

Wireless LAN Security

by

Ryan Moore

This paper is being submitted as fulfillment of the requirements for MGT 5387

University of Dallas

Graduate School of Management

Branden Williams

Spring 2005

3/10/2005

Table of Contents

Abstract.....	1
Executive Summary	1
Wireless Networks	2
Wired Equivalent Protocol.....	3
WEP Encryption and Authentication.....	3
Problems with WEP	4
Extensible Authentication Protocols.....	5
Cisco LEAP	5
WPA	6
PEAP and TTLS	6
TinyPEAP	7
Protecting Wireless Networks	8
Policies and Procedures.....	8
Wireless Intrusion Detection Systems	11
Summary.....	11

Abstract

This paper will examine the security problems inherent in Wireless LANs and detail the latest information on how wireless LANs can be secured. Wireless LANs provide a fast, easy and inexpensive method of accessing computer networks. However, unlike wired networks, wireless networks cannot be physically secured.

An attacker only needs to be close enough to receive the radio signals of the wireless network to attempt to gain access. In order for wireless networks to be used for mission critical applications they must be secure. This paper will detail encryption schemes, authentication methods, and technology advances that are available to secure wireless networks.

Executive Summary

Throughout the Evolution of Computing technology, every advance has made computers more accessible and easier to use. From the introduction of a remote terminal connected to a mainframe computer, to Local Area Networks and the creation of Wide Area Networks and finally connecting it all together in the Internet, every advance has given easier access to larger amounts of information. Of course, with each advance comes new security concerns that must be addressed.

Wireless networks are the latest advance in computer networking technology. Computer no longer need to be tied to the network by “the cable.” A PC with a wireless card can access a local wireless network from anywhere in range. Wireless networks are also a large cost savings for enterprises who utilize them. Cabling is a great part of the expense of installing any network, especially if the building was not originally designed to accommodate network cabling. With a few strategically placed Wireless

Access Points, an entire building can be given access to the network with little cabling needed. Unfortunately, wireless networks are inherently insecure. A wired network accommodates a reasonable measure of security. Access to the wires and cables can be physically secured. This is not the case in a wireless network. Anyone with range of a wireless Access Point's radio can attempt to gain access to the network and listen in to the traffic being transmitted. This paper will detail the current risks to wireless networks and ways to mitigate these risks.

Wireless Networks

What is a wireless network? There are many different kinds available today. Cellular phones are one kind of wireless network as are Bluetooth Devices, such as short range wireless headsets. This paper will examine wireless networks defined by the IEEE 802.11 Standards. ¹ The most common in use today are the 802.11b, 802.11g 802.11a standards.

802.11 wireless networks operate in 2 modes, either *ad hoc* or *infrastructure*. In *ad hoc* networking, each client communicates directly with another client that is in range. Much like if a cable was connected directly between 2 PCs. In *infrastructure* mode, each client connects to a centralized networking device known as an Access Point (AP). This would be the equivalent of connecting a PC to a wired network hub or switch. Most wireless networks in use today are *infrastructure* networks. *Ad Hoc* networks are only useful for connecting a few PCs for a short amount of time to exchange data. In an *Infrastructure* network a client looks for available APs to communicate with and learn their Service Set Identifier (SSID.) This is effectively the name of the wireless network. An AP can be set not to broadcast its SSID and in this

case the client must configure its wireless card to look for a specific SSID in order to gain access to the network. Once a client has found an AP, it sends an association request to the AP. The AP then responds to the association request and may require the client to Authenticate to the network in order to use it. Once the client has been associated to the AP it has joined the wireless network and the AP acts as a bridge for the client to the larger network.

Wired Equivalent Protocol

Interception of radio transmissions has been a problem since radios have been used to transmit sensitive information. Encryption of the transmitted data is the most common solution. The 802.11 standard provides an encryption and authentication mechanism for controlling the interception of wireless data called the Wired Equivalent Protocol (WEP.) WEP provides both an encryption scheme and well as an authentication method in order to secure a wireless network. The goal of WEP is to make wireless LAN communication as secure as its wired counterpart.

WEP Encryption and Authentication

WEP encryption uses a symmetric key system. This means that the key that is used to encrypt the data is the same key that is used to decrypt it. If both devices do not have the same key, then the communication fails. Each client must be configured with the WEP key for each network that it will join. The shared “WEP Key” is also used for authenticating the client to the wireless network. A client is configured with the networks WEP key. The AP then sends encrypted data to the client, if the client can decrypt it, then it is allowed access to the network. Most Vendors implement both 40-bit and 104-bit WEP encryption on their devices. (This may also be referred to as 64-bit

and 128-bit encryption.) For a more detailed discussion of WEP encryption and authentication see NIST publication SP800-48 Wireless Network Security.²

Problems with WEP

Potter and Fleck, in their book, 802.11 Security, detail the problems with WEP.³ WEP uses a shared secret key architecture. Every valid user on a WEP network must know the shared key in order to access the network. This implies a level of trust amongst all the users that is not realistic. Anyone on the network can decrypt anyone else's traffic. The shared key may also get passed to someone who should not have access to the network. WEP does provide for a key rotation scheme, but the keys must be pre-defined and all users must still know all of the shared keys in order to access the network. This does little to mitigate the problem.

WEP encryption can be either 40 or 104 bit. 40 bit encryption was included as part of the standard so wireless products could be exported to other countries. 140 bit encryption is considered "too strong" to be exported to some countries. Using brute force methods, a 40 bit key can be decrypted using a modern PC in only a few hours. The WEP standard also introduced a flaw into the RC4 encryption scheme. Normally, adding length to an encryption key makes the time needed to break it increase exponentially. The way RC4 is implemented in WEP; the time needed to break the key is linear. This means it takes only about 2.5 times as long to break a 104 bit WEP key as it does a 40 bit key if sufficient encrypted traffic can be captured. Ossman, in his article, *Wep: Dead Again*, discusses WEP cracking tools and the weaknesses of WEP.⁴ Initially, cracking tools such as *Airsnort* required that millions of packets be captured to decrypt the WEP key. Recently, a new program called *Aircrack* has reduced this

number to only a few hundred thousand. An attacker can easily use one of these tools and a network sniffer to gain access to a WEP secured network. The end result is that WEP is nowhere near “wired equivalence.”

Extensible Authentication Protocols

Wireless equipment vendors quickly realized that WEP was insufficient security. In response, vendors and standards bodies came up with solutions to mitigate the problems inherent in WEP. These protocols are known as Extensible Authentication Protocols (EAP). Unfortunately, some of these have weaknesses of their own.

Cisco LEAP

In response to the weaknesses in WEP, Cisco Systems came up with a proprietary Authentication Protocol known as Lightweight Extensible Authentication Protocol (LEAP).⁵ LEAP is a password based algorithm, which uses a mutual authentication scheme. This requires the user to authenticate the network as well the network authenticating the user. The password is one-way encrypted during the authentication process so it is impossible to “read” the encrypted password using a wireless sniffer. This overcomes many of the problems of WEP based authentication. Unfortunately, LEAP has its own problems. It is possible for an attacker to utilize a “dictionary attack” to discover LEAP passwords. The encrypted password is recorded by the attacker. Software is then utilized to encrypt words from a “dictionary” using the same encryption scheme as LEAP. When a match is found between one of the dictionary words and the encrypted password, the password has been broken.⁶ There is even a tool for this kind of attack known as *asleap*⁷. This kind of attack can be mitigated by the use of strong passwords, which cannot be easily found in a dictionary.

Cisco responded to *as/leap* by releasing a new EAP, called EAP-FAST. It creates an encrypted tunnel between the client and the authentication server in order to securely authenticate wireless users. This is similar to the scheme that other EAPs such as PEAP and TTLS use. Cisco claims its EAP-FAST protocol is easier to use than these other EAPs, in practice however, it is functionally the same.

WPA

Wi-Fi Protected Access or WPA is a subset of the 802.11i standards proposed by the IEEE intended to address the shortcomings of WEP. There are 2 modes of WPA operation, enterprise and consumer. Enterprise mode utilizes a radius server and allows per-user authentication, meaning each user is authenticated with a unique key and shared keys are not used. Consumer mode is simpler and utilizes a pre-shared key for authentication. The consumer mode of the WPA is vulnerable to dictionary attacks in the same way as Cisco LEAP. Unless, a strong pre-shared key is used, an attacker will be able to find the password with a dictionary lookup program. Takehiro Takahashi provides a good summary of both modes of WPA and the weaknesses of consumer mode.⁸ Recently, the Wi-Fi alliance⁹ has released WPA2 which improves on WPA security.

