GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Ready for Wireless LANs?

Hoa Nguyen

Version 1.4b GIAC Practical Assignment

October 27, 2003

Introduction

Have you ever wished to get rid of all the spaghetti cables or wondered where to drill a hole to extend the computer cable into the next room. Wireless is a better choice. Popular wireless devices are pagers, cellular phones, Personal Digital Assistants (PDAs), laptops/notebooks. As the performance of wireless technologies keep improving the prices continue to drop to affordable level where everyone can have it. The experts predict that the demand for wireless devices will quadruple in the next few years [3]. The wonderful flexibility, affordable price, and better services we see, have been applied everywhere in our communities. In the restaurant, the waiter holds his handheld computer and takes your order directly from your table to the kitchen without moving his legs [4]. The doctor can review his patient records anywhere from his PDA. The article "Parking tickets now print out wirelessly on the streets of New York" of Government Computer News reported that the New York City Police Department has purchased 1,000 handheld computers to have the ability to printout parking tickets. Compare to traditional handwritten tickets, the Finance Department officials said they save the city $2.5 million in the first year by reducing ticket errors rates from 13 percent to 1 percent [1].

With the great conveniences and effectiveness features in the report from Allied Business Intelligence says the number of wireless nodes (devices) will jump to 55.9 million in year 2006 [3]. But we must keep in mind that the security risks that come along with these devices regardless we want them or not. Most consumers use the wireless technology without wondering how it works or worrying about security issues. This document will briefly describe how the wireless local area network works, what are some of the security risks and how to minimize the security risks.

Wireless Terminologies

STA - The station is a term for a laptop with some types of wireless interface card.

AP - The access point consists of the wireless interface and the software that allows a wireless device to communicate to a wired network. The access point is also called the base station or wireless router.

BSS - The Basic Service Set is the group of STAs that are covered by an AP.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

ESS - The Extended Service Set is the interconnected of the BSSs. A station can roam from one BBS to another BBS inside an ESS.

MAC - The Medium Access Control is a unique hardware address that identifies each node (system) on a network.

SSID - The Service Set Identifier is a unique alphanumeric string identifier specified in the header of packet that looks like a password when a client connects to the given BBS.

NIC - The Network Interface Card that allows a system connect to a network.

VPN - The Virtual Private Network provides the secure data transmission across public network.

Beacon – The broadcast packet used to synchronize the members of a given BSS.

RADIUS – Remote Authentication Dial-In User Service.

Wireless LAN Networks

Actually wireless communication is not new (remember walkie-talkies, airplane ground control, etc.). However, the Internet feature on the wireless communication is new [2]. These wireless devices transmit data in the electromagnetic waves (spectrum). Most wireless technologies use the Radio Frequency (RF) from the 2.4 to 5 GHz bandwidths and the speed rate from the 2 to 54 Mbps. Based on the coverage range and the speed, it divides the wireless local area network into three main categories: Wireless Personal Area Networks (WPANs), Wireless Local Area Networks (WLANs), and Wireless Metropolitan Area Networks (WMANs) or Wireless Wide Area Networks (WWANs).

