Security Model for IEEE 802.11 Wireless Lan using WPA

Madhu S Nair[1]

Abstract

The increasing reliance on wireless networks for information exchange makes it critical to maintain reliable and secure communications. Much attention has been focused recently on security aspects of Wi-Fi (IEEE 802.11) wireless LAN systems. The paper discusses about two main wireless security protocols – WEP and WPA, used for secure transmission of data over wireless networks. These protocols strongly increase the level of data protection and access control for existing and future wireless LAN systems. The above-mentioned protocols will assure that only authorized network users can access the network. Wireless LANs must be secured to ensure protection of privacy and data integrity. The paper covers the native security issues in IEEE 802.11, and how WEP and WPA can be utilized to overcome the security problems.

Keywords: WEP, WPA, WLAN, Wireless, Security, Privacy, Protection, Encryption.

1. Introduction

Wireless communications provide potential security issues, as an intruder does not need physical access to the traditional wired network to gain access to data. 802.11 Wireless LAN standard incorporates four mechanisms to provide secure access to wireless LAN. The mechanisms are Service Set Identifier (SSID), Media Access Control (MAC) address filtering, Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA).

The SSID segments the wireless LAN into multiple networks, each of which has its own identifier. To access one of the multiple networks within the wireless LAN, the client and access point devices need to be configured with appropriate SSID. An attacker, so additional security measures are needed, can compromise the SSID identifiers.

MAC address filtering increases security by requiring each wireless access point to be configured with MAC addresses of authorized client devices. Only client devices with listed MAC addresses can connect through that access point. The weakness of this approach is that an attacker can intercept the MAC address by sniffing and then configure the attacker's wireless card on a client device with that MAC address to gain access to the network. Strong encryption algorithms can provide effective protection against sniffing [4].

Wired Equivalent Privacy (WEP) was originally designed to provide encryption and authentication as part of the 802.11 standard. It employs an encryption algorithm, which utilizes a key. With WEP, wireless clients and access points are manually configured with same key, which can be 40 or 128 bits in length. Publicly available tools are available that are designed to enable the recovery of encryption keys. It is possible for an attacker to sniff network transmissions and then use these tools to determine WEP encryption keys [1].

[1] Lecturer, Rajagiri School of Computer Science, Kalamassery, Kochi - 683 104, Kerala.

E-mail : [1]madhu_s_nair2001@yahoo.com,
madhu@rajagiri.edu

The Wi-Fi alliance is developing its own standard known as Wi-Fi Protected Access (WPA). WPA was developed to eliminate the vulnerabilities of WEP. WPA is based on the 802.11i draft and will work on existing access points and client cards. 802.11i standard was designed to improve the security of WLANs. The standard is based around 802.1x port based authentication for both users and devices. The standard includes WPA and Robust Security Network (RSN).

WPA uses Temporal Key Integrity Protocol (TKIP) as the protocol and algorithm to improve security issues of keys used with WEP. It changes the way the keys are derived and rotates keys more often for security. It also adds a message-integrity-check function to prevent packet forgeries. RSN uses dynamic negotiation of authentication and encryption algorithms between access points and mobile devices. The authentication schemes proposed in the standard are based on 802.1X and Extensible Authentication Protocol (EAP). The encryption algorithm is Advanced Encryption Standard (AES) [7].

2. Security in Wireless Networks

In wireless networks the threat to security of information flow is the most common. Unlike wired networks that have some degree of physical security, physical security of the wireless networks is impossible and therefore security attacks on information flow are the most widespread. Information security protocols must counter these attacks under the assumption that hardware and software compromises may occur. Most security protocols and architectures designed for wired networks may not be effective in wireless networks [10].

Currently most wireless networks rely on the inherent technical complexity as a principle means of security. Only confidentiality and authentication are given importance in current wireless networks. The key sizes used in current wireless systems are not sufficiently large enough for good security. In IEEE 802.11 WLANs a 40-bit key is used in encryption algorithm. In most cases the size of identification parameter and the algorithms employing it provide loopholes and vulnerability in the protocol. Security issues outside of confidentiality and identification are not often addressed in current wireless networks [5].

