Global Information Assurance Certification Paper

Security Vulnerabilities and Wireless LAN Technology

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Heather D. Lane
Location: Virginia Beach,
August/September, 2004

February 6, 2005

Table of Contents

Section I

A. Abstract/Summary

Wireless local area network systems (LANs), also referred to as Wi-Fi can be found everywhere. Since their introduction in the mid 990s, they have proliferated among home users and have taken over organizations whether or not they are authorized. We would be hard pressed to find a new computer that does not have wireless LAN capability, and like their wired counterparts, wireless LANs are prone to security vulnerabilities. However, most of these so-called vulnerabilities exist only because enough care is not taken to ensure that there is strong security in place. The only exception being Denial of Service (DoS) for which there is no one resolution so far, but it is possible to reduce the likelihood of it affecting your LAN by using a combination of precautions.

This paper describes many of the vulnerabilities that can exist for home wireless LAN systems, also referred to as small office/home office (SOHO) LAN systems, as well as for enterprise LAN systems. Both LAN types are vulnerable to the same kinds of attacks and errors, but this paper places the emphasis on details of the larger more complex enterprise wireless LANs. The paper discusses where the vulnerabilities reside, methods that can be used to detect them, and how to secure them. Discussion of hackers' tools, 802.11 security standards, and points to consider in planning a wireless LAN are also incorporated into the paper because of their importance when attempting to secure a wireless LAN. Although the main focus of the paper is wireless LAN security vulnerabilities, some information on current and future trends in wireless LANs is also included. The paper concludes that wireless LANs can be used safely, if safety measures are taken to secure them.

B. Introduction – What is a Wireless LAN

In its simplest form, a wireless LAN can be thought of as two or more unwired computers using the airwaves for typical computer purposes, with the help of an access point. In the case of a home computer system, one computer is usually wired while the other(s) is not, hence the wireless concept. The unwired computer uses a Wireless Access Point (WAP) to network the two computers, thereby allowing both machines to use the same Internet access, printer, scanner and other peripherals. This is in contrast to previous configurations that required that some form of cable be run to each computer on the network. In the case of an enterprise, a wireless LAN can consist of several computers, usually laptops because of the mobility factor, using wireless access points to connect to a larger, more complex enterprise system with large amounts of data transactions occurring over radio frequencies.

People want to be able to travel anywhere and use their laptops without the

need to connect to a wired central location. As a result an even newer technology known as WiMax is slated to be the next big step in the wireless industry. However, in keeping with the discussion of our current technology, wireless capabilities are popping up in coffee shops like Starbucks, hotels and motels, marinas, truck stops, even at the base of Mt. Everest. Wireless is also in use in law enforcement, the Department of Parks and Wildlife and other organizations that need to immediately communicate with headquarters. Because of the varying needs for wireless, organizations must have strict security policies in place and communicate the policies to their users. In conjunction with the security policies, adequate measures must be consistently implemented. It must be noted that the main difference in the vulnerabilities that SOHOs and enterprises suffer is found in the magnitude to which each group suffers loss. Enterprises are larger with more data, vital sensitive applications, and more people who can be affected therefore their loss may appear to be greater, when in fact a loss for the smaller SOHO can be just as devastating.

Since today's society is more mobile than in past years, wireless LANs are becoming more and more popular everyday. Everyone or all of those interested in technology or using computers, wants to have a "wireless" whether or not they know or understand the technology. In the past year, I have personally witnessed the explosion of requests for wireless in my company. The rush to wireless can present concerns because, in addition to its unique problems, it can also experience the security issues present in wired networks. This reality necessitates the implementation of tight security to prevent or curtail the vulnerabilities that wireless LANs present.

Section II

A. Some Common Wireless LAN Vulnerabilities

Vulnerability can be described as some event that exposes us, or in this case a network system, to an action that may be detrimental to its ability to operate efficiently and effectively with its desired level of confidentiality. Systems become vulnerable to negative forces due to the lack of proper safeguards, as in the case of wireless LANs. There are several known vulnerabilities that occur mostly because of the very nature of the LAN, which uses radio frequencies (RFs) to permit the transmission of data over the airwaves. One major reason that a number of vulnerabilities occur, in both SOHOs and Enterprises, is because uninformed users setup wireless LANs without the prudence necessary to secure these systems from malicious or even accidental events. Following are some of the commonly known Wi-Fi vulnerabilities.

1. No configured security or poor security

If the 802.11 security settings for authentication and encryption are not functional, or the service set identifiers (SSIDs) are not changed, this can cause

external attacks. For example, it is known that Linksys uses the default SSID "linksys ", Cisco defaults to "tsunami", and Symbol defaults to "101". Also, if an access point is configured simultaneously for both VPN and open authentication, authorized users will authenticate via VPN while unauthorized users will use open authentication to sneak in. Another configuration problem to be aware of is failure to change defaults in a Windows XP machine with wireless capability. In this case the XP system automatically searches for an access point connection and may accidentally connect to an undesirable system.

2. No set physical boundaries

Wireless access points can lose signals because of wall, doors, floors, insulation and other building materials. The signals may also enter into another user's airspace and connect with their wireless local area network. This is referred to as accidental associations and can occur in densely populated areas where several people or businesses use wireless technology.

3. Physically insecure locations

Access points should not be placed where they are easily accessible because they can be removed and tampered with (configurations copied or altered) then returned.

4. Untrained users setting up unauthorized workstations and networks

This group constitutes users who either are uninformed and therefore unaware of security measures that must be taken when deploying wireless, or whose desire to have wireless is so strong that it completely overshadows the rules set by the organization to ensure that systems are secure. These actions can be costly to an organization, therefore it becomes the enterprise's responsibility to change attitudes through education, and provide policies that outline consequences for violators. It has been my experience that in addition to having policies in place and outlining consequences, it is necessary to perform repeat monitoring to encourage compliance. Also, organizations must control who can gain access to the wireless LAN to prevent the unauthorized deployment of ad hoc networks where employees' machines can "talk" back and forth to each other.

5. Rogue access points

These may be illicit access points brought in to the enterprise by employees, or poor access point setup by the untrained employee described above. An employee might also mistakenly use SOHO access points that are not designed to be used in an enterprise because of its weak security options. Other rogues may include external malicious users such as hackers engaging in war driving in an attempt to access the wireless LAN from nearby locations.

6. Lack of network monitoring

Intrusion detection tools can be used successfully to continuously monitor for rogue access points. Not deploying some means of detection with alarms and event data recorders practically leaves the door wide open to hackers or other undesirable users.

7. Insufficient network performance.

This occurs when a network system is not designed for capacity. With the headers, packets, interframe spacing and other activities that occur, throughput becomes significantly degraded to cause the wireless LAN to operate at about half its expected data rate.

8. MAC address filtering

A media access control (MAC) address is a unique number assigned to a computer. In wireless LANs this number is used to allow an access point to connect to a particular network. Total reliance on this filtering can result in a security breach as a user may change the MAC address, which changes its 'identity', thereby resulting in identity theft. This is also known as MAC Spoofing.

9. Inadequate encryption standards

Wired equivalent privacy (WEP) is a weak encryption standard to say the least, therefore some users will not even enable it. This can prove to be detrimental to the wireless LAN because weak encryption is better than no encryption at all. Also, some users make the encryption key longer but this does not make the LAN more secure, it just makes the hacker work harder at trying to penetrate the system.

10. Off-hours traffic/War Driving

We've all heard the stories of hackers sitting in parking lots with equipment loaded with software like Net Stumbler, or using other detection devices in an attempt to gather data from enterprises with unprotected LANs. This is referred to as off-hours traffic and "some enterprises even take steps to turn off the access points during non-office hours". [1] Kozup, p. 3. In contrast, war driving actually refers to hackers driving from place to place attempting to find connections to which they can attach.

11. Unauthorized data rates.

If an access point appears to be accepting data at rates slower than those governed by the 802.11b standard, this could be a danger signal suggesting that an intruder is nearby trying to access data.

12. Easy to eavesdrop

Because Wireless uses the airwaves, it is easy to listen in on network traffic or even connect to a network. However, just listening to network traffic does not

necessarily produce results if the data is encrypted with strong encryption. If WEP encryption is used it is more likely that hackers can, with some effort decrypt the information they have intercepted.

