Wireless Networking Application and Security Architecture in A Campus Wide Local Area Network

Syed Shahzad Ali
MS(EE) Wichita State University, Wichita, KS USA
1(316) 618 8111
ssali@wichita.edu

Muhammad Aamir Usmani
Systems Manager Ablah Library, Wichita State University, Wichita, KS USA
1(316) 978 5131
muhammad.usmani@wichita.edu

Muhammad Saqib Ilyas
MS(EE) Wichita State University, Wichita, KS USA
1(316) 618 8111
msaqib@ieee.org

Abstract

WLANs (Wireless LANs) are a cost-effective solution for impossible or hard-to-wire locations. WLANs are gaining popularity because they are easy to deploy and provide ubiquitous access to enterprise resources from anywhere in the campus. However, Enterprises and Campuses must become fully aware of the security and management implications of adding wireless technologies to their network. Organizations must tightly integrate wireless LANs with wired LANs. Network managers are reluctant or unwilling to deploy wireless LANs unless those LANs provide the type of security, manageability, and scalability offered by wired LANs. Since wireless LANs broadcast data over the air using radio waves, virtually any wireless LAN client in the area served by the data transmitter can access that data. It is impossible to direct a wireless LAN transmission to only one, intended recipient. So data privacy and security becomes a real concern. This article explains how a campus-wide WLAN solution can have tight security by providing dynamic, per-user, per-session WEP, and by deploying other security features like "Mutual Authentication" via RADIUS servers and MAC Address-based Access Filtering.

Key Words

Wireless, Security, WEP, IEEE 802.11, RADIUS Server, WLAN, EAP

1. Introduction

Local Area Networks (LANs) are the essential entity in any Institute or Organization. And in today's world wireless LANs are becoming necessary. But Wireless LANs are security prone. The main security issue with wireless networks is that they radiate data over an area that may exceed the limits of the area the organization physically controls. For example, 802.11b radio waves at 2.4GHz easily penetrate building walls and are receivable from little far distances and someone can passively retrieve sensitive information by using the same wireless Network Interface Card (NIC) from a distance without being noticed by network security personnel.

This problem also exists with wired LAN networks, but to a lesser degree. Current flow through the wires emits electromagnetic waves that someone could receive by using sensitive listening equipment. However, a person would have to be much closer to the cable to receive the signal. Most LAN adapters offer a "promiscuous mode" that enable sniffing software to capture every packet being transmitted through LAN segment.

Measures taken to ensure the integrity and security of data in the wired LAN environment are also applicable to the wireless LAN's as well. Wireless LAN's, such as IEEE 802.11b include an additional set of security elements, namely WEP (Wired Equivalent Privacy).

Security encompasses two areas: access control and privacy. Access control ensures that sensitive data can be accessed only by authorized users. Privacy ensures that transmitted data can be received and understood only by the intended audience.

However, IEEE 802.11b standard has security weaknesses in terms of Wired Equivalent Privacy (WEP) standard on which most wireless LAN solutions are based now. This article explains how a campus wide WLAN (Wireless Local Area Network) solution can have tight security by providing dynamic, per-user, per-

session WEP that reduces many of the concerns regarding 802.11 WEP encryption and by deploying other security features like "Mutual Authentication" via RADIUS servers and MAC Address-based Access Filtering.

2. WEP

The acronym WEP stands for Wired Equivalent Privacy. WEP is a part of the original IEEE 802.11 [1] standard. From the beginning, the goal of WEP has been to provide at least an equivalent level of privacy, as is present in the wired LAN. Traditional wired LANs such as IEEE 802.3 (Ethernet) are protected by the physical security mechanism within the facility (such as controlled access to the wiring or building) and hence IEEE wired LAN standards did not incorporate encryption. Wireless LAN cannot be constrained within the physical boundaries so the WEP encryption is introduced as part of the IEEE 802.11 standard itself. This is done to make sure that wireless LANs could become as secure as a wired LAN.

