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 Defense In Depth

A lot has been said about wireless networking in recent years especially on the wireless LAN. More importantly, it has changed the way people think about wireless networks. Used to be seen as expensive technology for individuals, wireless LAN can now be seen not only in enterprise networks but also at public areas like the airport, hotels, coffee shops and also in shopping malls. This increasing trends has seen tremendous growth of wireless LANs usage and services. In fact, there has been increasing trends of having wi...

Copyright SANS Institute
Author Retains Full Rights

AD

Name: Wan Roshaimi Wan Abdullah
Title: Wireless LAN Security – Defense In Depth
Version: GSEC Practical Assignment Version 1.4b

1. Abstract

A lot has been said about wireless networking in recent years especially on the wireless LAN. More importantly, it has changed the way people think about wireless networks. Used to be seen as expensive technology for individuals, wireless LAN can now be seen not only in enterprise networks but also at public areas like the airport, hotels, coffee shops and also in shopping malls. This increasing trends has seen tremendous growth of wireless LANs usage and services. In fact, there has been increasing trends of having wireless hotspots in many countries. The benefits of mobility, easiness and convenience have made wireless LAN so popular.

This paper attempts to openly describe the technology of wireless LANs (mostly IEEE 802.11b), what are its standards and components, why it is less secure as compared to its' wired counterpart and what can be done or applied in order to make wireless networks more secured from the technology and human perspective. Moreover, this paper discusses limitations and risk of wireless LAN and how the defense in depth approaches can be deployed towards the implementation of a secure wireless LAN.

2. Introduction

With wireless LAN gaining its popularity in various sectors, security has become a primary concern. Just like any other technologies, wireless LAN also has its security shortcomings. As a matter of fact, a lot has been said about security of wireless local area networks, be it from the specification, management, usage, policy and undoubtedly implementation perspectives. Most of the information that gathered has somehow put stress on the technology being insecure. Whilst this finding is relevant, it is observed that the human factor does contribute to the security flaws in wireless networking. As a countermeasure to the technology's limitations and risks, man needs to be involved to make wireless networks more secure through appropriate enforcement of policies and procedures. Hence, the combination of technology and human factor can undoubtedly alleviate the security posture of the wireless networks.

When we talk about wireless LAN, we are talking about the mobile users who are connected to the network or the Internet with their wireless network cards. And, it is almost impossible not to mention that it will somehow be connected to the wired network as the latter will enable them to get access to the applications on the LAN or the Internet. Hence, when issues of wireless LAN security being discussed, the security of the wired LAN is thus implied. Both wireless and wired

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

LAN security must co-exist in order to achieve the desired security level for the wireless network.

3. IEEE 802.11 Standards

It is also important to review some of the relevant wireless networking standards that are available before we start looking into the security aspect of them. The understanding on how the wireless networking works will definitely help in understanding where the security concerns exist. The wireless network standards are defined by the Institute of Electrical and Electronics Engineers (IEEE).

802.11 is a member of IEEE 802 family that defines series of specifications for local area network(LAN). The reason why 802.11 is different from its members is because 802.11 allows for mobile network access. As a result, additional features were introduced into the media access control(MAC) layer to handle radio waves as the physical layer.

802.11 networks consist of four major physical components, which are summarized as follows:

- Distribution System
    - When several access points are connected to form a large coverage area, they must communicate with each other to track the movements of mobile stations. The distribution system is the logical component of 802.11 used to forward frames to their destination. 802.11 does not specify any particular technology for the distribution system. In most commercial products, the distribution system is implemented as a combination of a bridging engine and a distribution system medium, which the backbone network used to relay frames between access points. In almost all commercially successful products, Ethernet is used as the backbone network technology.
- Access Points
    - Frames on an 802.11 network must be converted to another type of frame for delivery to the rest of the world. Devices called access points perform the wireless to wired bridging function.
- Wireless Medium
    - To move frames from station to station, the standard uses a wireless medium. Several different physical layers are defined; the architecture allows multiple physical layers to be developed to support the 802.11 MAC. Initially, two radio frequency (RF) physical layers and one infrared physical layer were standardized, though the RF layers have proven far more popular.
- Stations

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

- Networks are built to transfer data between stations. Stations are computing devices with wireless network interfaces. Typically, stations are battery-operated laptop or handheld computers. However, there is no reason why stations must be portable computing devices. In some environments, wireless networking is used to avoid pulling new cable, and desktops are connected to wireless LANs.

[4]

Furthermore, there are also two types of 802.11 networks; 1) Independent networks or ad-hoc networks and 2) Infrastructure networks.

In ad-hoc mode, stations communicate directly with each other. It is called ad-hoc because the network is set up only when mobile devices want to talk to each other, normally for specific purpose and for a short duration. With ad-hoc network there is no connection to the other networks. In infrastructure network, the mobile stations communicate with each other by having an access point. As defined earlier, access points is the device that act as a bridge from the wireless network to the wired or fixed network.

The mobile stations and access points must establish a relationship before they start sending data. This process is called an association. The association process is a two step process involving three states:

- Unauthenticated and unassociated
- Authenticated and unassociated
- Authenticated and associated

To transition between the states, the communicating parties exchange messages called management frames.[5]

At present time, IEEE 802.11b technology is the most widely accepted and deployed around the world. This wireless standard technology uses 2.4 GHz band and with its direct sequence spread spectrum (DSSS) technology, it can support data rates up to 11 Mbps. In the initial stage, it supports only 2 Mbps but most of the wireless LANs today are running 11Mbps bandwidth. Moreover, 802.11b includes Physical Layer Convergence Procedure (PLCP) and Physical Medium Dependent (PMD) sub-layers. In short, "PLCP prepares 802.11 frames for transmission and directs the PMD to actually submit signals, change radio channels, receive signals and so on." [1]

Besides 802.11b, there are also 802.11a and 802.11g. IEEE 802.11a uses 5 GHz unlicensed band and can support data rates up to 54 Mbps. IEEE 802.11g is another future standard that can also support data rates up to 54 Mbps. The more interesting fact about 802.11g is not about the bandwidth but it is the fact that 802.11g operates in the 2.4 GHz frequency range. What this means is that, it uses the same frequency range as 802.11b but with higher data rates.

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

By far, we have learnt what is the 802.11b, what makes a complete basic service set (BSS) and briefly how it operates. In the later section of this paper, we shall look at areas that are concerning security and some of the best practices that should be applied when implementing wireless networks, in specific wireless local area network.

4. Defense in Depth

In deploying a wireless LAN, the same importance must be stressed in terms of security as when deploying a wired LAN. Security must be looked at several aspects like in the policy and the three A's of Security - Access control, Authentication and Auditing.[2] Defense in depth in particular defines several layers with each layer having its own security mechanisms and controls. The layers are the perimeter defense, network, host, application and information. Authentication will look at the perimeter defense and the network layer. This is basically looking at how users get authenticated and what defense strategies are applied at the perimeter. Access control meanwhile will define who can have access to the wireless network and how to control and monitor them. It will also look at the access control at the host level and application by implementing host based firewall for example. As to protect the information, security policies and procedures need to be defined and enforced while auditing your wireless network with relevant tools will strengthen all the layers defined earlier.

I strongly believe that in wireless networks, authentication plays the most important function besides having proper access control to ensure who gets what he is supposed to get and auditing mechanisms as part of preventive and corrective security measures.

a. Security Policy and Procedure

As mentioned previously, human factor does play its own role in relation to the issues that are being posed by the technology itself. As we know that all technologies will have their own advantages, disadvantages and limitations that will make the technologies useful to the users. Nonetheless, technology alone will not be able to be utilized to its most potential without the intervention of human factor, like the policies and procedures. Policies and procedures will become the guidelines for technology to be properly used and to get the most out of it. Hence, it is vital that any deployment of wireless LAN is preceded by a wireless security policy. Having a security policy that defines the right procedures for implementing wireless networks will help reduce the risk of wireless network being breached. Policy and procedures can help enforced standard rules sets required in a deployment of wireless network.

It is commonly known that most systems are often deployed in its default state. The same thing happen to the deployment of wireless LAN. Having the desire for what wireless LAN can do for us, we often forget the basic security features

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

that are built-in into the systems which are most of the time disabled for ease of configuration and installation purposes. Having utilize and enable these features, it will definitely put a barrier to any attackers and will require them putting extra effort to compromise the network as compared to networks that do not enable the basic security features.

Hence, it is recommended to implement the following security controls in order to maximize the 802.11b network by following certain best practices:

- Disable broadcast of the 32-bit plain text Service Set Identifier (SSID). This way, only clients with the known correct SSID can associate with the access point. By default, a client with any SSID can associate with an access point.

- More sophisticated attackers will counter a lack of broadcast SSID by analyzing the authentication frames with an 802.11 scanner to obtain the plain text SSID. To limit the effect of passive attacks, if possible, only broadcast beacon packets at higher bandwidth and reduce the frequency of beacon packets to inhibit such methods.

- Set non-standard SSIDs. Do not use your company name, address or any other easy to guess information about your organization.

- Do not choose SSIDs that could be attractive to attackers. Follow strong password generation methods to create SSIDs that are difficult to guess.

- Always enable 40-bit or 128-bit WEP encryption. Although there are numbers of WEP shortcomings, it will be a barrier to casual attack and it is surprising how most networks fail to use it.

- Choose strong encryption keys on all wireless devices and change shared keys regularly. Encryption key changes make it harder for attackers to obtain and maintain a foothold on your network.

- Change all default vendor passwords.

- Administer your wireless devices using secure protocols like SSH or HTTPS, instead of telnet and HTTP.

[2,3,6]

b. Authentication

Authentication is always the best possible security measures in any systems. In 802.11, it specifies two major approaches which are open system authentication and shared key authentication. We shall discuss both approaches in some detail to know how authentication is done in wireless networking.

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

The security issue in 802.11 authentication arises as it is a one way connection. Mobile stations who want to join to a network must authenticate to it but not the other way around. An access point needs not to be authenticated to a station thus opening a way for man-in-the-middle attack through rogue access points. [10]

Open system authentication is the default authentication method for 802.11. In open system authentication, the access point accepts anyone who requests authentication without verifying its identity. It works by exchanging only two management frames between the mobile station and access points.

Shared key authentication makes use of Wired Equivalent Privacy(WEP) and requires a shared key to be distributed to stations before attempting authentication. As with open system authentication, it works by exchanging management frames except with shared key authentication, it uses four management frames instead of two.

There is another mechanism used by vendors to provide security with the use of access control lists based on the Ethernet MAC address of the client. Each access points can limit the clients of the network to those using a listed MAC address. If a client's MAC address is listed, then they are permitted access to the network or else they will be rejected.[5] Moreover, it is important to note one security problem with the MAC access control list. This mechanism only authenticate the machine with the right MAC address but not the users.

With defense in depth concept in mind, it is generally not enough to go with the basic authentication especially when WEP is already proven to have so many flaws. Due to the flaws in WEP and in order to solve the user authentication problem, the 802.11 working group adopted the 802.1x standard that provides per-port authentication to improved authentication security. 802.1x provides port based authentication and wireless encryption key distribution capabilities.

As defined by Matthew S. Gast in his book,

> 802.11x defines three components to the authentication conversation namely the supplicant, authenticator and authentication server. The *supplicant* is the end user machine that seeks access to network resources, while the *authenticator* controlled the access to the network. Both the supplicant and authenticator are referred to as Port Authentication Entities (PAEs) in the specification. The authenticator terminates only the link-layer authentication exchange. It does not maintain any user information. Any incoming requests are passed to an *authenticator server*, such as RADIUS server, for actual processing.[4]
>
> 802.1x is based on the Extensible Authentication Protocol (EAP). EAP is formally specified in RFC 2284 and was initially developed for use with

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

> PPP. When PPP was first introduced, there were two protocols available to authenticate users, each of which required the use of PPP protocol number. EAP is a simple encapsulation that can run over any link layer, but it has been most widely deployed on PPP links. [4]

Furthermore, as stated in EAP working group Internet Draft,

> One of the advantages of the EAP architecture is its flexibility. EAP is used to select a specific authentication mechanism, typically after the authenticator requests more information in order to determine the specific authentication mechanisms to be used. Rather than requiring the authenticator to be updated to support each new authentication method, EAP permits the use of a backend authentication server which may implement some or all authentication methods, with the authenticator acting as a pass-through for some or all methods and users.[9]

This explains why we can have different solutions of authentication server rather than a pre-defined solution. This will allow wireless managers to vary their authentication methods based on their business and network requirements. Moreover, 802.1x is only a framework that provide the authentication base to be implemented by the authentication server. For example, "Cisco provides Lightweight Extensible Authentication Protocol (LEAP) authentication that is based on the 802.1x security standard."[7] With the framework, it is up the to the vendors on how to implement and add more value to it.

For corporate wireless networks users, that deals with corporate data, it is always recommended to use strong authentication mechanisms such as RADIUS, LDAP, Kerberos and physical tokens.[7] Another authentication method that can be used is by deploying a wireless virtual private network (VPN). VPN can provide not only another level of authentication but also can encrypt the communications channel via certain protocols. Still with defense in depth in mind, wireless network managers can also use secure communication protocols like the SSH or SSL in any application data channels. This type of authentication plus the necessary access control will add more security in authenticating wireless users.

c. Access Control

The nature of wireless networks can be treated as an external network to the enterprise LAN. As such, any security measure taken to secure your network from Internet access for example, can also be applied to your wireless network. As a matter of fact, that is how you should design the wireless network by segregating it from the wired network using a firewall, granting access to the network using dynamic host configuration protocol (DHCP) and possibly deploying intrusion detection systems (IDS) to monitor wireless network traffic for malicious and suspicious attacks.

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

One of the measures that can be applied to secure wireless LAN is by implementing a wireless firewall gateway. Wireless firewall is actually a wired firewall that bridge the wireless network and the wired network. "It works like a router between a wireless and wired network with the ability to dynamically change firewall filters as users authenticates themselves for authorized access." [8] Packet filtering can also the applied at the firewall to allow only selected protocols or hosts into the network.

In addition to having a firewall, an intrusion detection system must also be installed between the wireless network and the wired network. Intrusion detection system or IDS should be able to add more security to the network by sniffing the wireless traffics and alerting the administrators on suspected malicious traffics through defined signatures. This vigilance monitoring will provide administrators preventive and also response security measure as certain malicious traffics could be blocked before doing some damage to the network.

Furthermore, we can also deploy DHCP for issuing and maintaining IP addresses of wireless networks' clients. DHCP also allows you to group users into IP address range that is based on your requirement and defined in the firewall. This kind of arrangement will allow legitimate users to get access to the network and restrict other unnecessary access.

At the host level, it is recommended to have some kind of filtering mechanism like the personal firewall. This is to provide security access control and measure at the application and host layer.

d. Auditing

Auditing your own network is supposed to be the top priority for all network administrators. By auditing your network, you are actually looking at the vulnerabilities that are available inside your wireless networks. By finding and knowing what type of vulnerabilities existed in your network, it will prepare you to put necessary measures to overcome or prevent any kind of threats that resulted from the vulnerabilities.

There are a number of wireless network auditing tools that are available in the Internet today. One does not have to be a true hacker to be able to use these auditing tools as they are easy to use and menu driven. On the one hand, these tools have actually made hacking activities more interesting especially for casual attackers to scan for a wireless network and find known vulnerabilities. On the other hand, these tools can and in fact, should also be used and tested by network administrators on their networks.

Below are description of some commonplace wireless auditing tools:

- Airsnort – a common tool to break WEP encryption. It operates by passively monitor the transmissions. Once enough packets have been

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

gathered it will compute the encryption key. It can be found at http://airsnort.shmoo.com

- Netstumbler – windows wireless network scanner. For more information, please refer to http://www.netstumbler.com
- MacStumbler – Macintosh version of NetStumbler. For more information, please refer to http://www.macstumbler.com
- Kismet – a wireless network sniffer that separates and identifies different wireless networks in an area. For more information, please refer to http://www.kismetwireless.net
- Ethereal – a free network protocol analyzer. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session. For more information, please refer to http://www.ethereal.com
- AirDefense IDS – Wireless IDS that provides 24x7 monitoring. For more information, please refer to http://www.airdefense.net

5. Conclusion

In short, the trend of wireless LAN deployment is growing and one has to really understand the technology in order to know its security risk and limitations. Wireless LAN security can be achieved by implementing proper policy and procedures as well as deploying the right authentication and access control. Knowing and using wireless auditing tools definitely prepare administrators on what to expect on their wireless networks. Defense in depth therefore, must be applied for wireless networks in order to get the most out of our wireless networks. This approach adds more security controls and mechanisms at the perimeter defense layer, network layer and also at the host and application layer. With the availability of many security protocols like the SSH and VPN and enforced policy and procedures on wireless LAN deployment, it is hoped that the wireless LAN is more resilient and secure.

6. List of Acronyms

DHCP	Dynamic Host Configuration Protocol
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure HTTP
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
PAE	Port Authentication Entities
PLCP	Physical Layer Convergence Procedure
PMD	Physical Medium Dependent

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

RADIUS	Remote Authentication Dial-In User Service
SSH	Secured Shell
SSID	Server Set ID
SSL	Secure Socket Layer
VPN	Virtual Private Network
WEP	Wired Equivalent Privacy

7. List of References

[1] Geier, Jim. "802.11b Physical Layer Revealed."
URL: http://www.80211-planet.com/tutorials/article.php/2107261 (March 13, 2003)

[2] Watson, David. "How to Secure Your Wireless Network" Network Security, June 2002:8-11.

[3] Practically Networked. "Securing your Wireless Network"
URL: http://www.practicallynetworked.com/support/wireless_secure.htm (March 13, 2003)

[4] Matthew S. Gast. 802.11 Wireless Networks:The Definitive Guide. USA: O'Reilly & Associates Inc, April 2002. 9-10,100,106

[5] William A. Arbaugh, Narendar Shankar and Justin Wan. "Your 802.11 Wireless Network has No Clothes" March 30, 2001.
URL: http://www.cs.umd.edu/~waa/wireless.pdf (March 13, 2003)

[6] Konstantinos Karagiannis. "Ten Steps to a Secure Wireless Network" February 25, 2003. URL: http://www.pcmag.com/article2/0,4149,844020,00.asp (March 14, 2003)

[7] Gregory R. Scholz. "An Architecture for Securing Wireless Network"
URL: http://www.isoc.org/pubs/int/cisco-1-2.html (March 10, 2002)

[8] Nichole K. Boscia, Derek G. Shaw. "Wireless Firewall Gateway White Paper"
URL: http://www.nas.nasa.gov/Groups/Networks/Projects/Wireless/index.html (March 13, 2003)

[9] L. Blunk, J. Vollbrecht, B. Aboba, J. Carlson. "Extensible Authentication Protocol (EAP)" EAP Working Group, January 2003.
URL: http://www.ietf.org/internet-drafts/draft-ietf-eap-rfc2284bis-01.txt (March 13, 2003)

[10] Praphul Chandra. "802.11 Security" May 23, 2002.
URL: http://www.wirelessdevnet.com/articles/80211security/ (March 14, 2003)

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

Last Updated: May 25th, 2013

Upcoming SANS Training

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

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
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
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 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 San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	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 Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced