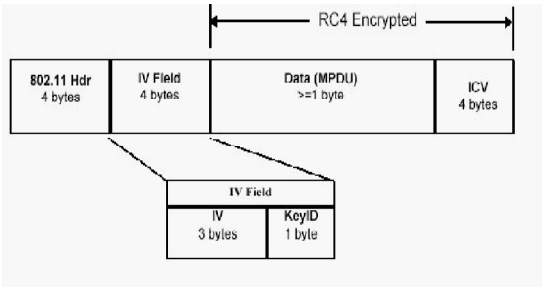

Fig 4. WEP-encoded MPDU

Wi-Fi Protected Access (WPA)

To overcome the limitations of WEP the WPA came into existence.WPA is the subset of the IEEE's 802.11i wireless security specification. Temporal Key Integrity protocol (TKIP) is the encryption method of WPA. The weaknesses of WEP addresses by TKIP by including mixing function, a message integrity check, an extended initialization vector, and a re-keying mechanism. The radius is to authenticate each server, WPA which depends upon central authentication. The compatible version of IEEE 802.11i is WPA, which is under development. To implement WPA both server and client computers updates their software's during 2003.WEP/WPA modes access points can operate to support both WEP and WPA clients. WEP security level is compatible with mixed level security for all users. The password will trigger authentication and TKIP encryption.

WPA-802.1x and WPA-PSK

WPA comes in two flavours, that is WPA-802.1x and WPA-PSK. WPA-802.1x is a good choice for large businesses

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.5 , No.1, Pages : 41 -45 (2016)
Special Issue of ICACEC 2016 - Held during 23-24 January, 2016 in Institute of Aeronautical Engineering, Quthbullapur, Telangana-43, India

because it combines access point authentication with another layer of authentication through external authentication services. This means that after the authenticating user associates with the wireless access point, his or her credentials are also checked against a locally stored database or even external sources (for example RADIUS or Kerberos). Authentication servers also distribute security keys to individual users dynamically. WPA-PSK on the other hand is a solution for small businesses and homes which utilizes so-called Pre-Shared Key (PSK) which is technically (from the user perspective) similar to how security keys with WEP are implemented but in a more secure way (more about this in the TKIP section below).

	Authentication	Encryption	Suitable for corporate WAN	Suitable for home and small business WLAN
WEP	none	WEP	poor	less than good
WPA (PSK)	PSK	TKIP	poor	best
WPA2 (PSK)	PSK	AES-CCMP	poor	best
WPA (full)	802.1x	TKIP	better	good (expensive)
WPA2 (full)	802.1x	AES-CCMP	best	good (expensive)

Table 2. Comparison between Wireless Security Protocols

As the name suggests, WPA2 is a second, newer version of Wireless Protected Access (WPA) security and access control technology for Wi-Fi wireless networking. WPA2is available on all certified Wi-Fi hardware since 2006 and was an optional feature on some products before that. It is designed to improve the security of Wi-Fi connections by requiring use of stronger wireless encryption than what WPA requires.
Specifically, WPA2 does not allow use of an algorithm called TKIP (Temporal Key Integrity Protocol) that has known security holes (limitations).
Most wireless routers for home networks support both WPA and WPA2 and administrators must choose which one to run. Obviously, WPA2 is the simpler, safer choice. Some techies point out that using WPA2 requires Wi-Fi hardware to work harder in running the more advanced encryption algorithms, which can theoretically slow down the network's overall performance compared to running WPA. Network owners can make their own choice but should run experiments to decide whether they notice any difference in their networks speeds with WPA2 vs. WPA.

Encryption algorithm and security fundamentals

WPA employs the RC4 encryption mechanism which is the same like WEP, but WPA uses a longer security key, 128 bit in length (compared to 104 bit in WEP) and longer initialization vector, 48 bit in length (compared to 24 bit in WEP). This gives WPA more strength compared to WEP because a hacker would need to capture significantly more data packets in case of WPA when trying to perform so-called *statistical attack*.

Encryption algorithms in WPA2

WPA2 compliments TKIP and the improved data integrity control algorithm with more secured encryption mechanism called Advanced Encryption Standard (AES) - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP). In other words, this means an improved encryption algorithm. Experts say that AES-CCMP is robust enough to be used for government data security purposes.

What are the disadvantages of WPA?

The disadvantage of WPA is that older wireless access points may need to have their firmware updated. Wireless clients' software also may need to be upgraded. For example, clients based on Windows XP effectively require either Service Pack 2 and some patches or the addition of the WPA client to their wireless configuration.

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: 802.1x and 802.11i.