PEAP and TTLS

PEAP stands for the Protected Extensible Authentication Protocol. PEAP was jointly created by Microsoft, RSA Security, and Cisco. It is used for transmitting authentication data, including passwords, securely over 802.11 wireless networks. PEAP employs digital certificates to insure a secure authentication environment. An encrypted tunnel using SSL/TLS is created between the client and an authentication

server. The encrypted tunnel protects the transfer of data from being sent “in the clear” over the wireless link.¹⁰

A competing standard to PEAP is Tunneled Transport Layer Security, or TTLS. TTLS functions in a similar way to PEAP and was created by Funk Software. Both of the protocols have so far proved to be secure, though they require the use of a back-end authentication servers and digital certificates to function. At the current time, PEAP and TTLS are the preferred method for secure authentication of clients to wireless networks. Paul Roberts discusses the competing standards in his article about Asleep, the LEAP cracking tool.¹¹

TinyPEAP

Home wireless users have been left out in the latest wave of improvements to wireless security. PEAP and TTLS both require the use of a Radius Authentication servers and Digital Certificates in order to secure access to the wireless network. Commercial Radius servers are not cheap or easy to use. A viable option for home wireless users is TinyPEAP.¹² TinyPEAP is a very small Radius Server than can be run on minimal hardware. It allows home users the benefits of PEAP authentication protection without the purchase of a full radius server. All the software used by TinyPEAP can be run on the access point itself. TinyPEAP is also relatively easy to configure. The only requirement is that the wireless AP/Router must support Radius Authentication.

Protecting Wireless Networks

Policies and Procedures

The first step to protecting a wireless network is having good wireless security policies backed up by clearly defined procedures. Farshchi¹³ wrote a set of excellent articles for Security Focus, that provides a framework for wireless network Policy development.

The Wireless security policy should be proactive and developed prior to the network itself. By including security as part of the network from the beginning, the network does not have to “catch-up” later when vulnerabilities are exposed. The policy should delegate a person to be the authority on the wireless network. This person is responsible for insuring that the security procedures are followed and with whom ultimate responsibility for the wireless network rests.

A risk assessment should also be performed. Evaluating the risks to the network and how to mitigate them will reveal how security should be implemented on the network. The function of the network should be taken into account when evaluating the risks. A small wireless network used only for web-surfing is not nearly as open to risk as a corporate wireless enterprise network. In some cases, the risk assessment may show that the risks of a wireless network are too great and one should not be implemented.

Wired and wireless networks should be separated. In this way a security breach on one network does not compromise the other. Wireless LANs should always be treated as an “untrusted” network and separated from the main wired network by security devices, such as a firewall.

An authentication standard should be detailed. Wireless networks, are by their nature, open networks, so a strong authentication method is necessary. A Mutual authentication protocol using digital certificates, like PEAP, is a good choice. This insures that the users are authenticated to the network and that the network is authenticated by user. The authentication policy should also detail user and group level access and how this access is managed.

Information transmitted on the network must stay confidential. As noted earlier in this paper, there are many tools for listening-in or sniffing wireless networks. An encryption standard for the network needs to be defined, and all equipment used on the network must conform to this standard. WEP is insufficient as an encryption standard. WEP is easily broken and provides no real security. Advanced encryption methods such as the Advanced Encryption Standard (AES) is a good choice. If it is not possible to implement a full encryption standard, another option is to treat the wireless network as completely untrusted and have users create a Virtual Private Network tunnel, using a VPN client, through the wireless network. The encrypted VPN tunnel would insure that all communications are kept confidential.

The wireless network policy should also contain procedures for insuring the availability of the network. Weather, new structures, radio interference, and many other factors can cause the coverage area of your wireless network to change. Coverage holes and weak areas can crop up in the network almost overnight. One way to insure network availability is to “wardrive” the network. Wardriving is the process of driving around your wireless network coverage area and mapping it out using topology tools. Hackers use wardriving to find unsecured wireless networks to attack, so including

wardriving procedures as part of your policy can also help reveal rouge access points and unsecured areas of the network.

Logging procedures are an important part of a wireless security policy. Logging access to the wireless network allows a network intruder to be tracked when a security incident occurs. The policy should delegate a person to be responsible for maintaining and reviewing network security logs. The logs should be reviewed in a timely manner.

Access point and client security are also important parts of good wireless network security. Access points should always be located in physically secure locations. If an access point is physically accessible, it is relatively easy to reset it to a default mode and gain access to the network. The access point should be configured with a strong login password to prevent an attacker from connecting to it and altering its configuration. Wireless clients need to be secured the same way as wired users. Wireless clients are more likely to come under direct attack than their wired equivalents, so personal firewalls and anti-virus software should always be installed. Ad-Hoc networking should also be disabled on all wireless clients. Ad-Hoc networking does not require authentication and allows many network exploits, such as man-in-the-middle attacks.

All wireless network users should receive some form of security awareness training. Educating users on the risks of wireless networks and what they can do to protect themselves will make the network more secure. A user who is aware of the reasons why ad-hoc networking is disabled and why using it makes the network less secure, is unlikely to re-enable it.

Wireless Intrusion Detection Systems

Good security policies and procedures are the first step to securing a wireless network. One recent advance in technology that can also aid in securing a wireless network is a wireless Intrusion Detection System (IDS). An IDS monitors and analyzes the traffic on the wireless network and looks for abnormal activity. Wireless IDSs work in the same way as their wired equivalents, they look for pre-programmed attack signatures occurring on the network. Wireless Intrusion detection systems can also aid in policy enforcement. They can identify rogue Access points, send an alert if an access point's configuration has changed, and log network activity. One of the most popular Wireless IDSs is *Airdefense*.¹⁴ *Airdefense* functions by using sensors placed near the wireless access points to monitor the traffic on the wireless network. One of the main problems with IDSs such as *Airdefense* is cost. The wireless sensors cost as much or more than the access points.

Summary

Wireless LANs are here to stay. They allow rapid deployment of low cost, high speed networks. Currently, wireless networks are not secure without using advanced technology, such as authentication servers and digital certificates. However, the demand for wireless technology is too great. Wireless vendors will continue pushing the envelope on new ways to secure wireless networks. Wireless products available today are more secure and reliable than products available only one year ago. Soon it may be possible that wireless networks can be as trusted as their wired counterparts.

Selected Bibliography

Bruce Potter and Bob Fleck, *802.11 Security*, (California: O'Reilly and Associates, 2003)

Tom Karygiannis and Les Owens, *Wireless Network Security*, (Washington, DC: National Institute of Standards Special Publication 800-48, 2002;) available from

http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

Jamil Farshchi , *Wireless Network Policy Development*, (California: Security Focus, 2003); available at

<http://www.securityfocus.com/infocus/1732> and <http://www.securityfocus.com/infocus/1735>

¹ *IEEE 802.11*, 1999 Edition , (ISO/IEC 8802-11: 1999); available from <http://standards.ieee.org/getieee802/802.11.html>

² Tom Karygiannis and Les Owens, *Wireless Network Security*, (Washington, DC: National Institute of Standards Special Publication 800-48, 2002 ;) available from http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf

³ Bruce Potter and Bob Fleck, *802.11 Security*, (California: O'Reilly and Associates, 2003), 15-17

⁴ Michael Ossmann, *WEP: Dead Again*, (California: Security Focus, 2004) available at <http://www.securityfocus.com/infocus/1814>

⁵ *A comprehensive review of 802.11 security and the Cisco Wireless Security Suite*, (California, Cisco Systems Incorporated;) available at http://www.cisco.com/en/US/products/hw/wireless/ps430/products_white_paper09186a00800b469f.shtml

⁶ Joshua Wright, *Weaknesses in LEAP Challenge/Response*, Available at <http://home.jwu.edu/jwright/presentations/asleep-defcon.pdf>

⁷ Sourcecode for the Asleep hacking tool available at <http://asleep.sourceforge.net/>

⁸ Takehiro TakaHashi, *WPA passive Dictionary Attack Overview*, Available at http://www.michiganwireless.org/tools/WPA-Cracker/WPA_Passive_Dictionary_Attack_Overview.pdf

⁹ Information on WPA2 can be found at http://www.wi-fi.org/OpenSection/protected_access.asp

¹⁰ Securing wireless LANS with PEAP, (Washington: Microsoft), Available at http://www.microsoft.com/technet/security/topics/cryptographyetc/peap_2.msp

¹¹ Paul Roberts, *Expert Releases Cisco Wireless hacking tool*, (InfoWorld , 2004), available at http://www.infoworld.com/article/04/04/08/HNciscohacking_1.html

¹² Information on TinyPEAP can be found at http://www.tinypeap.com/docs/TinyPEAP_White_Paper.pdf

¹³ Jamil Farshchi , *Wireless Network Policy Development*, (California: Security Focus, 2003); available at <http://www.securityfocus.com/infocus/1732> and <http://www.securityfocus.com/infocus/1735>

¹⁴ Information on Airdefense can be found at <http://www.airdefense.net/products/index.html>