WEP should be used as the first line of defense to discourage the casual intruders. But in the Campus-Wide LAN the value of data justifies the use of more advanced and sophisticated methods of Wireless transmission privacy and security. According to the recommendation of Wireless Ethernet Compatibility Alliance (WECA) for users in small organizations, home users or where the value of data is not a matter of much importance, the WEP key must be turned on. WEP key is normally 40-bit long but some vendors are also supporting 128-bit WEP key algorithm [2], which is the most recommended WEP key encryption. WEP key must be difficult to guess and it should be changed on a weekly or monthly basis. For a campus-wide LAN where hundreds of wireless users are present and tens of access points (AP) are being deployed it is relatively difficult to adopt the policy to change WEP key on weekly basis. Use of a session-based WEP key is encouraged, provided the vendor supports it.

WEP relies on a secret key that is shared between a mobile station (eg. a laptop with a wireless ethernet card) and an access point (i.e., a base station). The secret key is used to encrypt packets before they are transmitted, and an integrity check is used to ensure that packets are not modified in transit.

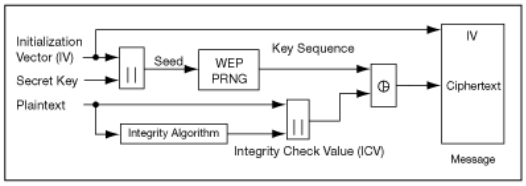

Figure 1. WEP Encryption

The latest Wired Equivalent Privacy (WEP) vulnerability [3] has increased the job of network managers to patch their flawed wireless systems and to think twice before adding new wireless software and features to their existing wireless network. The Gartner Group estimates that 30% of enterprises will have security breaches through insecure wireless networks in the next year [4]. Protecting 802.11 networks is difficult because users can add new wireless devices to the network dynamically without the security administrator knowing. Since wireless devices are usually shipped with WEP encryption and Shared Key Authentication turned off, a user could easily open a door that unleashes attacks on the network.

To help resolve these problems, network managers should install software and services that can perform Security Assessment, which could give early warning of security risks in networks. The assessment should identify unprotected access points, detect network design and implementation flaws and spot hardware vulnerabilities.

2.1 Inherent limitations of WEP

WEP has its inherent limitations. The extent of vulnerability depends on whether static or dynamic WEP is used. Many WLAN deployments use static WEP keys that significantly compromise security, as many users in a given WLAN share the same key. The Cisco Aironet wireless security solution augments 802.11b WEP by creating a per-user, per-session, dynamic WEP key tied to the network logon, thereby addressing the limitations of static WEP keys while providing a deployment that is hassle-free for administrators [5].

3. RADIUS Based Access Control

For large organization where data privacy is a great concern and value of data justifies strong

protection, network administrators should setup extended security measures. Some examples of these methods are RADIUS (Remote Authentication Dial-In User Service) [6] or Kerberose-based access control, end-to-end encryption, password protection, user authentication, Virtual Private Network (VPN), Secure Socket Layer (SSL) and firewalls. RADIUS has been specified as the technology to secure wireless LANs under the set of IEEE standards known as 802.1x. RADIUS servers add intelligence to the LAN-connected wireless receiver, called an access point. The standard calls for the access point are forwarded to a RADIUS server, which are checked in its database of authorized users. Wireless clients contact the access point, which contacts the RADIUS server located on the LAN to make sure the machine with that MAC (media access control) address is authorized to establish a link to the LAN. The server can accept, reject or further challenge the wireless device. If it accepts, the RADIUS server sends data to the access point so it can configure a secure connection with the wireless client. This data from the RADIUS server can include such things as security keys, assigning an IP address to the wireless device or establishing a time limit on the session.

Under the standard, the access point and RADIUS server use extensible authorization protocol (EAP) to communicate. EAP is a point-to-point protocol designed to support multiple authentication methods.

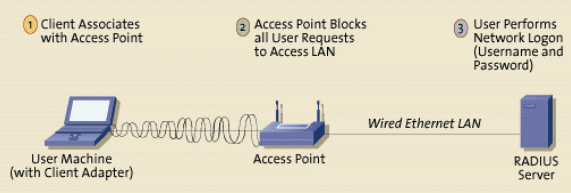

Figure 2. Authentication via RADIUS server

4. EAP

The Extensible Authentication Protocol (EAP) is a PPP extension that provides support for additional authentication methods within PPP [7]. The EAP part comes from the ubiquitous Point-to-Point Protocol (PPP), which activates the modems of most of today's remote users. An IETF standard, PPP is typically called on to establish peer-to-peer links. A PPP option also allows for user authentication via either Password Authentication Protocol (PAP) or Challenge Handshake Authentication Protocol (CHAP), either of which consults with a company's central RADIUS server to validate employee passwords. One of the key features of PPP is its extensibility, and one of PPP's little-known extensions is Extensible Authentication Protocol (EAP). But where PPP offers only simple peer-peer authentication using PAP or CHAP, EAP makes it possible to use a wider range of authentication protocols.

Through the use of EAP, support for a number of authentication schemes may be added, including smart cards, Kerberos, Public Key, One Time Passwords, and others. Cisco uses a variant of EAP called lightweight EAP (LEAP).

With the Extensible Authentication Protocol (EAP), an arbitrary authentication mechanism validates a remote access connection. The exact authentication scheme to be used is negotiated by the remote access client and the authenticator (either the remote access server or Internet Authentication Service, also known as IAS server). You can use EAP to support authentication schemes such as Generic Token Card, MD5-Challenge, Transport Level Security (TLS) for smart card support, and S/Key as well as any future authentication technologies.

LEAP allows for an open-ended conversation between the remote access client and the authenticator. The conversation consists of authenticator requests for authentication information and the responses by the remote access client. For example, when EAP is used with security token cards, the authenticator can separately query the remote access client for a name, PIN, and card token value. As each query is asked and answered, the remote access client passes through another level of authentication. When all questions have been answered satisfactorily, the remote access client is authenticated.

For network managers, authenticating remote access users is a simple process. The user dials in to the enterprise, the call is diverted to a RADIUS server, the server fires off a password challenge and if it receives the correct response, it lets the user into the LAN. But for users already inside the firewall - those working from their desktop PCs - few authentication methods exist. However, a proposal is before the IEEE that would extend the benefits of remote authentication to internal LAN users. And because it makes use of existing standard

technologies, the new Extensible Authentication Protocol Over Ethernet (EAPOE) specification promises to do the job without adding new client software to typical desktop PCs.

5. Other Methods

The default SSID (Service Set Identifier) that is actually a wireless network name should be changed to some unique name. The SSID-based security is also a means to protect and secure a wireless network, though not a reliable and efficient one. SSID is the part of IEEE 802.11 protocol suite. Apart from these techniques, MAC address based filtering [8] and using a VPN system adds to the list of the methods that could be deployed to have a secure network.

6. On-Campus Secure Wireless Local Area Network Deployment

To securely deploy our campus wide WLAN setup we chose Ablah Library, Wichita State University, Wichita, Kansas, USA. The reason to choose this site is obvious. Patron comes to the library to do research activities. And to provide them calm, quiet and secure environment is the responsibility of the library. Patron checks out laptops from the library and they can use the laptop with seamless roaming within the library premises. Main emphasis was paid on enabling following form of security features:

- SSID-based security
- MAC Address-based Security
- WEP-based security with 128-bit full encryption
- RADIUS-Server-based (UID/password) Security using EAP Protocol

Cisco Systems Inc. [8] wireless Aironet 340 Series 11MBPs PCMCI Wireless LAN Adapter were chosen that were Wi-Fi compatible and work in the 2.4 GHz (ISM) band. For access server, Cisco Aironet 340 Series 11MBPs AP (Access Points) were chosen with Wi-Fi compatibility standard that work in 2.4 GHz (ISM) band. Wireless LAN adapters were installed in state-of-the-art Dell Latitude Intel Pentium III Laptops and Microsoft Windows 2000 Professional is selected as the NOS (Network Operating System). Aironet Wireless LAN adapters come with three different types of software that are useful in deploying secure wireless link. One of the software is Cisco CEM (Client Encryption Manager), that writes WEP key into Adapter's flash. Cisco ACU (Aironet Client Utility) is a useful tool to assign generic parameters of the network configuration.

Cisco Secure ACS (Access Control Server) 2.6 for Windows 2000/NT Servers is a network security software that helps authenticate users by controlling dial-in or wireless access to a network access server (NAS) device, such as an access server, access point (AP) or router. Cisco ACS is being used as RADIUS server here. Wireless users trying to establish a link to the network have to be authenticated first. The username/password combination has to be present in RADIUS server to allow users. The Cisco Aironet security solution has several key features that alleviates potential security hazards and came up with its own version of EAP which is called LEAP (Lightweight EAP). It has several features like mutual authentication, secure session key derivation, dynamic per user, per session WEP keys and user definable WEP session key timeout.

The Cisco LEAP allows for a WEP key timeout that will force re-authentication, resulting in the derivation of a new WEP key for the session. By wisely setting the WEP key timeout, the WLAN session will change at a fast enough rate that will prevent an attacker from sniffing enough packets to derive the key.

7. Conclusion

Securing wireless LAN is becoming critical. With the advent of new technology and widespread standards and vendors in the market it is highly required to have a single wireless LAN standard. New Wireless Solution such as AirPort, BlueTooth and Home RF cover some percentage of the overall wireless market. IEEE 802.11b is the standard that is agreed upon among most of the vendor and more and more companies are joining the alliance. Vendor interoperability could become more crucial when the market grows in the future, and it could discourage WLAN deployment rate. Security risk will remain in the WLAN arena as they are in the wired-LAN environment. But these risks can be reduced if adequate security measures are being followed such as those that are discussed in our paper. On the upfront, enterprises may deploy VLAN and IP-Sec security [9] techniques

to have their Wireless-WAN safe against the potential intruders.

8. Future Work

Recently a new DHCP option had been added into the DHCP protocol that passes WEP key from the DHCP Server to the DHCP Client to configure the WEP key on a client's wireless card [10]. This option will remove the hassle for network administrator to change WEP key on hundreds or thousands of mobile clients. So this work needs to be done as part of our next step.

References

[1] Keith Biesecker, "The Promise of Broadband Wireless", Vol. 2, No. 6; NOVEMBER/DECEMBER 2000, pp. 31-39

[2] L.M.C.S of the IEEE Computer Society. Wireless LAN medium access control (MAC) and physical layer (PHY) specifications. IEEE standards 802.11, 1999 Edition, 1999

[3] Nikita Borisov, Ian Goldberg and David Wagner "Intercepting Mobile Communications: The Insecurity of 802.11", ACM SIGMOBILE Conf 2001

[4] http://www.gartner.com

[5] Gail Meredith, "Securing the Wireless LAN: Cisco plugs holes in the 802.11 standard", Packet Magazine Third Quarter 2001

[6] C. Rigney, S. Willens, A. Rubens, W. Simpson "RFC 2865: Remote Authentication Dial In User Service (RADIUS)", June 2000

[7] L. Blunk, J. Vollbrecht "RFC 2284: PPP Extensible Authentication Protocol (EAP)", March 1998

[8] J. Walker, http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0P802-15_TG3-Overview-of-802-11-Security.ppt", Mar. 2001

[9] http://www.cisco.com

[10] S. Kent, R. Atkinson. "Security Architecture for the Internet Protocol. Internet Request for Comment RFC 2401, Internet Engineering Task Force", Nov. 1998

[11] Narendar Shankar , William Arbaugh , Kan Zhang "Wireless Key Management using DHCP. Internet-Draft, Internet Engineering Task Force", Jul. 2001

About the authors

Syed Shahzad Ali has completed his MS degree in Electrical Engineering from Wichita State University KS, USA. He completed his Bachelor's degree in Computer Systems Engineering from NED University of Engineering & Technology Karachi, Pakistan and then worked in different ISPs (Internet Service Providers) as Network as a Systems Engineer. He has three years of IT industry experience.

Muhammad Aamir Usmani completed his Bachelor's degree from Wichita State University , Wichita, KS, USA and is presently working in Ablah Library at Wichita State University as Systems Manager and he is pursuing his MS degree program in Electrical Engineering.

Muhammad Saqib Ilyas has completed his MS degree in Electrical Engineering from Wichita State University, Wichita, Kansas. He completed his Bachelor's degree from NED University of Engineering & Technology Karachi, Pakistan and then started teaching there as a lecturer.