802.1 xs

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.

i. 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.

ii. Supplicant

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

iii. Port Access Entity (PAE)

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

iv. Authentication Server

Authentication server is an entity that provides authentication service to the Authenticator. It may be co-located with Authenticator, but it is most likely an external server. It is typically a RADIUS (Remote Access Dial In User Service) server. The supplicant and authentication server are the major parts of 802.1x.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol.5 , No.1, Pages : 41 -45 (2016)
Special Issue of ICACEC 2016 - Held during 23-24 January, 2016 in Institute of Aeronautical Engineering, Quthbullapur, Telangana-43, India

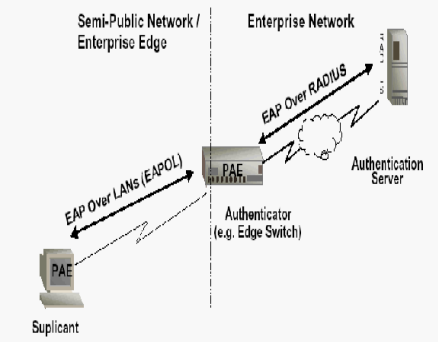

Fig 4.1: General topology of 802.1x components

RESULT

Security settings in wireless router/access point shown the below figure.

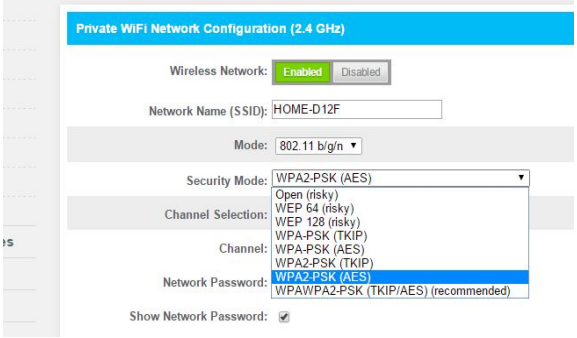

Fig.4.2 Security settings in wireless router/access point

APPLICATIONS

Applications of wireless communication involves in Computer devices like Laptops, Smart Phones, Tablets, Notebooks, security systems, television remote control, Wi-Fi, Cell phones, computer interface devices and various wireless communication based projects.

CONCLUSION

The development of wireless network is the unique and outstanding in the technology world because of its various advantages, portability and convenient to end user.

But security is the main concern, without implementation of security features in wireless network results data hacking and data will be infected by some malicious virus or Trojan horses. So to avoid this huge loss we need to use security features like WEP, WPA,WPA2 algorithms and while configuring wireless router or wireless access point.
Apart from the above algorithms we need to implement few incorporate access control Features such as MAC address filtering that deny requests from unwanted clients and also basic security precautions.

FUTURE SCOPE

Wireless technology development is growing rapidly and usage of wireless network among the people growing because of its convenience and faster working. Now days without wireless network we can't imagine this new generation. But as the Wi-Fi users are growing day-by-day there is a need to increase data rates and also high frequency bandwidth devices.
Recently a new technology has been introduced and made the wireless technology more advance, named as the Wireless Gigabit technology or WIGIG. Basically it is defined as the wireless technology that operates wireless over 60 Hz frequency band is called as the WIGIG technology. This technology is designed for the sake of the faster communication and faster transmission of data from one place to another at the more speed then Wi-Fi or the wireless LAN

REFERENCES

1. ANSI/IEEE Std 802.11, "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications," 1999.
2. Kevin Tyrrell, "An over view of Wireless security issues" GSEC V1.4b SANS Institute 2003
3. Stanley Wong, "The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards,
4. http://www.cisco.com/offer/urls/60628/1/210247_4
6."Overview of Wireless Communications"
7.http://www.cambridge.org/us/catalogue/catalogue.asp.isbn=0521837162&ss=exc
8.Wireless LAN Technologies". http://sourcedaddy.com/networking/wireless-lan-applications.html.

AUTHORS BIOGRAPHY

1. Deepthi S Working as Assoc. Professor in the Dept.of ECE at IARE, Hyderabad. 8 years of Experience in Teaching.Intrested areas Circuit designing, networking protocols, embedded systems

2. G. Mary Swarnalatha Working as Assoc. Professor in the Dept. of Electronics & Communication Engineering at IARE. 8 Years of experience in teaching .Interested areas Networking, Signal processing, embedded systems

3. Paparao Nalajala working as Asst. Professor in the Dept. Of ECE at IARE.4 Years of teaching and one year of Industry experience. Interested areas embedded systems, sensor technology, signal processing.