13. Man-in-the-middle attacks

External rogues can launch man-in-the-middle attacks that attract legitimate connecting access point traffic at authorization time, forcing users to connect to the rogue. The hacker gathers all the authentication information of the legitimate computer as it connects to the access point, then uses this information to send a request. The access point sends the virtual private network (VPN) challenge to the legitimate system, which returns a valid response. The hacker using this information pretends to be the access point and the request, challenge, response transactions continue with the hacker now appearing to be legitimate.

14. Unsecured holes in the Network

A hacker can enter a wireless LAN by circumventing firewalls then allowing others to come in, as a result sensitive data on the network may be compromised. Hackers may also use the enterprise's resources including the Internet connection.

15. Denial of service Attacks

External rogues can cause Denial of Service (DoS) attacks where the network is flooded with data packs forcing users to disconnect continually thereby disrupting enterprise operations. These disruptions can be caused by noise from microwaves, cordless phones, or other appliances that operate on the 2.4 GHz radio frequency on which 802.11b wireless LANs also operate. Disruptions can also be caused by hackers using access points to send dissociate commands.

B. Solutions

What are some of the security problems wireless LANs can face? In a nutshell there are - - untrained, uninformed people, misconfigured or unconfigured equipment, and hackers or other "undesirables". So how do we solve these problems?

As stated earlier, wireless LANs can be secure and if secured properly they can be more secure than wired networks. If this is so what can be done to ensure this security? Since the "people" factor has been previously discussed this paper will now focus on the technical equipment factors.

For the convenience of having wireless LANs organizations must:

- ***invest time and money to continually monitor and secure their airways and networks***

To secure wireless LANs, ensure that there is a centrally managed firewall and implement security at each of the five levels of layers --- perimeter, network, host, application and data. This secures the perimeter and communication, as well as monitors network traffic.

Monitoring devices like scanners and sniffers should be set in place to detect activity from hardware, software, and other machines that may be searching for a connection. One of the systems that can be put in place is the "walkthrough" or site survey. This could be time consuming, and by no means is the best solution because it requires an individual to physically walk through the installation with handheld RF signal analyzers checking for illegitimate connections. Another solution is to install rogue access point sensors, but users can disconnect their rogue access points as they become aware of the searches, or set their access points to duplicate their laptop's media access control (MAC) address so they become invisible. Furthermore, the result of the search is only accurate at the exact point in time that the sweep occurs.

When unauthorized activity is detected, the enterprise must have measures in place to find and eliminate it. The best method of finding the activity once it has occurred might be as simple as having the audit or monitoring employee go directly to the perceived location. The best method to eliminate or limit rogue attacks before they occur is to implement 802.1X with AAA. To prevent man-in-the-middle vulnerability attacks use an Extensible Authentication Protocol (EAP) method that does not allow a hacker to re-route packets. However, the best monitoring environment is one which has sensors in place to detect unauthorized activity; and services that can notify authorities via an alarm, analyze data, and provide reports.

- ***Ensure that security policies are put in place and IT staff is trained in setting up equipment.***

This removes the people/employee factor because there is now a greater potential for consistency and correctness in configuring the wireless LAN equipment. IT staff must:

1) Change SSID so that the manufacturer's defaults do not remain, therefore cannot be compromised.
2) Enable WEP (wired equivalent privacy). WEP, the original wireless security standard, has some security issues but temporal key integrity protocol (TKIP) addresses them. Wi-Fi protected access (WPA), if it works with the system, is an alternative to WEP since it is a combination of TKIP and 802.11i.
3) Set wireless to MAC address that can be filtered by a firewall.
4) Turn off Dynamic Host Configuration Protocol (DHCP) so that IP addresses are not automatically given out to every user attempting to access the network.
5) Have users report all stolen or misplaced equipment.

Section III

A. Hackers Tools and Methods

The hacker's goal is to break security standards as they are developed which in turn keeps the IEEE busy developing new standards. Several detection and encryption breaking tools as well as the sharing of "how to" papers/articles are made available on the Internet for free, adding to the problem. As a result even the novice wireless user can attempt some of the hacking techniques provided online. The goal of the enterprise is to find the tools that will give them an edge in detecting flaws in their LAN structure, then fixing the problems to secure the LAN. Below are some examples of the tools that hackers use. Note that these tools can also be used by the enterprise during their vulnerability/risk assessment to find the holes in their systems before hackers do.