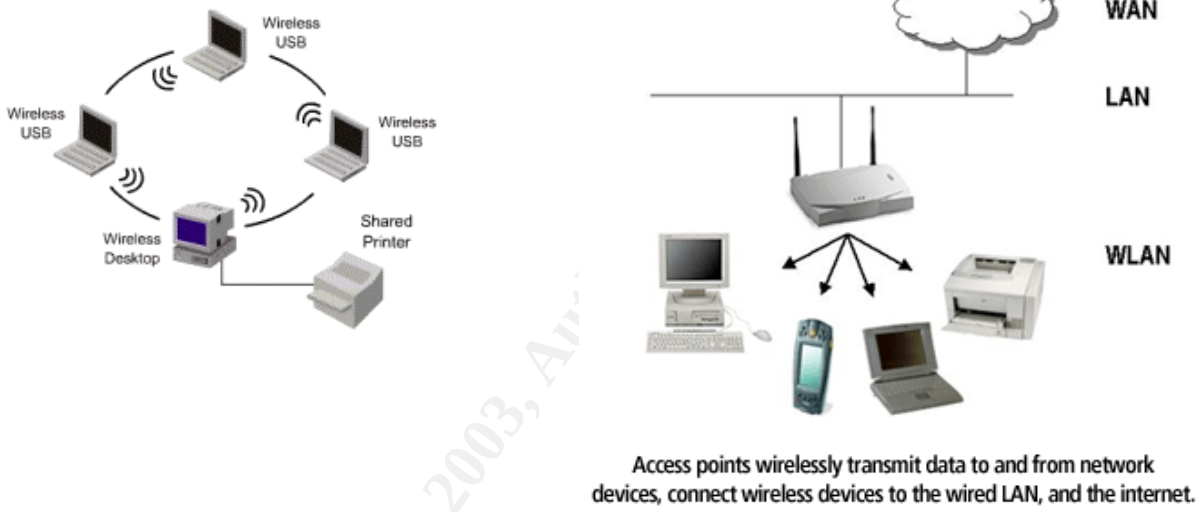
A WPAN connects systems (devices) in small areas such as offices or homes. WPANs operate in the short distance range about 10 to 30 feet and transmit data at the rate between 2 Mbps to 11 Mbps. WPANs have low power consumption and limited security features.

A WLAN connects systems and other components by using one or more Access Points (APs). The WLAN transmitting speed is in the range of 2 Mbps to 54 Mbps and communication distance expands up to hundreds of feet.

WMAN and WWAN operate at the high-speed wireless for site-to-site connections, and are long-range radio networks that provide the mobile voice and data to devices like PDA, pagers, and cellular phones. Both WMAN and WWAN have the distance range up to miles.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Wireless networks operate under two modes: Ad hoc network and infrastructure network (fig. 1) [7]. An Ad Hoc network is the independent network that allows a group of stations talking to each other without AP in a small area. This Ad Hoc network is suitable for environments that have no security concern. An infrastructure network consists of the group of stations and AP(s) as well as distribution system (i.e. wired network) behind the AP.



Ad Hoc Network **Infrastructure Network (WLAN)**

Figure. 1

802.11 Standards

Since wireless technologies have been rapidly grown, the possibility of vendors produce incompatible products. To avoid this happened the Institute of Electrical and Electronics Engineers (IEEE) organization approved the 802.11 Wireless LAN standard in 1997. This standard defines all the definitions and provides everything from how the wireless devices can communicate to each other to the security of the wired network [3]. To enhance the performance and the security, the IEEE 802.11 standard has extended into 802.11b, 802.11a, 802.11g, 802.11h, 802.11i, 802.1x, 802.11e, 802.11f standards.

The 802.11b has the transmission rate from 2 Mbps up to 11 Mbps in the 2.4 GHz spectrum band. The 802.11a supports up to 54 Mbps rate in the 5 GHz band. The 802.11g also have the 54 Mbps rate but in the 2.4 GHz band.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

The 802.11h Task Group is making the 802.11a becomes compatible with European standard. The 802.11i Task Group is concentrating on enhancements to encryption and authentication. The 802.1X Task Group is supporting the Extensible Authentication Protocol (EAP). The 802.11e Task Group is focusing on the transmission quality of services of multi media. The 802.11f Task Group is working on recommendations for Inter-Access Point Protocol (IAPP) of advanced multi-vendors [2,5].

Because it is easy and inexpensive to implement the first three wireless standards 802.11b, 802.11a, and 802.1g are the best choices for the vendors. They have developed their devices base on these three standards in the wireless LAN market. The term Wi-Fi is preferred to the first three popular standards 802.11a, 802.11b, and 802.11g specially 802.11b standard is most dominate for WLANS [3].