The major drawback of current approaches is that they do not consider security issues related to location, mobility and radio resource management procedures. The Internet Engineering Task Force (IETF) is now investigating authentication, authorization and accounting (AAA) procedures in the context of mobile IP. In WLANs the point of access (AP) is small and inexpensive, thus WLAN APs must be authenticated. Finally, wireless communication devices are expected to be mobile and should thus consume as little power as possible while performing computations for encrypting or decrypting data [12].

3. Wired Equivalent Privacy (WEP)

WLANs are vulnerable in various ways, and all the vulnerabilities can be classified into two types:

- Unauthorized Access Threats
- Denial of Authorized Access

The first involves threats from hackers and viruses, in an attempt to get into the network and access the data. The second type is more or less like a Denial of Service (DoS) attack, where some other device may affect the functionality of the network, either intentionally or unintentionally [3].

Wired Equivalent Privacy (WEP) is an encryption standard for 802.11b networks. It was introduced a long ago, and even though it was found to contain severe security flaws, continues to be in use today by somewhat outdated equipment. The figure: -1 shows a point to multipoint mode connection with secured connection.

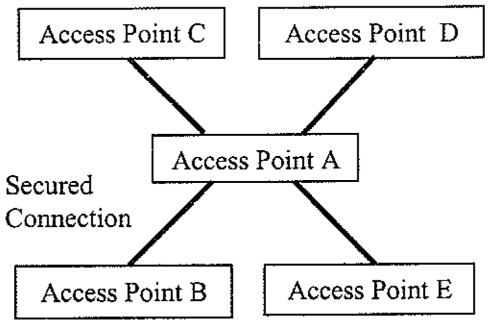

Fig 1. Point to Multipoint Mode

The secured connection between the Wireless-enabled device and the Access Point can be implemented using WEP protocol. It is shown in figure:-2.

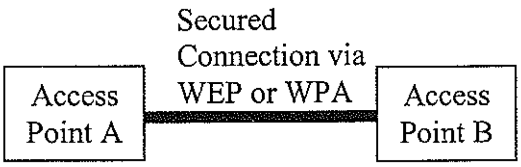

Fig 2. Wireless network using WEP

WEP is a form of encryption, which provides privacy comparable to that of a traditional wired network. If the wireless network has information that should be secure then WEP should be used, ensuring the data is protected at traditional wired network levels. This security protocol is available in 40-bit to 512-bit encryption. Most access points and interface providers offer these protocols [11].

WEP security is good enough and uses a common key shared among all of the devices on the network to encrypt wireless data. Unfortunately, WEP is a very weak form of security. Hackers can access tools freely available on the internet like WEPcrack, Aircrack, and Airsnort that can crack a WEP key in as little as fifteen minutes. Once the WEP key is cracked, the network traffic instantly turns into clear text – making it easy for the hacker to treat the network like any open network.

WEP uses the RC4 encryption algorithm, which is known as a stream cipher. A stream cipher operates by expanding a short key into an infinite pseudo-random key stream. The sender XORs the key stream with the plaintext to produce cipher text. The receiver has a copy of the same key, and uses it to generate identical key stream. XORing the key stream with the cipher text yields the original plaintext [8].

A high percentage of wireless networks have WEP disabled because of the administrative overhead of maintaining a shared WEP key.

WEP has the same problem as all systems based upon shared keys: any secret held by more than one person soon becomes public knowledge. An example is an employee who leaves a company and the employee still knows the shared WEP key and could sit outside the company sniffing network traffic or even attacking the internal network. The initialization vector that seeds the WEP algorithm is sent in the clear and the WEP checksum is linear and predictable. The static nature of the shared secret keys emphasizes this problem. 802.11 don't provide any functions that support the exchange of keys among stations. As a result, system administrators and users generally use the same keys for weeks, months, and even years. This gives mischievous culprits plenty of time to monitor and hack into WEP-enabled network.

WEP encryption standard only encrypts data packets, and not any of the management packets. Since the SSID (Service Set Identifiers) is sent out in these management packets, namely the beacon and probe management packets, it is not encrypted even if WEP is turned on. The SSID goes over the air in clear text, making it easy for an intruder to get hold of. It is better off turning SSID broadcasts off, and forcing the clients to do a network search when they boot up [6].

Despite its flaws, WEP provides some margin of security compared with no security at all and remains useful for casual home users. For large enterprise users, WEP native security can be strengthened by deploying it in conjunction with other security technologies such as Virtual Private Networks (VPNs) or 802.1x authentication with dynamic WEP keys. Nevertheless, Wi-Fi users demanded a strong, interoperable, and immediate security enhancement native to Wi-Fi. The result of this demand is Wi-Fi Protected Access (WPA).

4. Wi-Fi Protected Access (WPA)

IEEE is working on a number of security enhancements to the 802.11 standard, collectively known as 802.11i. It accelerated the implementation of robust wireless LAN security solutions by multiple vendors. The subset of the 802.11i draft standard is called Wi-Fi Protected Access (WPA) and is forward compatible with future 802.11i standard. It provides WLAN users with data protection while helping to ensure that only authorized users gain access to the network. WPA is designed to address all known WEP vulnerabilities, and can provide effective protection against both non-targeted and targeted attacks. WPA implementation will make it possible for enterprises to protect their campus WLAN with scalability, without deploying Virtual Private Network (VPN) or firewall technology.

WPA had several design goals, that is, be a strong, interoperable, security replacement for WEP, be software upgradeable to existing Wi-Fi certified products, be applicable for both home and large enterprise users, and be available immediately. To meet these goals, two primary security enhancements have been made. WPA was constructed to provide an improved data encryption, which was weak in WEP, and to provide user authentication, which was largely missing in WEP. The first one, to improve data encryption, Wi-Fi Protected Access utilizes its Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a per-packet key mixing function, a Message Integrity Check (MIC), an extended Initialization Vector (IV) with sequencing rules, and a re-keying mechanism. TKIP, through these enhancements, addresses all WEP's known vulnerabilities. The second one, WPA provides an Enterprise-Level User Authentication via 802.1x and Extensible Authentication Protocol (EAP). WEP has almost no user authentication mechanism. To strengthen user authentication, WPA implements 802.1x and EAP. These implementations provide a framework for strong user authentication. The framework utilizes a central authentication server, such as Remote Authentication Dial-In User Service (RADIUS), to authenticate each user on the network before they join. It also employs mutual authentication so that wireless user doesn't accidentally join a dangerous network that might steal its network credentials. The figure: -3 shows a wireless network that uses 802.1x security.

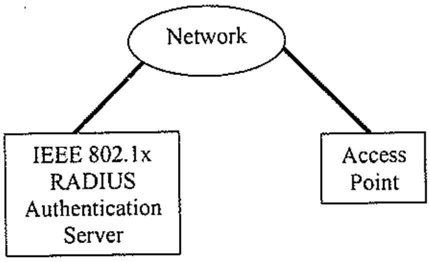

Fig: 3 Wireless Network using 802.1x

WPA will be forward compatible with IEEE 802.11i security specification currently under development by the IEEE. The main pieces of the 802.11i draft that not included in WPA are secure Independent Basic Service Set (IBSS), secure fast handoff, secure de-authentication and disassociation, as well as enhanced encryption protocols such as Advanced Encryption Standard -

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES – CCMP). These protocols will require hardware upgrades to implement. The latest version of WPA, named WPA-2, offers forward compatibility with WPA. WPA-2 provides final 802.11i standard and uses new AES cipher, but will require hardware upgrade.

WPA effectively addresses the WLAN security requirements for the enterprise and provides a strong encryption and authentication solution. WPA should be used in conjunction with RADIUS authentication server to provide centralized access control and management. In a home or Small Office/Home Office (SOHO) environment, where there are no central authentication servers, WPA runs in a special home mode. This mode called Pre-Shared Key (PSK) allows the use of manually entered keys and is designed to be easy to set up for the home user [2].

The intrinsic encryption and authentication schemes defined in WPA may also prove useful for Wireless Internet Service Providers (WISPs) offering Wi-Fi public access in hot spots where secure transmission and authentication is particularly important to users unknown to each other. The authentication capability defined in the specification enables a secure access control mechanism for the service providers and for mobile users not utilizing VPN connections [9].

