Global Information Assurance Certification Paper

SANS GSEC Security Certification

Scott Simon
Version 1.4b

Wireless Local Area Networks in Urban Apartments

Abstract

Over the last decade, computer availability has directly led to the expansion of household Internet usage. The growth of the internet is in relation to the availability of computers. Computer manufactures have made computers so inexpensive that having more than one computer is very common in today's society. Is there a way for these computers, from a single location, to access the Internet at the same time through a single modem? The computers are able to gain the connection by setting up a Local Area Network (LAN.) A LAN is a group of computers and associated devices that share a common communications line or wireless link. The increase in the popularity of using wireless links through LAN's for connectivity in households has also provided for a rise in security issues revolving around these connections. The focus of this paper is to educate users about wireless technology and show the security issues involved with wireless local area networks (WLANs) in urban apartments.

About Wireless

A wireless local area network (WLAN) enables computers to be connected throughout a network by means of radio wave transmissions. To fully understand the risks involved in wireless technology one must first understand what exactly "wireless" is and how wireless technology is incorporated in the computer industry. The term wireless describes all telecommunications where electromagnetic waves are used to carry a signal over a common communication path; therefore, it eliminates the need for transmissions through wires[1]. The transfer of data through electromagnetic waves between wireless devices in a computer is made possible through the standard called 802.11. The 802.11 is a family of four specifications applying to WLANs developed by IEEE (Institute of Electrical and Electronics Engineers) that specifies an over-the-air interface between two wireless clients or between a wireless client and a base station[2]. The four specifications in the 802.11 family are 802.11, 802.11a, 802.11b, and 802.11g.

- **802.11**

  The 802.11 standard supports infrared light transmissions and two types of radio transmissions. The two types that make up the supported radio transmissions are Frequency Hopping Spread Spectrum (FHSS) and Direct

Sequence Spread Spectrum (DSSS,) and they are supported in the 2.4 GHz frequency band.[3]

- **802.11a**

  The 802.11a standard is an extension of 802.11 that runs in the 5 GHz frequency band and supports data transmissions up to 54Mbps. It only supports radio transmissions using Orthogonal Frequency Division Multiplexing (OFDM). This type of transmission helps reduce the possible interference from other radio transmissions.

- **802.11b**

  The 802.11b standard (a.k.a. "WiFi" or "Wireless Fidelity") is an extension of 802.11 that operates in the 2.4 GHz frequency band, supports data transmissions up to 11Mbps, and is backwards compatible with 802.11. It does not work with infrared transmissions and only supports the DSSS type of radio transmission.[4]

- **802.11g**

  The 802.11g standard functions almost exactly as 802.11a except that it is compatible with 802.11b, because they both operate in the 2.4 GHz frequency band which creates the potential for possible data transmissions between the two. The means by which the two standards communicate effectively is by enabling "802.11b protection".[5] IEEE has made it a necessity for wireless manufacturers, whose wireless devices are 802.11g specific, to be equipped with "802.11b protection" functionality. This protection function enables the 802.11g devices to transfer data to the 802.11b devices with transmission rates at or below 11Mbps. The devices using the 802.11g standard, while communicating with the 802.11b device at 11Mbps, can also transmit data concurrently at 54Mbps. The only problem with the 802.11g device transmitting at concurrent transmission speeds is that throughput is lowered so data is actually transmitted at rates lower than advertised.

There are two types of network authentication that the 802.11 family supports are "Open Systems Authentication" and "Shared Key Authentication." Each extension of the 802.11 family supports these two types authentication and are always used in WLANs. Open systems authentication is not really a type of authentication since anyone requesting authentication is automatically given access. Shared key authentication is a form of authentication used when a wireless network has enabled Wired Equivalent Privacy (WEP). Between these two types of authentication, the only one that actually provides authentication is shared key authentication.