Antennas are used to detect 802.11 signals.

Encryption breaking tools like AirSnort and WEPCrack are used to lie in wait of data that is repeated so that they can break the encryption keys.

War Driving, as mentioned before, can be effective because hackers drive around using scanners and probing devices like Netstumbler to find ill configured access point locations so that they can enter a wireless LAN. Hackers even post maps and data on the Internet identifying LANs that were easy to penetrate in the past. "High-grade antennas that produce strong yet tight signals" [2] Phifer, can be used to help keep war drivers at bay because their narrow signals may not reach the street.

Malicious Association can be achieved by using the HostAP tool. This tool allows a machine to convert to an access point which then connects to the network via an unsuspecting, unsecured access point as it searches the airwaves for a connection.

B. 802.11 Standards

The Institute of Electrical and Electronics Engineers (IEEE) is responsible for developing the radio technology standards to be used by wireless LANs. These standards pertain to the 802 wireless standards including 802.11, the first one that was developed, and several variations of it. Each standard though developed for wireless LANs serves a different purpose for the LANs, due in part to hackers, as well as others who might challenge its security for the purpose of strengthening their own enterprise security. As vulnerabilities, or holes, are found they become public knowledge and the IEEE proceeds to update the standard. The standards (versions) listed below are the most common ones, a

list of which can be found in any wireless LAN literature or in IEEE published data.

802.11 usually referred to as Wi-Fi, was approved in 1997 and is the first wireless standard pulling together the network link and MAC address.
802.11a is an extension of 802.11 that uses 5 GHz radio frequency with data rates up to 54 Mbps. The transmission rate may be half as much as dictated by 802.11b and 802.11g.
802.11b is also an extension of 802.11 but it uses 2.4 GHz radio frequency with data rates up to 11 Mbps. 802.11b is, "the defacto wireless networking standard of the last few years" because "it offers excellent range and respectable throughput". [3] Flickenger, p.10.
802.11g uses 2.4 GHz radio frequency with data rates up to 54 Mbps. It is also backwards compatible to 802.11b.
802.16 describes bandwidth between 10GHz and 66GHz and between 2GHz and 11 GHz frequencies, and it supports high bit rates for up to 30 miles. It is expected to be popular in the future supporting WIMAX technology.
802.1X provides stronger wireless LAN security for user authentication. It is standard for port based network access control with EAP and allows a new key for each user and each session, but this standard has already shown vulnerability.
802.11n is currently under development to solve the 802.1X vulnerability issues. It is expected to have data rates over 100 Mbps.

C. Points to Consider When Planning a LAN Deployment

Once top management's support is obtained, a 'roadmap' or project plan should be developed to aid in the deployment effort. This in turn requires that much thought and formal planning is undertaken for the success of the project. In deploying a LAN consideration must be given to the cost, human factor, the current organization structure, current and future needs of the enterprise, physical structure of the building(s), technical aspects of the enterprise network including equipment, and the method that will be used for the deployment. Following are some questions to address, and things to think about during your planning sessions:

- **Cost effectiveness** -- will LAN deployment be cost effective in terms of saving money by not having wires? Will it be costly if there is no deployment or partial deployment and rogues spring up?
- **Policy** -- must be specific enough so that employees know why the policy is written, what it means, the role the employee plays in observing the policy, and the consequences for not following the policy. Keep in mind that tougher security stymies mobility, but policies are necessary.
- **Organization structure** -- should take into consideration the mobility of employees and the kind of equipment they will need to use the wireless

LAN. Are these needs changing? If so, can future needs be predicted with some degree of accuracy? How far in the future should the plan cover? Is there enough IT staff to configure the equipment and monitor the wireless LAN, and still stay abreast of new risks as they are made known?

- **Physical structures** -- how many buildings? Are all tenants in the building from the same enterprise? If not how many floors, which floors? Is the building(s) in close proximity to other enterprise buildings that might be using wireless LANs?
- **Network structure** -- is there a firewall? What is the latest or developing wireless LAN technology and does it fit the organization's needs?
- **Deployment effort** -- will deployment be enterprise wide or for selected groups only? Keep in mind that if the LAN is not deployed enterprise wide impatient employees will deploy rogue access points.
- **Equipment needs** -- what kind of monitoring equipment will the enterprise need, and on what scale? Will camera phones be allowed in? What other mobile equipment will be needed?
- **Deployment methods** -- what kind of authentication and encryption will be used?
- **Vulnerability/risk analysis** -- which tools will be used to conduct the study? At what point will it be undertaken?

D. Current and Future Trends

Wireless LANs are used in sales, streaming video, underwater video, security cameras, learning institutions, banking, corporations, homes, and will some day be used in outer space. In other words, if you can think of a need, as long as a radio signal can be transmitted and then received by some kind of access point, it will be possible to use a wireless LAN.

Worldwide Interoperability for Microwave Access (WIMAX) products are expected to be competitive with DSL and broadband, maybe even replacing them in the long run. The hope is that WIMAX will operate much like a cell phone by allowing your wireless computer to connect to the nearest WIMAX antenna.

Smartphones also referred to as Softphones have voice communication, web based applications and other web services. They are expected to become the "mobile platform of choice for the information elite." [4] Molta, p. 2.

Wireless PDAs with Wi-Fi and/or cellular are already popular but are expected to grow in popularity. They can access business applications and will become more popular than laptops. For example, they can be used to gather real time information for hospitals. Health workers can review patient charts, check for medicine interactions etc. Information from a patient's monitoring devices can be made available via a wireless LAN to health care workers. Tests and x-ray

results or any other patient information can also be accessible if needed in the operating theater. This technology is currently being used at local hospitals in my area.

Voice Over IP (a wireless LAN with IP technology) is expected to mature as it becomes more popular. This technology is currently popular in hospitals where cell phones are banned for fear of interference with vital machines. It provides contact with hospital personnel instead of having to use a paging system. There are also VOIP products that allow people to make calls over the Internet without using a phone or dialer.

Scanning/barcode technology providing real time information for manufacturers continues to be popular. For example, some companies use scanners that read barcodes to send information like the number, type, color etc. of a product being released to a shipper as the product is loaded on the forklift. But is it possible that this technology can evolve to the point of not having to physically scan barcodes? It has. This technology is called Radio Frequency ID (RFID).

RFID is being used with everything from tagging newborn babies, to tagging clothes and is currently being tested to investigate its potential use in tagging visitors to the United States. Its largest area of use is in manufacturing but some industries are reluctant to invest in RFID because the technology has not yet matured and it is still an expensive technology.

Consider the following scenario --- After the product is manufactured it is placed on pallets in quantities that are recorded as they are stored in the warehouse. Each package has a tag (sensor) that transmits a signal to a wireless LAN as the product is removed by the forklift. This information is now recorded in the database, the transaction is confirmed and the product is shipped. This would remove the need for hand scanners, remove the possible error of the forklift operator failing to scan the product, and the shipping process would be faster.

Section IV

Conclusion

Wireless LANs are very valuable in today's mobile society. They have proliferated over the past few years, and although the market has not quite reached its maturity level due to refinements to some of the hardware and software, it is no longer a secret to the public at large. Anyone who does not personally have a wireless LAN knows someone who does, uses one at work,

has heard of the technology or is unknowingly affected by the technology each day of their lives. Although wireless LANs for both small office/home office and the enterprise have some security vulnerabilities, if care is taken to implement the following safeguards the vulnerabilities will be greatly minimized or removed allowing the LAN to be used safely:

- inform and train users
- configure the access points
- monitor the LANs
- use strong encryption
- implement 802.1X with authentication, authorization and accounting (AAA)
- deploy an EAP method

To compliment the measures above, there should also be:

- a system of checks and balances in place, for example, have a second IT staff member double checked the access point configuration.
- a plan to consistently demand better products from manufacturers
- an effort to stay abreast of the latest in developing technology

With newer technology that promises greater built-in or add-on security measures, wireless LANs will attract greater, more sophisticated hacker attacks -- another chapter in the continuing saga of security versus hacker. We know that hackers will never go away, so we bear the burden to provide the best 'locks' we can to protect our LANs. Finally, whatever the outcome, wireless LANs will survive and are here to stay even if the technology has a new look and, or feel in coming years.

Section V
Works Cited

"Best Practices for Rogue Wireless LAN Detection"
AirDefense, Inc. White Paper. 2003. October 05, 2004.

Botelho, Greg. "Reaching the Far Reaches of the World Without Wires."
Technology. Wireless Life. CNN.com. Friday, November 19, 2004. November 29, 2004.
<http://www.cnn.com/2004/TECH/internet/10/18/wireless.rural/index.html>

Flickenger, Rob. Building Wireless Community Networks, 2nd Edition.
California: O'Reilly, 2003.

Kozup, Chris. "The Top 10 Wireless LAN Policy Violations."
WLAN WATCH Security Newsletter, May 2003. October 4, 2004.
<http://www.airdefense.net/eNewsletters/May03/feature.htm>

Lindstrom, Pete. "Selecting the Right Wireless LAN Monitoring Solution."
WLAN WATCH Security newsletter, November/December 2003. October 4, 2004.
<http://www.airdefense.net/eNewsletters/Nov03/feature.shtm>

Lopez, Jason. "WLANs Vulnerable to Hacking."
NewsFactor Technology News. June 14, 2004. January 1, 2005.
<http://www.newsfactor.com/perl/story/25380.html>

Ludden, Michael. "The Internet's Next Big Step."
Technology. Wireless Life. CNN.com. Tuesday, November 9, 2004. November 29, 2004.
<http://www.cnn.com/2004/TECH/internet/10/18/wireless.broadband/index.html>

Molta, Dave. "The State of Wireless Networking."
Mobile & Wireless Technology. Network Computing, May 27, 2004. January 11, 2005.
<http://www.nwc.com/showitem.jhtml?articleID=20900233>

Molta, Dave. "Adding 'Quality' to Wireless LANs - WLANs Get Priority."
Mobile & Wireless Technology. Network Computing, December 9, 2004. January 11, 2005.
<http://www.nwc.com/showitem.jhtml?articleID=54200974>

Molta, Dave. "Survivor's Guide to 2005: Mobile and Wireless."
Mobile & Wireless Technology. Network Computing, December 16, 2004. January 11, 2005
<http://www.nwc.com/showitem.jhtml?articleID=55301616>

Muller, Nathan J. Wireless A to Z
New York: McGraw Hill, 2003.

Phifer, Lisa. "Air Safety".
Information Security. TechTarget, April 2003. December 16, 2004.
<http://infosecuritymag.techtarget.com/2003/apr/airsafety.shtml>

"Retailers Dragging Feet on RFID Initiatives."
Wireless Tracking. Wireless: NewsFactor Network. January 27, 2005. February 1, 2005.
<http://wireless.newsfactor.com/gps/story.xhtml?story_title=Retailers-Dragging-Feet-on-RFID-

Initiatives&story_id=30054&category=gps>

Sharma, Chetan and Yasuhisa Nakamura. Wireless Data Services Cambridge, UK: Cambridge University Press, 2003.

"The Wireless LAN Book for Enterprises". Trapeze Networks. 2003. December 16, 2004

"Understanding the Layers of Wireless LAN Security and Management" AirDefense, Inc. White Paper. 2003. October 05, 2004.

Wi-Fi Glossary. Airespace Inc., 2005 <http://www.airespace.com/products/glossary.php>

"Wireless LAN Policies for Security & Management" AirDefense, Inc. White Paper. 2003. October 05, 2004.

"Wireless LAN Security: What Hackers Know That You Don't" AirDefense, Inc. White Paper. 2003. October 05, 2004.

Endnotes

[1] Kozup, Chris. "The Top 10 Wireless LAN Policy Violations." WLAN WATCH Security Newsletter, May 2003. October 4, 2004. <http://www.airdefense.net/eNewsletters/May03/feature.htm>

[2] Phifer, Lisa. "Air Safety". Information Security. TechTarget, April 2003. December 16, 2004. <http://infosecuritymag.techtarget.com/2003/apr/airsafety.shtml>

[3] Flickenger, Rob. Building Wireless Community Networks, 2nd Edition. California: O'Reilly, 2003.

[4] Molta, Dave. "Survivor's Guide to 2005: Mobile and Wireless." Mobile & Wireless Technology. Network Computing, December 16, 2004. January 11, 2005 <http://www.nwc.com/showitem.jhtml?articleID=55301616>