In a large network with many clients, some access points may operate in a mixed mode, which supports both clients running WPA and clients running original WEP security. While useful for transition, the net effect of supporting both types of client devices is that security will operate at the less secure level (WEP), common to all devices. Organizations will benefit by accelerating the move to WPA for all Wi-Fi clients and access points.

5. Security Model

The proposed model assumes that no node trusts any other node, whether it is internal or external. Each node has to implement a Firewall application with encryption/decryption facility, to protect the threats from illegal intrusion. The model also uses a centralized access control and management through RADIUS Authentication Server.

Access points are connected to the RADIUS server through secured WPA connection. In this model, double security is provided using Firewall and WPA. The architecture of the model is given in the fig: 4.

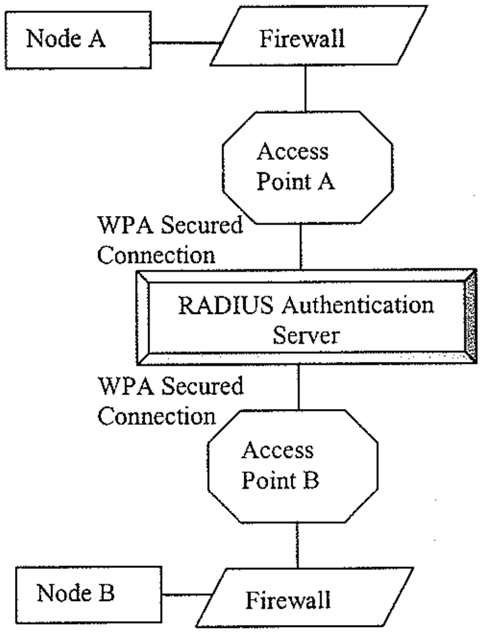

Fig: 4 Security Model Architecture

Two more security enhancements are added to the model. First one; the RADIUS Authentication Server can use a three-way handshake method, for allowing a node to join the network. Using this three-way handshake approach, an added security in the form of confirmation can be obtained.

Second one; a dynamic key exchange mechanism between the nodes is incorporated into the model. Each time a transmission is initiated between two nodes, they

Despite its flaws, WEP provides some margin of security compared with no security at all and remains useful for casual home users. For large enterprise users, WEP native security can be strengthened by deploying it in conjunction with other security technologies such as Virtual Private Networks (VPNs) or 802.1x authentication with dynamic WEP keys. Nevertheless, Wi-Fi users demanded a strong, interoperable, and immediate security enhancement native to Wi-Fi. The result of this demand is Wi-Fi Protected Access (WPA).

4. Wi-Fi Protected Access (WPA)

IEEE is working on a number of security enhancements to the 802.11 standard, collectively known as 802.11i. It accelerated the implementation of robust wireless LAN security solutions by multiple vendors. The subset of the 802.11i draft standard is called Wi-Fi Protected Access (WPA) and is forward compatible with future 802.11i standard. It provides WLAN users with data protection while helping to ensure that only authorized users gain access to the network. WPA is designed to address all known WEP vulnerabilities, and can provide effective protection against both non-targeted and targeted attacks. WPA implementation will make it possible for enterprises to protect their campus WLAN with scalability, without deploying Virtual Private Network (VPN) or firewall technology.

WPA had several design goals, that is, be a strong, interoperable, security replacement for WEP, be software upgradeable to existing Wi-Fi certified products, be applicable for both home and large enterprise users, and be available immediately. To meet these goals, two primary security enhancements have been made. WPA was constructed to provide an improved data encryption, which was weak in WEP, and to provide user authentication, which was largely missing in WEP. The first one, to improve data encryption, Wi-Fi Protected Access utilizes its Temporal Key Integrity Protocol (TKIP). TKIP provides important data encryption enhancements including a per-packet key mixing function, a Message Integrity Check (MIC), an extended Initialization Vector (IV) with sequencing rules, and a re-keying mechanism. TKIP, through these enhancements, addresses all WEP's known vulnerabilities. The second one, WPA provides an Enterprise-Level User Authentication via 802.1x and Extensible Authentication Protocol (EAP). WEP has almost no user authentication mechanism. To strengthen user authentication, WPA implements 802.1x and EAP. These implementations provide a framework for strong user authentication. The framework utilizes a central authentication server, such as Remote Authentication Dial-In User Service (RADIUS), to authenticate each user on the network before they join. It also employs mutual authentication so that wireless user doesn't accidentally join a dangerous network that might steal its network credentials. The figure: -3 shows a wireless network that uses 802.1x security.

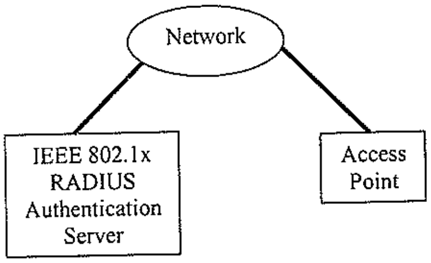

Fig: 3 Wireless Network using 802.1x

WPA will be forward compatible with IEEE 802.11i security specification currently under development by the IEEE. The main pieces of the 802.11i draft that not included in WPA are secure Independent Basic Service Set (IBSS), secure fast handoff, secure de-authentication and disassociation, as well as enhanced encryption protocols such as Advanced Encryption Standard -

Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (AES – CCMP). These protocols will require hardware upgrades to implement. The latest version of WPA, named WPA-2, offers forward compatibility with WPA. WPA-2 provides final 802.11i standard and uses new AES cipher, but will require hardware upgrade.

WPA effectively addresses the WLAN security requirements for the enterprise and provides a strong encryption and authentication solution. WPA should be used in conjunction with RADIUS authentication server to provide centralized access control and management. In a home or Small Office/Home Office (SOHO) environment, where there are no central authentication servers, WPA runs in a special home mode. This mode called Pre-Shared Key (PSK) allows the use of manually entered keys and is designed to be easy to set up for the home user [2].

The intrinsic encryption and authentication schemes defined in WPA may also prove useful for Wireless Internet Service Providers (WISPs) offering Wi-Fi public access in hot spots where secure transmission and authentication is particularly important to users unknown to each other. The authentication capability defined in the specification enables a secure access control mechanism for the service providers and for mobile users not utilizing VPN connections [9].

In a large network with many clients, some access points may operate in a mixed mode, which supports both clients running WPA and clients running original WEP security. While useful for transition, the net effect of supporting both types of client devices is that security will operate at the less secure level (WEP), common to all devices. Organizations will benefit by accelerating the move to WPA for all Wi-Fi clients and access points.

5. Security Model

The proposed model assumes that no node trusts any other node, whether it is internal or external. Each node has to implement a Firewall application with encryption/ decryption facility, to protect the threats from illegal intrusion. The model also uses a centralized access control and management through RADIUS Authentication Server.

Access points are connected to the RADIUS server through secured WPA connection. In this model, double security is provided using Firewall and WPA. The architecture of the model is given in the fig: 4.

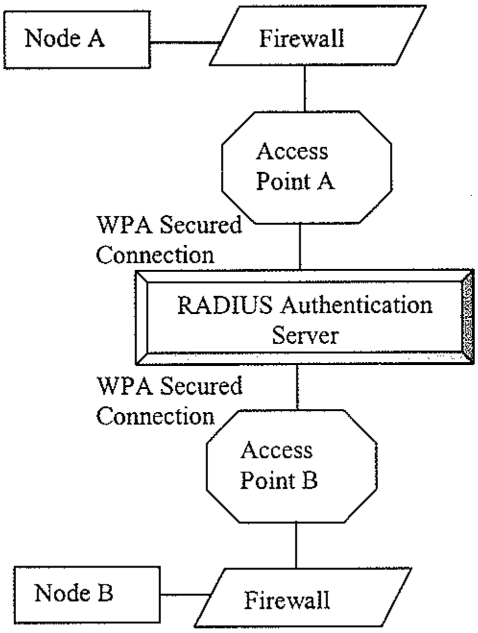

Fig: 4 Security Model Architecture

Two more security enhancements are added to the model. First one; the RADIUS Authentication Server can use a three-way handshake method, for allowing a node to join the network. Using this three-way handshake approach, an added security in the form of confirmation can be obtained.

Second one; a dynamic key exchange mechanism between the nodes is incorporated into the model. Each time a transmission is initiated between two nodes, they exchange the keys to be used for next transmission. For initial transmission, a default key can be used which will be decided by the RADIUS Authentication Server. By dynamically changing the keys to be used for transmission, protection from outside attacks can be achieved. The mechanism can be implemented in two ways: Centralized or Decentralized. In Centralized dynamic key exchange, RADIUS Authentication server will decide the dynamic keys to be used between the nodes, whereas in Decentralized scheme, the individual nodes will decide the keys to be used for data transmission.

The only drawback of this model is that data transmission will take time, as it has to pass through two security levels. Since the wireless medium is not secured compared to physical medium, the model has given more importance to security than time. The time consumption problem can be solved to a certain extent by using fast processors and high-speed wireless data transmission devices.

6. Conclusion

The greatest threat to the security of an enterprise LAN probably results from the failure to implement the effective security solutions that are currently available. While 802.11 WLANs that only utilize WEP have significant security vulnerabilities. VPN technology provides additional protection for mission-critical data, and it can be scaled to meet the needs of large networks. The IEEE 802.1x standard is a port-based authentication framework with dynamic distribution of session keys for WEP encryption. The availability of these solutions makes it possible for enterprises to deploy WLANs with security. The emergence of WPA-enabled devices provides enterprises with a clear migration path from 802.11 with WEP to 802.1x to WPA with TKIP, and ultimately to 802.11i security solutions with the robust encryption of AES.

7. References

[1] "LAN MAN Standards of the IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification, IEEE Standard 802.11, 1997 Edition", 1997.

[2] Dirk Balfanz, Glenn Durfee, Rebecca E. Grinter, D.K. Smetters, Paul Stewart, "Network-in-a-Box: How to Set Up a Secure Wireless Network in Under a Minute", Palo Alto Research Center, 2004

[3] P. Krishnamurthy and J. Kabara, "Security architecture for wireless residential networks", *Proc. VTC'2000,* Boston, MA, September 2000.

[4] W. Stallings, "*Cryptography & Network Security: Principles & Practice, 2nd Ed.*", Prentice Hall, Inc., Upper Saddle River, NJ, July 15, 1998.

[5] E.J. Byres and G. Gillespie; "Is Wireless Ethernet Safe to Use?" , *Sensors Magazine*, Advanstar Communications Inc, Cleveland, July 2002,

[6] Walker, Jesse, "Unsafe at any Key Size: an analysis of the WEP encapsulation, November 2000 "

[7] *Jim Geier*, "WPA plugs holes in WEP", *Network World*, 2003.

[8] Fluhrer, Mantin, Shamir,. Weaknesses in the Key Scheduling Algorithm of RC4., August 2001.

[9] C. Ellison and B. Schneier, .Ten Risks of PKI: What You're Not Being Told About Public Key Infrastructure, http://www.counterpane.com /pki-risks.html.

[10]Jim Geier, "WPA Security Enhancements", Wi-Fi Planet, 2003.

[11]http://www.wifialliance.org/opensection / protected_access.asp.

[12]Joseph Kabara, Prashant Krishnamurthy, David Tipper, "Information Assurance in Wireless Networks", University of Pittsburgh CRDF program, Dept. of Information Science and Telecommunications.

Author's Biography :

Madhu S Nair Currently working as Lecturer in Computer Science at Rajagiri School of Computer Science, an academic unit of Rajagiri College of Social Sciences. He is a First Rank holder in both BCA (Bachelor of Computer Applications) and MCA (Master of Computer Applications). He has two years experience in the academic field. He also holds a Post Graduate Diploma in Client Server Computing (PGDCSC) from Amrita Institute of Technology (AICT). He has published an article in a reputed International Journal. He also provides consultancy to various organizations like CUSAT and CSI.