Wireless technology has been introduced into the computer scene to allow the transmission of data, not through wires, but through unseen electromagnetic waves. Wireless technology has eliminated the necessity of Ethernet wires to connect to other PC's and has extended the range for users to travel while keeping a connection. A good example of this is in a household that has a LAN. There are not any wires running all over the home. These are called wireless local area networks (WLAN). WLANs in close-knit communities such as apartment complexes pose a larger threat for unauthorized users to gain network access compared to WLANs in a neighborhood of individual homes or other widespread communities because of the range of area between each apartment building.

WLAN Configuration

There is an infinite number of ways to configure a WLAN; it just depends on how creative the developer is. In most home WLANs, the wireless area usually consists of an access point and wireless client devices connected to the access point. An access point is "a hardware device or a computer's software that acts as a communication hub for users of a wireless device to connect to a wired LAN".[6] There are some WLANs that are a lot more complex than just an access point and wireless clients, but these are not to common in apartment complexes.

There are two things a WLAN must contain for proper wireless communication. The first is that all wireless devices must be compatible. This means they must be deploying the same 802.11 standard or one that is compatible. The second thing is that they must be configured correctly. There are many different configuration options that manufacturers make available. These configuration options must be identical to each wireless device in the WLAN. The first step is to set your configuration settings on the access point. Depending on what configuration options the manufacturer has made available, you should be able to set such options as the SSID, the channel, the MAC address, WEP keys, etc. Once the access point has been configured, all potential wireless clients must set their configuration settings to mimic those of the access point.

Background

The area over which the study was conducted was an urban apartment complex consisting of 480 individual apartments covering 30 acres.[7] . I live in this apartment complex and have a WLAN in my apartment. Over this time period, I have come to learn a lot about wireless security issues. I noticed that whenever my Internet service went out I jumped right back on through someone else's wireless connection. After learning this, I realized that I was not the only person who has a wireless network, and then I started wondering if my wireless network was accessible to others as well. I began to investigate my suspicions and it turns out that my WLAN was wide open for anyone to access. So after finding

out this shocking information I reconfigured my wireless network to keep out unauthorized users.

Wardriving

During my search about wireless security I came across a term called wardriving. I found out that wardriving is a process that enables someone to search an area for unsecured wireless networks by means of a car and a laptop computer. A more formal definition of this process is "Driving around looking for unsecured wireless networks". [8]

In the case study I conducted for this paper, I was able to determine, through the process of wardriving, the potential security risks resulting from WLANs in urban apartment complexes.

Note: This study was conducted to explore the security issues related to WLANs. There was no malicious activity involved with this study. The information about the wireless network that was logged was kept private and files that could have been possibly accessed were never viewed, copied, modified, or deleted.

Hardware and Software

The wardriving process requires specific tools for complete functionality. Having the correct hardware is the most important requirement for wardriving. The laptop must be compatible with the wireless network interface card (wireless NIC,) and the NIC must be capable of constant channel scanning. The hardware tools I used were a Dell Latitude laptop and a wireless network interface card (NIC) made by Orinoco.

The next requirement is software. The software must be capable of interacting with the wireless NIC, able to set the NIC's configuration settings, and must be compatible with the operating system you are using. The software package I choose to use is called NetStumbler[9]. It is essentially a tool for wardriving, but it is also designed for users to check coverage of their Wireless LAN, gatherers of demographic information about 802.11 popularity, drive-by snoopers, and overly curious bystanders. NetStumbler is a software package that is specific to wireless NIC's that are capable of channel scanning such as the Orinoco wireless cards (http://www.orinocowireless.com). It interacts with the wireless cards directly and automatically configures the card to constantly scan multiple channels sniffing for network "hotspots." (http://www.netstumbler.com) It is compatible with Windows 2000, Windows 9x, and Windows XP. Once your hardware and software requirements are fulfilled, the next step is to get into a car and start driving around and let the computer go to work.

Process

There are a few things I had to do before I started the process. First, I had to configure the software to enable the wireless NIC to continuously scan multiple channels, searching for access points that were broadcasting on those channels. Next, I tested the software by trying to scan for my access point. After successfully testing the software, I made sure my battery was fully charged and the computer was functioning correctly. Once I was in the car and the car was running, I started up NetStumbler and began scanning.

