Global Information Assurance Certification Paper

Wireless LANs and 802.1x
Daryl Stargel
GSEC
Version 1.2f
December 12, 2001

1.0 Introduction

As wireless Local Area Networks (LANs) are being deployed and used in increasing numbers, opportunities for an attacker to access and penetrate these networks and their host network, a wired LAN, also increase. Due to the radiation characteristics of the wireless LAN, it presents an attacker with a potential back door into the network. Monitoring, or eavesdropping, and access can be gained outside of the physical security perimeter of the network, be it used by a company or a home. The Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard provides authentication and privacy protective security services. Recently, 802.1x has been approved and addresses port-based network access control.

2.0 Background

2.1 Wireless LANs

A wireless LAN is a flexible and dynamic data communications system that transmits and receives information over the air. It is typically part of a larger network and interfaces to a wired LAN. An access point (AP) bridges or interfaces the wireless stations to the wired LAN. The wireless stations have network interface cards (NIC) that interface the stations to the APs by radio frequency (RF) transmissions. Another wireless LAN configuration consists of a standalone RF network that is made up of only wireless stations. It operates as an independent wireless LAN and is known as an ad-hoc or peer-to-peer network.

2.2 IEEE 802.11

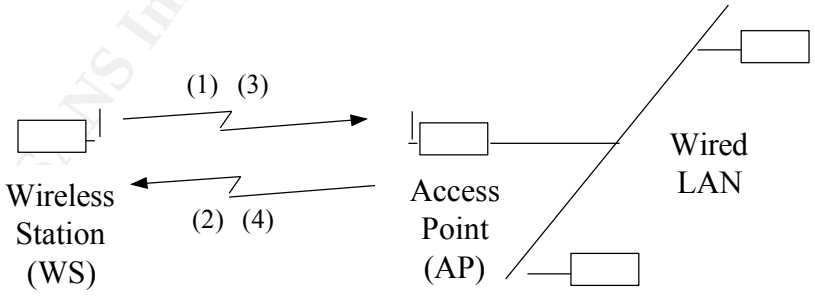
While there are other standards and protocols, such as the European Telecommunications Standards Institute (ETSI) HiperLAN2 [ETS], only the IEEE 802 standards are considered in this paper. Before 1997, there were no standards for wireless LAN products. Each vendor defined and implemented its own proprietary network protocols and signaling waveforms for its line of wireless products. Different vendor products were not interoperable and required the wireless network to operate with only one vendor's products. The IEEE formed a working group to standardize the protocols and signaling for wireless LANs. This working group had the IEEE 802.11 standard accepted in 1997 which operated at 1 Mbps with an optional 2 Mbps data rate. The IEEE 802.11 standard [PAR] defined three different physical implementations, a Media Access Control function, and a Management function. The physical implementations include an infrared (IR) and two RF spread spectrum (SS) implementations at 2.4 GHz. The spread spectrum defined for the wireless LANs are direct sequence (DS) and frequency hopping (HP) schemes. The IEEE 802.11b standard is the most dominant wireless LAN standard used today. Here the data rates have increased to 11 Mbps from the original 1 Mbps. Other IEEE working groups have other standards that have been accepted or are still under development for wireless LANs [IEE]. From the security perspective of interest is the Task Group i which is to enhance

the 802.11 Medium Access Control (MAC) to improve security and authentication mechanisms specifically for wireless LANs. Task Group i is in the development phase. Just recently approved is the IEEE 802.1x standard, Port-Based Network Access Control. 802.1x is intended to apply to all 802 technologies and not just to wireless applications, such as Ethernet and Token Ring.

3.0 Security Issues

802.11 defines authentication and privacy services to provide wireless LANs with the equivalent functionality of a wired LAN. Because of the over-the-air communications media of a wireless LAN, it does not possess the physical connection or the controlled environment of a wired LAN. 802.11 provides link level authentication between wireless stations and APs. End-to-end or user authentication is not provided by 802.11. Authentication services for a wireless LAN is to be equivalent to a wired LAN having a wired connection. Also privacy services for a wireless LAN is to be equivalent to a wire environment.

The 802.11 standard defines two types of authentication, Open Systems and Shared Key. In Open Systems authentication, any wireless station is authenticated to join the network. Actually, Open Systems provides no authentication at all. For Shared Key authentication, wired equivalent privacy (WEP) is to bring the wireless LAN connection up to the equivalent physical security of a wired LAN. Authentication is demonstrated by verifying that symmetrical encryption keys are possessed by the wireless station and the AP, see Figure 1. The AP generates a 128-bit challenge. The wireless station returns the challenge but it is encrypted with a key that both the AP and wireless station are configured with. The AP decrypts the frame and if it matches the challenge originally sent by the AP, the wireless station is considered authenticated. The encrypted challenge also has a CRC to verify the integrity of the wireless stations challenge response. An attacker who captures this exchange sequence now has the plain text, the initialization vector (IV), and the cipher text. The IV is sent unencrypted in the WEP frame and is appended to the encryption key. By changing the IV, the keystream is easily changed [HOD]. The attacker now has enough information to determine the keystream and can now access the network and be authenticated. There are a variety of other attacks that can be mounted against WEP [UCB].



Authentication sequence
(1) from WS to AP, request authentication, frame unencrypted
(2) from AP to WS, with WEP generated challenge text, frame unencrypted
(3) from WS to AP, repeat received challenge text from (2), frame encrypted
(4) from AP to WS, if decrypted challenge text in (3) is identical to transmitted challenge text in (2), successful status sent to WS, if not identical,

unsuccessful status sent to WS, frame encrypted

Figure 1 802.11 Shared Key Authentication

Physical security prevents unauthorized access to a wired LAN. The 802.11 standard provides for encryption of the data to bring the privacy functionality up to the equivalent of a wired LAN. Note that the encryption algorithm is specified to provide privacy up to the level of a wired LAN and no more. The privacy service can be selected for no encryption, or sending data in the clear, or encryption using the RC4 algorithm. WEP authenticates stations trying to access the network and provides confidentiality for wireless data when encryption is selected.

Two other methods are used for access control to an AP; service set identifier (SSID) and MAC address filtering but they are transmitted unencrypted [PHI]. Each AP is programmed with an SSID that is unique for a specific wireless network. For a wireless station to access this network, it must be configured with the correct SSID. To access an AP, the wireless station must send the correct SSID, which is similar to using a password, to access the network. APs transmit a beacon management frame at fixed intervals. This frame can be configured to contain the network name, or SSID and is sent by the AP unencrypted. A wireless station receives this beacon frame to identify the SSID and responds to the AP. Any wireless station that is not configured with the correct SSID will still receive the SSID transmitted by the AP. An attacker could monitor the wireless LAN to obtain the SSID and then configure his wireless station with this SSID. The AP transmitting the SSID compromises any access control provided by this method.

While not defined in the standards, some vendors use AP access control lists based on the Ethernet MAC address of the wireless stations that are part of the wireless LAN. The wireless stations that can access the AP are limited to the MAC addresses configured for the AP. An attacker could eavesdrop on the network data and obtain the MAC addresses, which are sent unencrypted, of valid wireless stations. The attacker could then program his NIC with one of these valid MAC addresses and access the AP [ARB].

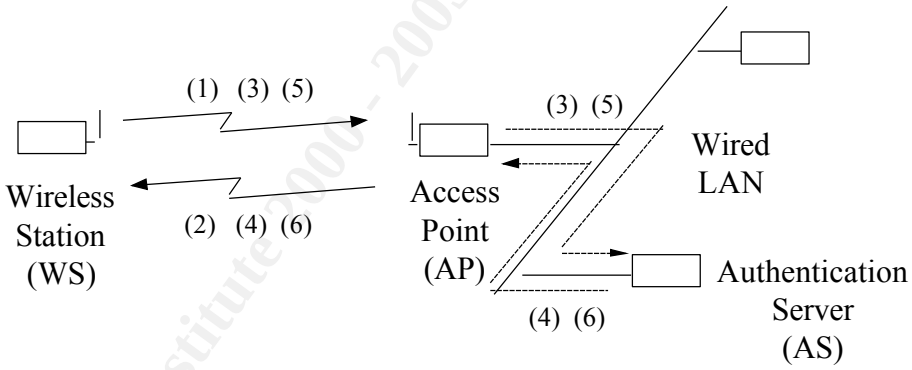
Along with WEP, all three methods can be implemented or in any combination. A network that does not implement any of these three methods would have no access control and all data would be sent in the clear.

4.0 IEEE 802.1x

Time changes, and so have LANs and their applications. LANs are now being used where unauthorized devices can be physically attached or attempt to access networks through existing ports, such as APs. An example would be a corporate LAN that would offer services to other organizations or to the general public. This could be a university or government agency that has a LAN with a public interface. This evolution impacts both wired and wireless LANs. This led to the 802.1x standard [POR], Port-Based Network Access Control, being ratified in June 2001 and is applicable to Ethernet and Token Ring, and wireless LANs. 802.1x provides authentication and authorization of devices attaching to a LAN port, an AP for a wireless LAN, and prevents access when this process fails. For wireless LANs, 802.1x applies to the association of wireless stations to an AP with a supporting authentication server. The authentication server functions can be collocated or included as part of the AP or in a separate enclosure.

4.1 Extensible Authentication Protocol

The 802.1x authentication process uses the Extensible Authentication Protocol (EAP) between the wireless station and the authentication server. EAP is a general protocol and allows different authentication protocols to be selected, such as smart cards, Remote Authentication Dial-In Service (RADIUS), Public Key Encryption and others. Initially, a wireless station requests access to an AP. The AP passes the request to the authentication server that handles the authentication exchange. The AP passes the data between the wireless station and the authentication server. Once the wireless station is authenticated, the authentication server provides an encryption key to the AP. The AP uses this key to encrypt a session key or broadcast key and sends to the wireless station. The ability to transmit a key is an option of the 802.1x to give the network the ability to dynamically manage and generate encryption keys, a capability not present in the 802.11 standards where manual key distribution is used. At this point, the wireless station has access to the network and the transmissions between the wireless station and the AP are encrypted, see Figure 2. At present 802.1x identifies the WEP encryption algorithm, RC4, but allows for other algorithms to be implemented. This will allow expansion to algorithms like the Advanced Encryption Standard (AES). It can be expected that when 802.11i is approved, 802.1x will support the security enhancements in that standard.



Extensible Authentication Protocol sequence
(1) from WS to AP, Start
(2) from AP to WS, Request Identity (AP can initiate authentication by starting at (2)
(3) from WS to AS, Response Identity
(4) from AS to WS, One Time Password (OTP) Challenge (OTP used as example, EAP does not specify authentication protocol)
(5) from WS to AS, Response OTP
(6) from AS to WS, Success (Failure), Port now authorized (not authorized)
(7) Optional, Transmit Key Information (session key can be transmitted from AS or AP to WS)

Figure 2 802.1x EAP Authentication

4.2 Vendors

The following is a partial list of vendors and their products, which are just coming on the market or will be shortly that support 802.1x:

- Microsoft – Windows XP
http://www.microsoft.com/presspass/press/2001/Mar01/03-26XPWirelessPR.asp

- Cisco– Aironet products, Catalyst 5000 switches
http://newsroom.cisco.com/dlls/prod_111201.html

- Bluesocket – WG-1000 gateway
http://www.bluesocket.com/news.html

- Agere – AP-2000 Access Point,
http://www.orinocowireless.com/template.html?section=m58&page=3040&envelope=94

- Enterasys – Matrix Switching Platform and NetSight Management Applications
http://www.enterasys.com/corporate/pr/releases/2001/mar/3-7a.html

- Funk Software – Steel-Belted Radius v3.0
http://www.funk.com/News&Events/wirelessLANbeta_pn.asp

5.0 Security Policies and Practices

If your network includes a wireless LAN or you are planning to augment your existing network with a wireless LAN, your security policies and practices must address the different and unique vulnerabilities of a wireless LAN. You must understand the security issues that are caused by radio transmissions versus a wired network. Also, there are practices that apply to all type networks. For example, equipment can be shipped with default setting that if not changed will create a potential security flaw applies to wired and wireless LAN products.

Consider the physical location from where an attack can occur on a wireless LAN. Due to the radiation characteristics of a wireless LAN, an attacker must have his radio equipment located within a limited radius of the operating wireless LAN. Typically, in an office environment this range is 75 to 150 feet [GRI] but is dependent on the gain of the antenna and the propagation environment. Where a wired LAN connects to the internet, an attacker can try to enter and manipulate the wired LAN from any location where there is access to the internet. This location can be anywhere in the world. In the case of a wireless LAN attack via RF, an attacker, or at least his equipment, must be in the local area. Options that could be considered are shielding to reduce the area of coverage or using IR for its directional characteristics. Of course, your application and environment must be considered. If the wireless stations are constantly changing location and are mobile, then shielding and IR would not be practical to implement.

Consider the case where a hospital was planning to upgrade its wireless LAN. After evaluating the access procedures and security measures, some data was considered too sensitive to be transmitted over the wireless LAN. An example would be where doctors writing orders are limited to the wired LAN and not allowed to be send this data over the wireless LAN [DRU]. Other sensitive data could only be accessed from the wireless LAN as read-only.

6.0 Summary

There is no perfectly secure network, be it a wired or a wireless network. Do not count on technology alone to solve all your network security problems. A security plan must address the network architecture, what is being protected and to what degree it is to be protected. You must keep up with the latest and evolving threats, products, technology and standards. If wireless LANs are part of your network architecture but is not considered in your security policy and procedures, your protection will be limited. Even with the reported flaws in WEP, it is still better to have WEP active than having nothing. Also, having equipment settings left at known defaults opens your network to attacks. A solid security policy and practices, which includes periodic reviews and incorporating a defense in depth concept will yield an optimal secure network.

VII. References

[ARB] Arbaugh, W., Schanker, N., Wan, Y. "Your 802.11 Wireless Network has No Clothes". March 30, 2001
http://www.cs.umd.edu/~waa/wireless.html

[DRU] Drucker, David. "Security Flaw Isn't Death Knell For WLANs". August 27, 2001
http://www.internetweek.com/story/INW20010827S0009

[ETS] ETSI HiperLAN/2 Standard
http://portal.etsi.org/bran/kta/Hiperlan/HiperLAN2.asp

[GRI] Griffin, Sean. "Security and the 802.11b Wireless LAN". September 16, 2001
http://www.sans.org/infosecFAQ/wireless/80211b.htm

[HOD] Hodges, Ken. "Is Your Wireless Network Secure?". September 10, 2001
http://www.sans.org/infosecFAQ/wireless/wireless_net2.htm

[IEE] Institute of Electrical and Electronics Engineers, Inc. "Quick Guide to IEEE 802.11 WG & Activities".
http://grouper.ieee.org/groups/802/11/QuickGuide_IEEE_802_WG_and_Activities.htm

[PAR] "Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications". ANSI/IEEE Std 802.11, 1999 Edition

[PHI] Phifer, Lisa. "Wireless Privacy: An Oxymoron?". April 26, 2001
http://www.isp-planet.com/technology/2001/wep.html

[POR] “Port-Based Network Access Control”. IEEE Std 802.1X-2001, June 14, 2001

[UCB] University of California, Berkeley. Computer Science Division. “Security of the WEP Algorithm”.
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html