The 802.11 standard requires privacy to wireless network. With this privacy requirement, protection from eavesdropping the Wired Equivalent Privacy (WEP) protocol was born. However WEP can't provide fully three basic security services Authentication, Confidentiality and Integrity (ACI). WEP has many flaws because using the simple RC4 encryption algorithm, and static key algorithm the attackers can crack a WEP easy. WEP also send the 24-bit initialization vector (IV) in the clear text. All stations (nodes) use the same key. The Cyclic Redundancy Check (CRC) algorithm in the packet load doesn't guarantee the data integrity [2]. There are several automatic tools available such as AirJack , AirSnort, and Wepcrack which can crack WEP [2].

Extensible Authentication Protocol (EAP) is one of the short-term solutions for WEP. EAP is based on 802.1X standard and provides the username/password base authentication between the wireless client and the Remote Authentication Dial-In User Service (RADIUS) server. EAP generates dynamics WEP keys that are more secure than the keys. Because the keys are changed frequently, it will take a longer time to crack the keys, and by that time the login session may be over [8].

How WLAN works

When a user wants to access the Internet from his wireless device he/she really activates a wireless adapter which is installed inside a laptop (station) provides an interface between the client Network Operating System (NOS) and the airwaves via an antenna to an AP. The AP, acts as transmitter or receiver (transceiver), connects to wired network from a fixed location using regular cable. The operation between the station and AP is called client and server model.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

At normal case the AP verifies the authentication of the wireless client first. Either the Open System authentication or Shared-key authentication is configured in the AP. The Open System authentication allows a station to join a network without any identity verification as long as it responds with a Medium Access Control (MAC) address during the exchange with an AP. The second Shared-key authentication requires a station supplies the secret cryptographic key. After the authentication is done the AP receives, buffers, and transmits data between wireless LAN and wired LAN.

The Physical Layer in the Open System Interconnect (OSI) protocol handles the transmission across the physical media. Base on the 802.11 standard, in the physical layer, it allows to use the radio frequency (RF) transmission technology and infrared (IR) transmission technology (fig 2.)

Infrared technology is not widely implemented because it can't penetrate opaque objects, and it operates in limited to three-meters range. The remote controls, the bar code readers use this IR technology.

Most of the access points use radio frequency (RF) technology that can penetrate walls and travel long distances. The narrowband and spread spectrum are two types of radio network technologies that operate in 2.4 GHz frequency band with the speeds up to 11 Mbps. Narrowband technology transmits and receives user information on the specific narrow radio frequency that makes it more difficult for keep track of the different users on the different channel frequencies. Spread spectrum is mostly used in WLAN that spreads out its signal to the maximum frequency range. Spread spectrum is strong for efficiency, but is weak for reliability, integrity and security.

The spread spectrum is classified into two types Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS). The FHSS splits the signal up across the time domain (2.4 GHz band) that is divided into 75 narrowband frequencies (channels) [10]. The data is sequentially transmitted on different narrowband frequencies. The sequence of frequencies (pattern) is chosen pseudo randomly. The sender and receiver agree on the sequence pattern so that the transmitted data can hop over different narrowband channels. The original 802.11 uses this FHSS technology. FHSS devices use less power, and it has lower performance. To increase the reliability and throughput, 802.11b uses DSSS technology. The DSSS divides the 2.4 GHz band into large 14, 22 MHz channels and utilizes the same channel for the time of transmission. The United States uses the first 11 channels only. The European community uses the first 13 channels, and Japan uses channel 14. [2].

OSI Model

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Application		
Presentation		
Session Layer		
Transport		
Network		
802.11 Data Link Layer Logic Link Control (LLC) Media Access Control (MAC		
802.11 Physical Layer		
IR	FHSS	DSSS

Figure 2.