While the wireless NIC is scanning for access points, it is also reporting its finding back to the software. The data that is returned to the NetStumbler software is translated into an understandable format and is then displayed to the user. Once I completed driving around the apartment complex, I went back to examine the results.

Results

The software enabled me to scan and log a total of 15 different wireless LANs. The logged data supplied by NetStumbler allowed me to view very detailed information about others WLAN configurations. The list below contains some of the types of information that was made available after scanning for access points.

- MAC address
- SSID
- Channel
- Vendor
- If encryption is enabled
- Signal strength
- Noise
- Signal to noise ratio (SNR+)
- The time the network was first and last seen
- The actual position of the hotspot (Latitude and Longitude)

From the data that was supplied by the NetStumbler software, I was able to reconfigure my wireless cards settings to mimic the settings of the scanned access points and gain access to other networks. Once I became part of other people's networks, I was given the capability to freely browse the Internet, and the ability to access files that were shared across their LAN. This level of access in which I was granted poses a very large threat if it were to fall in the hands of a destructive user.

The reason I was able to gain this access is because some of the WLANs were using open systems authentication specified in the 802.11 standard. As stated earlier, this is not really a form of authentication because it allows any wireless

device access to the network. As soon as I configured my wireless NIC with the values that match one of the scanned access points, I was then authenticated to their LAN.

Not all of the scanned wireless LANs were accessible. The reason that I was unable to gain access to some of the wireless networks was because they were using shared key authentication, which is deployed whenever a WLANs has WEP turned on. WEP, which stands for "Wired Equivalent Privacy"[10] is a security protocol designed for wireless LAN's. WEP enables data packets to be encrypted as it passes through one wireless device to another. Only half of the scanned access points had WEP enabled. So it turns out that fifty percent of wireless users are unaware of the hazards that a WLAN poses.

Securing Your WLAN

Having a router or a firewall is a good idea if you are trying to secure a wired network. The problem with having a WLAN inside a wired network is that an intruder can gain access to your network through your wireless access point without ever having to go through the firewall or router. There needs to be additional security measures taken in order to avoid unauthorized users gaining access to your network. There are only a handful of ways to properly securing a WLAN. Following these network security practices will result in additional layers of protection over the WLAN.

The most popular way of securing your wireless LAN is to enable WEP encryption. WEP falls under the Media Access Control (MAC) Layer in the Open System Interconnection (OSI) model. The MAC layer is a sub-layer of the Data link layer that is responsible for data packets to be encrypted and transmitted between two NIC's.

WEP uses "Shared Key Authentication," so each wireless device must contain identical pre-defined WEP keys. The process of shared key authentication is explained:

> "A station requesting 802.11 service sends an authentication frame to another station.
>
> 1. When a station receives an initial authentication frame, the station replies with an authentication frame containing 128 octets of challenge text.
> 2. The requesting station copies the challenge text into an authentication frame, encrypts it with a shared key using the WEP service, and sends the frame to the responding station.
> 3. The receiving station decrypts the challenge text using the same shared key and compares it to the challenge text sent earlier. If they match, the receiving station replies with an authentication acknowledgement. If not, the station sends a negative authentication notice."[11]

There are two primary functions of WEP. One is to protect against network snoopers who are attempting to monitor a wireless network, and the other is to deny any attempts by unauthorized users to gain access to a wireless network[12]. WEP was developed to add privacy to your network, and almost all wireless manufacturers have enabled their products to support WEP. Since WEP is the most commonly used type of security for a WLAN, it became a primary target for hackers to try to crack. Although WEP can be cracked and it is not 100% secure, is just another barrier to aide in protecting against unauthorized access. Since WEP has already been cracked, its serves as only a temporary barrier between an access point and a persistent intruder.

Other methods of security

- Media Access Control address (MAC address) based access is another form of security that may be used for authenticating wireless devices. The MAC address of a computer is a unique hardware number that determines "who is who" on a network. MAC address access implies the use of a machines MAC address to access a network. To access the network, the computers MAC address must mach one of the defined MAC address from the list contained in the access point. The only computers allowed to access the access point have their MAC address stored in the access points MAC address list. This seems like a pretty secure method right? Well, just like WEP, this method is also not secure since some software has made it possible to "spoof" or mimic another's MAC address.

- Make sure that your wireless hardware contains the most up to date firmware. Many of the first 802.11 products, when they were first introduced, provided sloppy security features. Upgrading the firmware of these devices will provide you with the most current security functions allowing another layer of protection across your WLAN. The firmware updates should be done on a regular basis. You can find these upgrades by going to the hardware manufacturers home page.

- Many access points support the saying,"ready to go right out of the box." To support this functionality, manufacturers have pre-configured their access points (functioning as a router and supports DHCP) to be run as a DHCP server. Dynamic Host Configuration Protocol (DHCP), describes the means by which a system can connect to a network and obtain the necessary information for communication upon that network. DHCP works by a client computer on a network is requesting information from the server, the server will send out this information and automatically configure the client machine. Pre-configured wireless DHCP servers pose a security threat because many people will leave DHCP running with the default settings. All someone needs to do to gain access to the access point is to scan for access points with software such as Netstumbler, and enter in the SSID for their wireless card. If they do this they will have

become a member of the network without anybody knowing. If DHCP is required for a network, make sure you configure it to be very limited in the way it functions.

- Do not allow your access point to broadcast its Service Set Identifier (SSID,) a unique sequence of characters that acts like a password and differentiates one WLAN from another.[13] When there are multiple access points being broadcasted, the SSID allows for a wireless client to determine which access point to attempt to connect to. A simple scan of a wireless network will easily capture the SSID of a machine. Not all access points have the ability to disable their SSID from being broadcasted, but many newer models have incorporated this option.

- You need to be very careful on choosing an access point for your WLAN, especially when it will act as the main source of security for your WLAN. Here is a list of requirements that an access point should satisfy:

    - Capable of 128 WEP encryption
    - Act as a router and support NAT firewall security
    - Provide multiple ports for wired connections
    - DHCP server
    - Advanced security management functions
    - Web based configuration

  Access points that do not meet these requirements should not be considered as possible investments. Once you have purchased and set up the access point, move it to the center of the room away from windows. This will provide good wireless coverage and make it harder for the signal to escape.

Opting to use the aforementioned security practices above will provide a stronger defense system for wireless LAN's to protect against unauthorized access and to make it much harder for an intruder to gain access. Even though you can never be 100 percent secured wirelessly it's always better to have some protection instead of none at all.

---

[1] Anonymous. URL: http://whatis.techtarget.com/definition/0,289893,sid9_gci213380,00.html (24 Apr 2003).

[2] IEEE 802.11 Standard – "A 802.11 Planet Definition" URL: http://80211-planet.webopedia.com/TERM/8/802_11.html.

[3] Wireless Background. Office of Information Technology Network Services, U of Florida. URL: http://net-services.ufl.edu/provided_services/wireless/background.html

[4] Webopedia.
URL: http://www.webopedia.com/TERM/8/802_11.html.

[5] SearchMobileComputing.com.
URL:http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci855455,00.html

[6] MIT Information Services.
URL:http://web.mit.edu/IS/help/network/glossary.html.

[7] Homestore.com
URL:http://www.springstreet.com/apartments/fyp/search/brochure/feature.jhtml?cPointer=&propid=431875

[8] About WarDriving.
URL: http://www.wardriving.com/about.php.

[9] NetStumbler.com, home page.
URL:http://www.netstumbler.com

[10] 802.11 Planet.
URL:http://www.80211-planet.com/tutorials/article.php/1368661

[11] Wireless.itworld.com
URL: http://wireless.itworld.com/4246/ITW1844/page_1.html.

[12] "Security of the WEP Algorithm".
URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[13]SearchMobileComputing.com.
URL:http://searchmobilecomputing.techtarget.com/sDefinition/0,,sid40_gci855455,00.html .

Last Updated: May 25th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event