Interested in learning
more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Wireless LAN: Security Issues and Solutions

Wireless local area network (WLAN) has been widely used in many sectors. The popularity gained is due to many reasons, such as ease of installation, installation flexibility, mobility, reduced cost-of-ownership, and scalability. However, regardless of the benefits, WLAN have some security threats. This paper begins by introducing the concept of 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 Denial...

Copyright SANS Institute
Author Retains Full Rights

AD

Automate more Web application scanning.

watchfire

Wireless LAN: Security Issues and Solutions

Rafidah Abdul Hamid

GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4b
Option 1

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Table of Contents

Abstract 3

1.0 Introduction to WLAN 3

1.1 WLAN Components 4

1.1.1 Access Points 4

1.1.2 Network Interface Cards (NICs)/client adapters 4

1.2 WLAN Architecture 4

1.2.1 Independent WLAN 4

1.2.2 Infrastructure WLAN 5

1.2.3 Microcells and Roaming 5

2.0 Security Threats of WLAN 6

2.1 Denial of Service 6

2.2 Spoofing and Session Hijacking 7

2.3 Eavesdropping 7

3.0 Wired Equivalent Privacy 7

3.1 How WEP Works? 7

3.2 Weaknesses of WEP 9

3.2.1 No forgery protection 9

3.2.2 No protection against replays 9

3.2.3 Reusing initialization vectors 9

4.0 Practical Solutions for Securing WLAN 10

4.1 Changing Default SSID 10

4.2 Utilize VPN 10

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4.3 Utilize Static IP 11

4.4 Access Point Placement 11

4.5 Minimize radio wave propagation in non-user areas 12

5.0 New Standards for Improving WLAN Security 12

5.1 802.1x 12

5.1.1 PPP 12

5.1.2 EAP 13

5.1.3 802.1x 13

5.2 802.11i 15

5.2.1 TKIP 15

5.2.2 CCMP 16

6.0 Tools for Protecting WLAN 16

6.1 AirDefense 16

6.2 Isomair Wireless Security 17

6.3 Wireless Security Auditor (WSA) 17

7.0 Conclusion 17

References 19

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Abstract

Wireless local area network (WLAN) has been widely used in many sectors. The popularity gained is due to many reasons, such as ease of installation, installation flexibility, mobility, reduced cost-of-ownership, and scalability. However, regardless of the benefits mentioned above, WLAN have some security threats, in which anyone who use it or intend to use it should be aware of.

This paper begins by introducing the concept of 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 Denial of Service, Spoofing, and Eavesdropping. The paper will then explain how Wired Equivalent Privacy (WEP) works, which is the IEEE 802.11b/WiFi standard encryption for wireless networking. The discussion of WEP continues by examining its weaknesses, which result in it being much less secured than what was originally intended. 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. The 802.1x is actually included in 802.11i, a newly proposed standard for key distribution and encryption that will play a big role in improving the overall security capabilities of current and future WLAN networks. The 802.11i standard provides two improved encryption algorithms to replace WEP, which are Temporal Key Integrity Protocol (TKIP) and CBC-MAC Protocol (CCMP). This paper will also list down several products that will assist users to protect their wireless networks from attacks. Finally, this paper ends with the conclusion of highlighted issues and solutions.

1.0 Introduction to WLAN

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. In 1997, 802.11 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. The currently most spread and deployed standard, IEEE 802.11b, was introduced late 1999. It still operates in the same frequency range, but with a maximum speed of 11 Mbps.

WLAN has been widely used in many sectors ranging from corporate, education, finance, healthcare, retail, manufacturing, and warehousing. According to a study by the Gartner Group, approximately 50 percent of company laptops around the world will be equipped for WLAN by 2006 [14]. It has increasingly becoming an important technology to satisfy the needs for installation flexibility, mobility, reduced cost-of-ownership, and scalability.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

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 (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.

1.2 WLAN Architecture

The WLAN components mentioned above are connected in certain configurations. There are three main types of WLAN architecture: Independent, Infrastructure, and Microcells and Roaming [12].

1.2.1 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 LAN NIC/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 be

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

set up whenever two or more wireless adapters are within range of each other. Figure 1 shows the architecture of Independent WLAN.

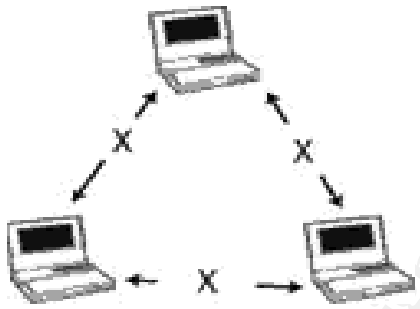

Figure 1: Independent WLAN [12].

1.2.2 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. Figure 2 shows the architecture of Infrastructure WLAN.

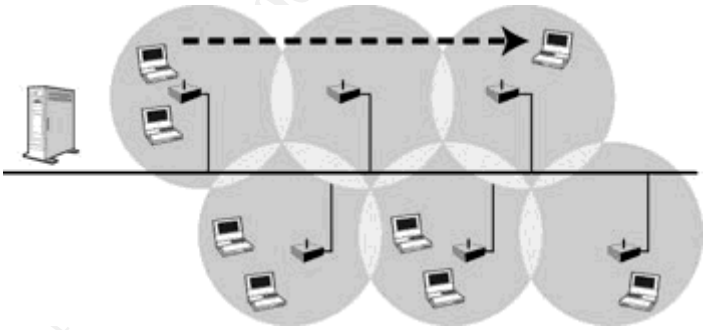

Figure 2: Infrastructure WLAN [12].

1.2.3 Microcells and Roaming

The area of coverage for an access point is called a "microcell'. The installation of multiple access points is required in order to extend the WLAN range beyond the coverage of a single access. One of the main benefits of WLAN is user mobility. Therefore, it is very important to ensure that users can move seamlessly between access points without having to log in again and restart their applications. Seamless roaming is only possible if the access points have a way of exchanging information as a

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

user connection is handed off from one access point to another. In a setting with overlapping microcells, wireless nodes and access points frequently check the strength and quality of transmission. The WLAN system hands off roaming users to the access point with the strongest and highest quality signal, in accommodating roaming from one microcell to another. Figure 3 shows the architecture of Microcells and Roaming.

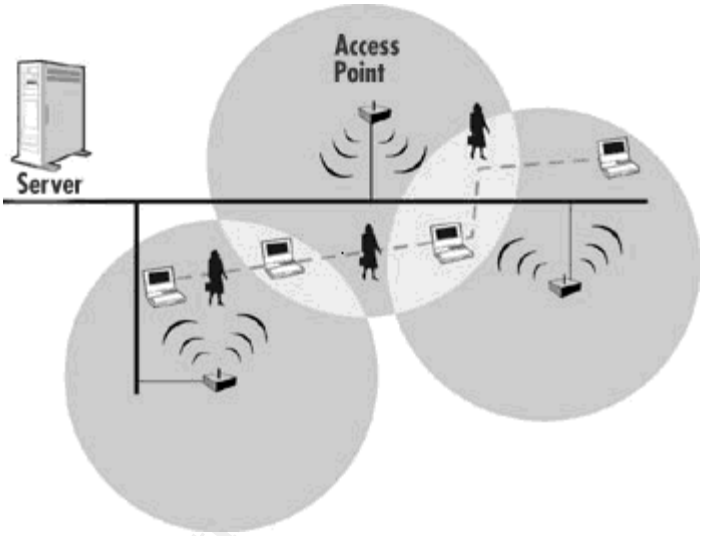

Figure 3: Microcells and Roaming [12].

2.0 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.

2.1 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 [9]. By using a powerful enough transceiver, radio interference can easily be generated that would unable WLAN to communicate using radio path.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

2.2 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 [9]. In eliminating spoofing, proper authentication and access control mechanisms need to be placed in the WLAN.

2.3 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.

3.0 Wired Equivalent Privacy

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

3.1 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 [16].

WEP uses a pre-established shared secret key called the base key, the RC4 encryption 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 KeyIDs 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. Some implementations also support a set of nameless per-link keys called key-mapping keys. However, this is less common in first generation products, because it implies the existence of a key

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

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 802.11 devices.

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-bit value. 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 KeyID identifying the selected key are encoded as a four-byte string and pre-pended to the encrypted data. Figure 4 depicts a WEP-encoded MPDU.

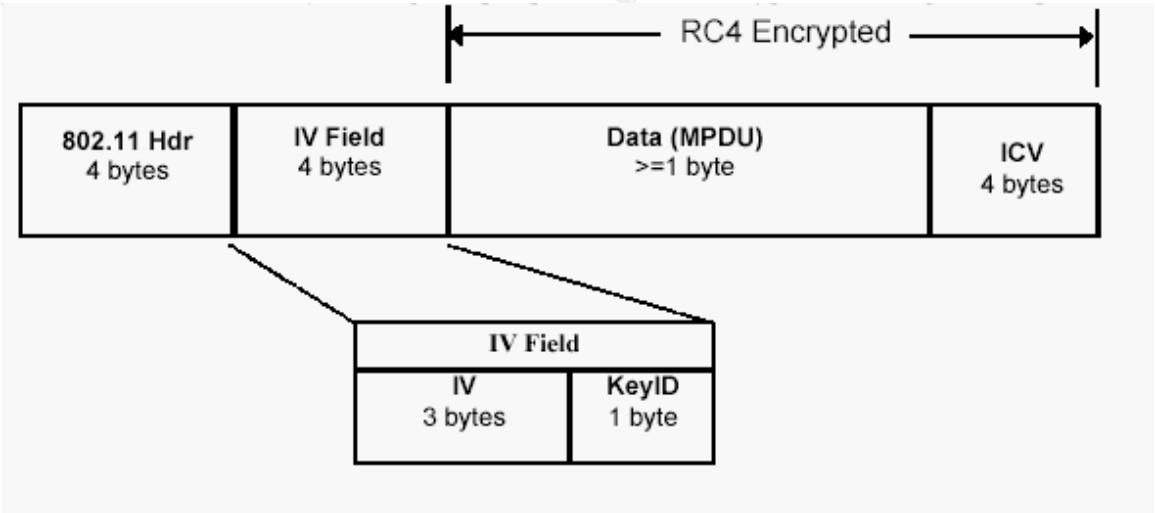

Figure 4: WEP-encoded MPDU [16].

The IEEE 802.11 standard defines the WEP base key size as consisting of 40 bits, so the per-packet key consists of 64 bits once it is combined with the IV. Many in the 802.11 community once believed that small key size was a security problem, so some vendors modified their products to support a 104-bit base key as well. This difference in key length does not make any different in the overall security. An attacker can compromise its privacy goals with comparable effort regardless of the key size used. This is due to the vulnerability of the WEP construction which will be discussed in the next section.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

3.2 Weaknesses 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 [17]:

3.2.1 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.

3.2.2 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.

3.2.3 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 [2] 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.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4.0 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 [5]:

4.1 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 only security 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.

4.2 Utilize VPN

A VPN is a much more comprehensive solution in a way that it authenticates users coming from an untrusted 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 5 shows secure method of implementing a wireless AP.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

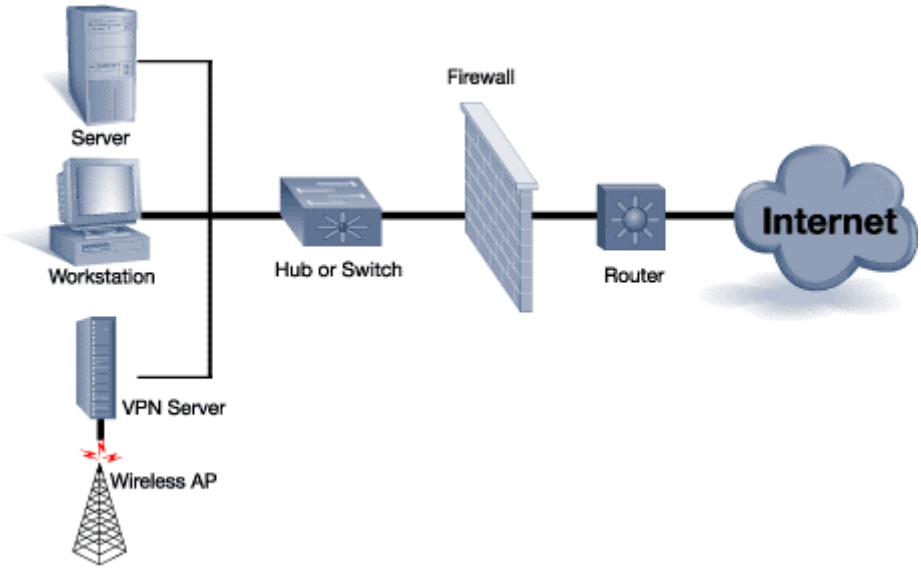

Figure 5: Securing a wireless AP [10].

4.3 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.

4.4 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.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

4.5 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.

5.0 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.

5.1 802.1x

One of the standards is 802.1x which was originally designed for wired Ethernet networks. This standard is also part of the 802.11i standard that will be discussed later. 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.

5.1.1 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, error detection, and option negotiation for such capabilities as network-layer address negotiation and data-compression negotiation [11]. 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 [13]. This leads to the designation of a new authentication protocol, called Extensible Authentication Protocol (EAP).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

5.1.2 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 [15]. 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 [13].

How does EAP relate to 802.1x? The next section will explain the relation.

5.1.3 802.1x

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 [18].

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 maybe co-located with Authenticator,

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

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. Figure 6 below shows the general topology of the above mentioned entities:

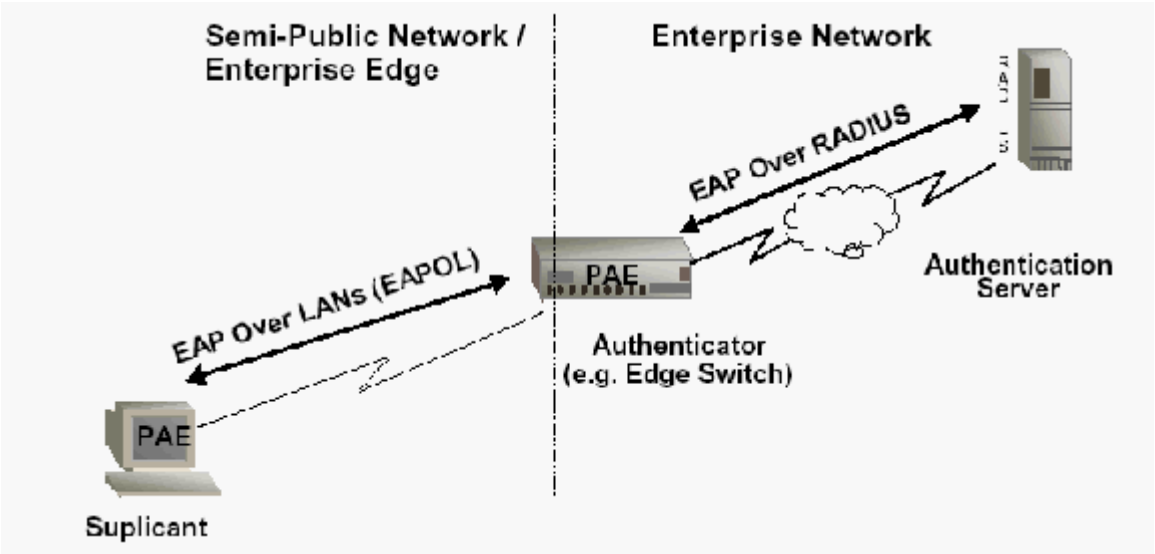

Figure 6: General topology of 802.1x components [18].

EAP messages are encapsulated in Ethernet LAN packets (EAPOL) to allow communications between the supplicant and the authenticator. The following are the most common modes of operation in EAPOL [13]:

i. The authenticator sends an "EAP-Request/Identity" packet to the supplicant as soon as it detects that the link is active.

ii. Then, the supplicant sends an "EAP-Response/Identity" packet to the authenticator, which is then passed to the authentication (RADIUS) server.

iii. Next, the authentication server sends back a challenge to the authenticator, with a token password system. The authenticator unpacks this from IP and repackages it into EAPOL and sends it to the supplicant. Different authentication methods will vary this message and the total number of messages. EAP supports client-only authentication and strong mutual authentication. Only strong mutual authentication is considered appropriate for the wireless case.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

iv. The supplicant responds to the challenge via the authenticator and passes the response onto the authentication server. If the supplicant provides proper identity, the authentication server responds with a success message, which is then passed to the supplicant. The authenticator now allows access to the LAN, which possibly was restricted based on attributes that came back from the authentication server.

5.2 802.11i

In addition to 802.1x standard created by IEEE, one up-and-coming 802.11x specification, which is 802.11i, provides replacement technology for WEP security. 802.11i is still in the development and approval processes. In this paper, the key technical elements that have been defined by the specification will be discussed. While these elements might change, the information provided will provide insight into some of the changes that 802.11i promises to deliver to enhance the security features provided in a WLAN system.

The 802.11i specification consists of three main pieces organized into two layers [4]. 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.

5.2.1 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 [6], 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

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

weaknesses in WEP security, especially the reuse of encryption keys. The following are four new algorithms and their function that TKIP adds to WEP [17]:

i. A cryptographic *message integrity code*, or MIC, called Michael, to defeat forgeries.

ii. A new IV *sequencing discipline*, to remove replay attacks from the attacker's arsenal.

iii. A per-packet *key mixing function*, to de-correlate the public IVs from weak keys.

iv. A *re-keying* mechanism, to provide fresh encryption and integrity keys, undoing the threat of attacks stemming from key reuse.

5.2.2 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 [3]. 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 CBC-MAC 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 [4].

6.0 Tools for Protecting WLAN

There are some products that can minimize the security threats of WLAN such as:

6.1 AirDefense™

It is a commercial wireless LAN intrusion protection and management system that discovers network vulnerabilities, detects and protects a WLAN from intruders and attacks, and assists in the management of a WLAN. AirDefense also has the capability to discover vulnerabilities and threats in a WLAN such as rogue APs and ad hoc networks. Apart from securing a WLAN from all the threats, it also provides a robust WLAN

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

management functionality that allows users to understand their network, monitor network performance and enforce network policies [1].

6.2 Isomair Wireless Sentry

This product from Isomair Ltd. automatically monitors the air space of the enterprise continuously using unique and sophisticated analysis technology to identify insecure access points, security threats and wireless network problems. This is a dedicated appliance employing an Intelligent Conveyor Engine (ICE) to passively monitor wireless networks for threats and inform the security managers when these occur. It is a completely automated system, centrally managed, and will integrate seamlessly with existing security infrastructure. No additional man-time is required to operate the system [8].

6.3 Wireless Security Auditor (WSA)

It is an IBM research prototype of an 802.11 wireless LAN security auditor, running on Linux on an iPAQ PDA (Personal Digital Assistant). WSA helps network administrators to close any vulnerabilities by automatically audits a wireless network for proper security configuration. While there are other 802.11 network analyzers such as Ethereal, Sniffer and Wlandump, WSA aims at protocol experts who want to capture wireless packets for detailed analysis. Moreover, it is intended for the more general audience of network installers and administrators, who want a way to easily and quickly verify the security configuration of their networks, without having to understand any of the details of the 802.11 protocols [7].

7.0 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 the new standards, such as 802.11i, which is planned to be released later this year. 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.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

However, there will be no complete fix for the existing vulnerabilities. All in all, the very best way to secure WLAN is to have the security knowledge, proper implementation, and continued maintenance.

© SANS Institute 2003, Author retains full rights

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

References

[1] AirDefense™, Inc. "Wireless LAN Security: Intrusion Detection and Monitoring for the Enterprise." 4 Dec. 2002. URL: http://www.airdefense.net/products/index.shtm (30 Oct. 2002).

[2] Borisov, Nikita, Goldberg, Ian and Wagner, David. "Security of the WEP Algorithm." 13 Dec. 2002. URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (3 Dec. 2002).

[3] Computer Security Research Centre, National Institute of Standards and Technology. "Announcing the Advanced Encryption Standard (AES)."Federal Information Processing Standards Publications 197. 13 Dec. 2002. URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf (3 Dec. 2002).

[4] Eaton, Dennis." Diving into the 802.11i Spec: A Tutorial." 3 Jan. 2003. URL: http://www.commsdesign.com/design_corner/OEG20021126S0003 (18 Dec. 2002).

[5] Geier, Jim. "Guarding Against WLAN Security Threats." 2 Dec. 2002. URL: http://www.80211-planet.com/tutorials/article.php/1462031 (28 Oct. 2002).

[6] Geier, Jim. "802.11 Security Beyond WEP". 2 Dec. 2002. URL: http://www.80211-planet.com/tutorials/article.php/1377171 (28 Oct. 2002).

[7] IBM Corporation. "Wireless Security Auditor (WSA)." 4 Dec. 2002. URL: http://researchweb.watson.ibm.com/gsal/wsa/ (30 Oct. 2002).

[8] Isomair.com. "Isomair Security for Wireless World" 4 Dec. 2002. URL: http://www.isomair.com/products.html (30 Oct. 2002).

[9] Knowledge Systems (UK) Ltd. "Wireless LAN Security Issues." 2 Dec. 2002. URL: http://www.ksys.info/wlan_security_issues.htm (28 Oct. 2002).

[10] Penton Media, Inc. "Use a VPN for Wireless Security." 20 Dec. 2002. URL: http://www.mobile-and-wireless.com/Articles/Index.cfm?ArticleID=27095 (18 Dec. 2002).

[11] Pulsewan.com. "What is PPP?" 3 Jan. 2003. URL: http://www.pulsewan.com/data101/ppp_basics.htm (18 Dec. 2002).

[12] Pulsewan.com. "What is WLAN?" The Wireless Networking Industry's Information Source. 2 Dec. 2002. URL: http://www.pulsewan.com/data101/wireless_lan_basics.htm (7 Oct. 2002).

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

[13] Snyder, Joel. "What is 802.1x?" 9 Dec. 2002. URL:http://www.nwfusion.com/research/2002/0506whatisit.html (2 Dec. 2002).

[14] Swisscom.com. "Swisscom Mobile to launch Public Wireless LAN on 2 December 2002." 2 Jan. 2003. URL: http://www.swisscom.com/mr/content/media/20020924_EN.html (9 Dec. 2002).

[15] The Internet Engineering Task Force. "PPP Extensible Authentication Protocol (EAP)." 9 Dec. 2002. URL: http://ietf.org/rfc/rfc2284.txt (18 Dec. 2002).

[16] Walker, Jesse "802.11 Security Series Part I: The Wired Equivalent Privacy (WEP)." 13 Dec. 2002. URL: http://cedar.intel.com/media/pdf/security/wired.pdf (3 Dec. 2002).

[17] Walker, Jesse. "802.11 Security Series Part II: The Temporal Key Integrity Protocol." 13 Dec. 2002. URL: http://cedar.intel.com/media/pdf/security/80211_part2.pdf (3 Dec. 2002).

[18] Working Group Areas, IEEE. "IEEE 802.1x Overview. Port Based Network Access Control." 9 Dec. 2002. URL:http://grouper.ieee.org/groups/802/1/mirror/8021/docs2000/P8021XOverview.PDF (2 Dec. 2002).

© SANS Institute 2003, Author retains full rights.

© SANS Institute 2003, As part of the Information Security Reading Room. Author retains full rights.

Last Updated: June 20th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Melbourne 2013	**Melbourne, AU**	**Sep 02, 2013 - Sep 07, 2013**	**Live Event**
SANS Capital City 2013	**Washington, DCUS**	**Sep 03, 2013 - Sep 08, 2013**	**Live Event**
Network Security 2013	**Las Vegas, NVUS**	**Sep 14, 2013 - Sep 23, 2013**	**Live Event**
SANS Canberra 2013	**OnlineAU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**