Wireless Local Area Network Threats

Potential threats are divided into natural threats and man-made threats. Natural threats include floods, wind, fire, and electrical disturbances. Man-made threats are from those who target the systems for their own purposes such as criminal activity, unlawful use, or malicious harm. The most likely threat involves an unauthorized user known as attacker (or hacker). There are two types of network security attacks: passive and active attacks. The passive attack is happened when the unauthorized user gains access to a network and doesn't modify the message (packet). The eavesdropping and traffic analysis are the passive attacks. When an unauthorized user makes the modification to the message. The masquerading, relay, message modification and denial-of-service are active attacks. [4]

All the threats on wired networks also apply on wireless network and it is possible the new threats haven't discovered yet due to the new wireless technology. Below is the list of most common potential security threats on WLAN [2,6,8].

1. There is no physical boundary in the wireless network. Wireless networks transmit data through air that we don't have ability to control. The wireless signal is propagated for the APs to receive including the high-gain antenna of an attacker. The attacker can be any where from the parking to a building mile away. The article "War driving by the Bay" of Kevin Poulsen described Peter Shipley drove around the San Francisco Bay in the rush hour traffic with his antenna on top of his car and collected close to eighty open networks ready for anyone to tap in.

2. It is easy to discover a wireless local area network. The attacker can use NetStumber software or Aerosol software to identify where is WLAN, what channel is to be used, signal strength, etc. These two software packages are free from Internet.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

3. The broadcast networks are great for sniffers. The attackers can use the sniffers Kismet or Ethereal (these two software are available from public domain) to monitor your wireless traffic. With this collected information the attackers now can attack your network.

   . The insertion attack happens when an attacker tries to connect his device (laptop or PDA) to an AP without authorization.

   . The jamming attack consists of creating the signal interference on the same radio frequencies of the wireless network. This attack causes the Denial-of-Service (DoS).

   . The attacker can become "Man-in-the-Middle" to see the transmitted data between client and access point. The "Man-in-the-Middle" attack happens when an attacker sniffs the packets, modifies them, and inserts them back into the network.

4. The manufactures ship APs with default Service Set Identifier (SSID) passwords, and the broadcast SSID turned on by default. Most of hackers know the vendor default SSID passwords. For example, the default SSID of Intel is "intel", Cisco has "tsunami", and 3Com is set to "101". The un-protected SSID generates a high potential threat on a WLAN by creating backdoors for the intruders to access to the wired network. Even WEP doesn't protect much but it is better than nothing, and the vendors turn WEP off by default.

5. WEP also contributes to WLAN threats because the encrypted data traffic can be captured. The encrypted key can be cracked in the matter of hours. The 801.11b MAC header contains information about the network, and it is not encrypted. The attacker can use the brute force technique to crack a secret key. The freeware AirSnort and WEPCrack are available on the Internet. The WEP key is same to all its stations and the key can be compromised if the "inside" attacker uses social engineering to get the key.

6. With a valid SSID the attacker can set up a rogue access point that goes nowhere to collect the authentication information from the careless users.

7. Address resolution protocol (ARP) poisoning is the vulnerability that wireless introduces to internal local network through the access point. To understand more about ARP poisoning attack see http://www.cigitallabs.com/resources/papers/download/arppoison.pdf.

8. Your neighbor, people in office next to yours or tourists can accidental connecting to your network without malicious purposes that could jam your network or the confidential information are revealed. Unintended plug-in

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

any device is in 2.4 GHz spectrum such as microwave ovens, cordless phone also interfere your 2.4 GHz network

Minimize Wireless Security Threats

Following are suggestions that will help to minimize the risks to the wireless network [2,6,8,9].

1. The first thing the company needs to do is establish a security policy for its wireless local area networks, and WLANs at remote location if applicable. The security policy should cover the important issues such as defining who are allowed to use the computer, for what purpose, and why this policy must be followed. The company also needs to create an incident handling procedure which instructs management what actions are to be taken when incidents happens.

2. Proper configuration on APs and stations.

   a) Access Point - Minimum configuration:
   . Change the default SSID to the unique one.
   . Disable the SSID beacon broadcasts.
   . Change the default password for Administrator account on regular basic
   . Enable the MAC Address filtering to permit only known or trusted MAC address.
   . Turning off broadcast pings that make it invisible to 802.11 analysis tool such as NetStumbler.
   . Enable WEP. (If possible, select 128-bit encryption however this will reduce the performance of network).
   . Changing the WEP keys periodically.

   Optional configuration (highly recommended):
   . If there is a firewall in your network place the APs outside to protect your internal network.
   . Support for advanced authentication (AP with 802.1X standard).
   . Support VPN pass through.
   . Change the default channel for less interference with other APs (for performance purpose only)

   b) Station configuration:
   . Have the personal firewall to lock down who can gain access to the client.
   . Run the desktop virus scan to identify the any virus

3. Deploy the strong authentication such as setting strong password policy. Deploy an authentication network using VPN, if possible. Install wireless LAN Products that supports 802.1X such as Cisco LEAP (Lightweight Extensible

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Authentication Protocol) and EAP –Transport Layer Security (EAP-TLS) [11]

4. Run a discovery tool on regular basic to detect any unknown SSIDs, APs, STAs, etc.

5. Identify all the systems that need to be monitor, and install audit tools. The manager must assign to someone be responsible for daily reviewing the audit logs (system logs, firewall logs, etc.) to discover any intruder, any unauthorized user.

6. Protect against wireless virus uses the software such as McAfee VirusScan for wireless, Trend Mirco PC-cillin for wireless, F-Secure Antivirus for Palm OS and Pocket PC.

7. Subscribes to the security alert site such as CERT (http://www.cert.org) to be notified immediately for any vulnerability.

8. Update patches and upgrade software as soon as possible.

9. Educate the employee/users. The company should schedule a security brief on regular basis to re-enforce the company policy (lock to screen when user is away from his computer, reports any abnormal activities to supervisor, etc.). The security brief updates (or refresh) the security threats to the employees. When the employees have more knowledge about security awareness then they can recognize the abnormal activities and report the problem right away, and corrective action will be followed.

Conclusion

There is no such as perfect security. Then the question is why we still need to consider it? The story "Two men and a bear" of Dianna Kelly from InfoSec World Conference and Expo 2003 gives us a better picture. Two men were in the woods. A big bear appeared to attack them. First man said, "I need to run as fast as I can". The second one said, "Why run? We can't run faster than the bear". The first one replied, "No, I can't run faster than a bear, but I just need to run faster than you." The attackers usually pick the easy target. We can't have 100 percent security, but the preventing action is much easier to implement than recovery the disaster.

Regardless of the size of an organization, we need to protect our assets. A company needs to know how important the computer system contributes to their business profit, define the security risks of your company, what level of risk the company is willing to accept, and how much the company willing to spend on security. When the company lays out all possibilities that could happens in the worse case, and analyzes them carefully the company should have enough input to make a decision whether to switch to wireless or not.

© SANS Institute 2003, As part of GIAC practical repository. Author retains full rights.

Reference:

[1] Government Computer News (Oct 13, 2003 issue).

[2] InfoSec World Conference and Expo 2003 notes (speaker: Mark Kean, Dianna Kelly, Gary McGraw)

[3] System Admin magazine (May 2002 issue).

[4] http://giactc.giac.org/cgi-bin/momgate (Appendix B - Wireless Networking Security section)

[5] http://grouper.ieee.org/groups/802/11/index.html

[6] http://reviews.cnet.com/4520-3513_7-5024551-1.html?tag=dir

[7] http://www.symbol.com/products/wireless/WLAN.gif

[8] http://timhogan.info/WirelessSecurity.html

[9] http://reviews.cnet.com/4520-3513_7-5021249-1.html?tag=dir

[10] http://www.airdefense.net/whitepapers/index.html (Article – How to protects WLANs)

[11] http://www.cisco.com/warp/public/784/packet/exclusive/apr02.html

© SANS Institute 2003, Author retains full rights.

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor