Global Information Assurance Certification Paper

An Overview for a Wireless Security Assessment

Luiz Carlos Mariante Alves

GSEC Practical Assignment Version 1.4b Option 1

June 09, 2003

Abstract

This paper will give the reader general information about a wireless networks security assessment based on the 802.11b standard. It gives an explanation of the architecture and how the devices communicates, the equipment available and what you need to know about them to do the assessment. Shows a method of planning and executing an assessment to improve security and keep track of breeches that may exist within the WLAN and it offers several actions you can take to reduce the visibility of your wireless network as well as make access more difficult to intruders to obtain. Some knowledge of 802.11b and networking is assumed of the reader.

Introduction

Convenience, low cost, easy to install, easy to use and increase of productivity are some of the many good reasons why wireless networks based on the 802.11b standard are becoming so popular. However wireless networks brought a new genre of security risks to the network and most security administrators are unfamiliar with them.

Wireless local area network (WLAN) signals goes through the air, making it a lot easier for intruders to monitor traffic, disturb the transmission of data and break

into the network. This is very worrisome for businesses with sensitive data for which security is paramount.

Nobody wants confidential or personal information to be seen by unauthorized people. The necessity of keeping the integrity, confidentiality and availability of sensitive information is of extreme importance and if you are not careful, wireless networks may leave doors opened for the loss of all these three elements in your company, small office or home.

Wireless assessment. What for?

- Have you once tested the effectiveness of your wireless security safeguards?
- Do you know if unauthorized wireless networks are sending your confidential information to outside your organization?
- Are the security controls you have put into your wireless network effective?

If you have answered “no” to any of these questions, you should do an assessment on your WLAN.
Most companies, small offices and home offices when deploying a wireless LAN don’t think about security. Their priority is to guarantee if it’s working correctly and if all employees can use it.

Approximately 70% of the wireless access points[1](AP) in the world are currently running without encryption and 27% are still using the default settings that came with the hardware. [2]

That’s a big mistake, especially if your work resides in confidential data.
After deploying a wireless network, you need to implement a security assessment to verify that your WLAN complies with effective security policies. For most cases, this is necessary whether or not the network implements effective security mechanisms.

Never rely only in the design of a system. It’s best to run tests to be sure that the network is hardened enough to guard company resources against intruder attacks.

The WLAN connectivity

To perform a wireless assessment an understanding of how the WLAN devices are connected and how they communicate is required. This section is intended to give an overview of the three main types of 802.11b architecture and how they communicate.

[1] Access Point (AP) is a wireless gateway, which connects wireless clients to the wired network.

1) Ad-hoc WLAN

The simplest wireless network configuration is the ad-hoc (peer-to-peer) WLAN. An Ad-hoc network is formed when computers equipped with wireless adapter (NIC cards), communicate directly with each other without a central Access Point (AP). This type of WLAN can be set up whenever two or more wireless adapters are within range and using the same radio channel. Figure 1 shows the architecture of the ad-hoc WLAN.

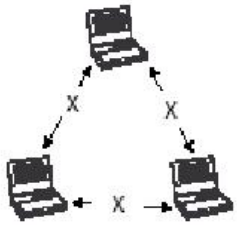


Figure 1 [12]

Ad-hoc networks are inherently insecure and will not be discussed in this paper.

2) Infrastructure WLAN

An infrastructure WLAN consists of various access points (AP) and wireless stations. The stations communicate through the AP that links the wireless network to the wired network allowing users to share other resources. This type of network allows an administrator to monitor activity and enforce security measures for all wireless devices in communication.
The devices in this type of WLAN, communicates in two different ways. In open networks the access points sends out periodic transmissions called beacons, which advertise stations within range of it existence. This beacon contains the network name, also referred to as SSID. The stations within range compare the SSID received with its own. If they are the same the station can connect to the WLAN. In closed networks, the station is the one that sends a request similar to a beacon, containing its SSID and the access point decides if the station can connect or not, based on the SSID received.
None of these types of communication is secure, but to make intrusion a little more difficult, stick with the second option, since the burden of discovery an access points relies on the station.
Figure 2 shows the architecture of a infrastructure WLAN.

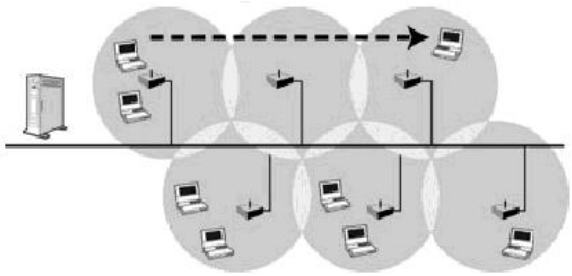


Figure 2 [12]

3) Microcells and Roaming

Access points have an area of coverage called microcells. To extend the WLAN range beyond the coverage of a single AP, the installation of many access points is necessary. To ensure that users can move seamlessly between AP without having to log in again every time they are in range of another AP is only possible if the access points have a way of exchange information as a user connection is passed from one AP to another. Figure 3 shows the architecture of Microcells and Roaming.

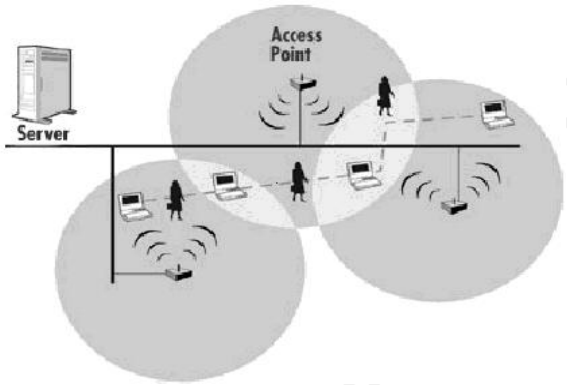


Figure 3 [12]

The Equipment

Certain types of equipment will be necessary to execute the assessment. A laptop, wireless cards, antennas and GPS devices, play a large role in what kind of assessment and at what range the assessment will be successful. Basically you will need the wireless network interface connector (NIC) card used by a desktop, laptop, or handheld computer to provide wireless network access, an antenna for better reception of the signals and software that shows the information captured in the signals. The topics below explain more about each one.

Cards

There are many different wireless cards available today. It is important to understand the requirements and limitations of the card you plan to use. Some cards require more power, are less sensitive, and might not have an available antenna jack for expanding the range with an additional antenna. [13] They have also significantly different setup procedures with different operating systems. With Linux or BSD, you have to recompile the kernels with the proper pcmcia-cs drivers, which may not be an easy task if you have no or little Unix experience. Windows, on the other hand, has a much easier setup process, but there are far

fewer tools, exploit and techniques you can use in the assessment from the windows console.
Three major types of NICs exist for wireless devices with different features:

- *Lucent Hermes based* (Used in Orinoco cards, supported by most wireless tools, includes an external antenna jack)
- *Intersil Prism II based* (Used in SMC, Netgear, Linksys, D-Link and most Proxim cards, not supported by most commercial tools, the most common 802.11b network cards)
- *Cisco based* (Included proprietary features to improve 802.11 security, farthest range and quality of reception)

Antennas

To choose the right antenna you must first know what type of assessment you are going to do. The size of the area for the assessment, the existence of barriers such as walls, floors, buildings. If you are going to be inside a car or on foot, indoors or outdoors. All these considerations must go into decision for the antenna you are going to use.

To pick the right one, you need to understand antenna direction. *Directional antennas* are used when targeting specific areas and are not very effective if you are doing the assessment while driving. Directional antennas are most effective in long-range packet capturing because the power and waves are tightly focused in one direction. (Figure 1). *Omnidirectional antenna* is the most effective in close city driving because it transmit and receive signals from all directions, but it has a smaller range as compared with the first one (Figure 2).
There are plenty of antenna types available today with different power and ranges. Just be sure to pick the right one for your kind of assessment.

Figure 1 - Directional grid antenna [8]

Figure 2 - Omnidirectional antenna connected in a card [8]

Software

Numerous software possibilities are available with a range of price and features. *Kismet*[2] *(Freeware linux)*, includes the most robust features to identify access points. It includes a feature to map networks when combined with a GPS. It works on laptops or many handheld devices, but it lacks integrated reporting features. *NetStumbler*[3], the most popular freeware tool for windows has also a feature for GPS mapping and it's easy to use but cannot detect access points with a specific security setting (Broadcast Probe Request) disabled.
There are many others like AiroPeek, Wireless Scanner, Wellenreiter and etc.

GPS (Global Positioning System)

This kind of equipment (Figure 3) keeps a real-time log of the device's position by mapping the longitude and latitude coordinates with corresponding time-stamps. It can create colorful and accurate maps for identifying access points and their ranges using proper software. If you are going to assess a small area don't waste your time using it. But, it may be of a great help if you want to cover big areas. (Figure 4 – The map was made using a software program called Netstumbler, a laptop running Windows, a lucent wireless network card, an external antenna using a mag-mount, a small handheld GPS unit, Stumbverter software and Microsoft's Map Point software [11]. The green ones represent AP with no security enabled)

Figure 3 – GPS equipments [10]

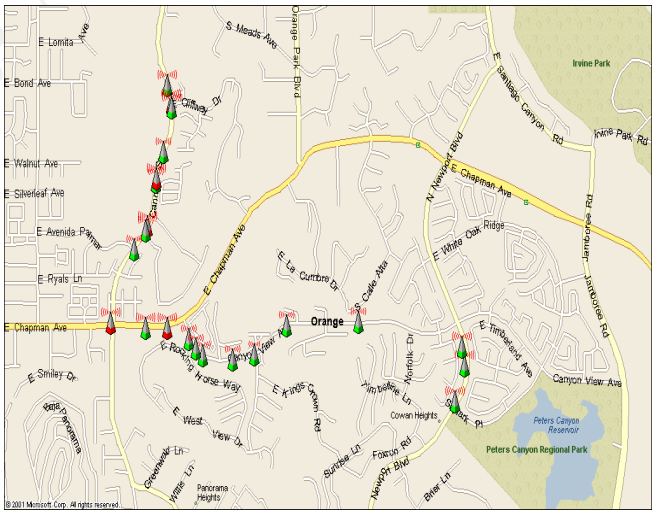


Figure 4 –Street map generated from GPS coordinates. [11]

[2] www.kismetwireless.net/
[3] http://www.netstumbler.com/

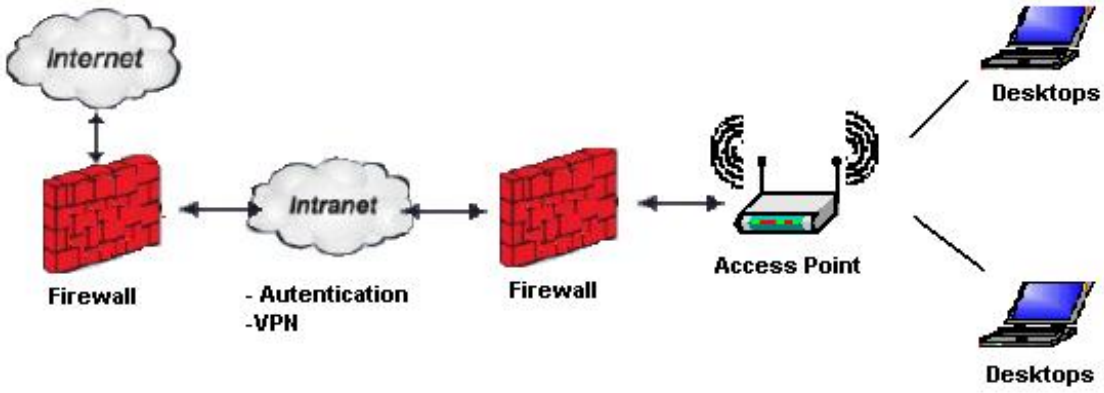
Phases for a WLAN assessment

The assessment is supposed to be done with very little company-wide visibility, because this creates the most realistic environment for true security measures to be tested. Often, the most vulnerable part of the wireless network is also the first part to be turned off or set aside while wireless security assessment is being performed. The more visibility the assessment has, the more it can lose effectiveness since not all vulnerabilities would be exposed. With that in mind let's look at the phases that should be done for a complete assessment of a wireless network.

1) Review wireless policies, architecture and configuration

When most people think about assessing a WLAN, the first thing that popup on their minds is the image of a guy walking or driving around the place with a laptop, a wireless card, software tools like NetStumbler sniffing information that is going through the air and trying to find vulnerabilities within the network. Well that's the basics of it, but there are plenty of things you can do to improve the WLAN assessment to help you find more security issues and recommend better and more efficient improvements.

To begin, start the assessment with a review of the system architecture and configurations of the wireless network. Meet with the WLAN administrators and information systems personnel to a read through documents related to wireless network architecture, device locations and previous wireless reports or assessments (if available). You will need this information to determine whether there are any design flaws that provide weaknesses that could allow a hacker inside the network. The following diagram shows an example of a properly configured network to handle wireless traffic.



This review will also give the magnitude of the assessment. Number of locations, the layout of the place, if it's a building, must be considered the number of floors to assess, if there are many others buildings around (that could be using wireless

and interfere on your assessment). It will also help you decide what kind of equipments (including antennas types and GPS) to use, authorizations to ask, and plan your time schedule.

The knowledge of a company's policies concerning wireless LAN should be taken very seriously, because this knowledge will enable one to determining whether or not a company is following it's own wireless LAN security policies. Furthermore, you will also be able to make an evaluation and parallel recommendations for policy changes. Make sure the policy has no "holes" for a hacker or angry personnel to access or damage company's resources. For example, any and all policies regarding the wireless LAN should mandate that no one could or should install access points without previous authorization from company's IT group.

Communication is the key to guarantee that all the policies are known and are being used accordingly. Don't assume that just because a policy exist that all employees are aware of it. To be on a safe side, talk to a sample of employees to make sure they know and are following all the policies. Also, it's a good idea to check if employees are utilizing personal firewalls when connecting to the WLAN.

Another issue that is very important is the physical security of the devices. Walk around and do an inspection of all the installations of access points, noting their physical convenience, types and orientation of the antennas, and radio wave broadcast into segment of the facility that don't have physical security controls. Also, the location of the access points should be planned with care, so it would be difficult for someone to see it and have access to it.

Also check for electronic devices and verify if these devices cause RFI (Radio Frequency Interference) on the WLAN. The 2.4Ghz frequency used by the WLAN is an unlicensed frequency and many different electronic devices such as cordless phones and BlueTooth are transmitting on that band. They can be interfering with the proper communication between clients and access points on the WLAN.

2) Social Engineering

To assess a network and verify for vulnerabilities you must employ the methods the intruders apply. Attackers often use social engineering to save some time and gather some precious information without any work at all, just with a smooth talk

Social Engineering is a technique used to gain information from a company by social means, such as interacting with employees, convincing someone to let you into the building, or asking someone for their password. Even though it may not sound productive, the human nature to trust is generally agreed upon to be the weakest link in security chain. No matter how technologically secure the wireless

network is, the threat can only be reduced to a certain level and then it's up to the employees to keep the corporate network secured [7].

Exploring this method is a good option to gather as much information as you can about WLAN (SSID, IP addresses, encryption type, user passwords, devices passwords, and even physical access to networks and secured areas). Be sure that before starting social engineering with the company's employees, obtain a signed document by a senior manager allowing the utilization of such methods, especially If you are a third-party doing the assessment for another company.

3) Investigating Access Points

As part of the assessment, wardrive[4] through the facilities having access points and use all the equipment discussed a few sections above to capture the access points configurations, to determine which security mechanisms are actually in use and whether or not they comply with effective policies.
Most of the time, when access point configurations don't comply with security policies, the result is an open, non-secure entry port to the corporate network. There is a good chance it is a rogue AP.

Rogue access points are a problem because most of the time they are using the default settings or others policies that do not comply with the company policy and leave a big whole in the network security.

As a result, scan for these unauthorized access points as part of the assessment. The most common and least expensive method for detecting rogue access points is to walk through the facilities with monitoring tools, such as AiroPeek or AirMagnet. Capturing data in this fashion is only valid at the time of capture. Someone could activate a rogue seconds after you turn of the sniffing device, and you won't have any idea that it's present. [3] (That's one of the reasons why keeping the assessment exposure as low as possible is very important)

You can also check configuration settings and look for potential rogue access points from a console attached to the wired side of the network, if the company has centralized support tools. Use this opportunity to learn as much as possible about procedures the company has in using these tools, because you can spot potential security issues.

4) Perform penetration tests.

After you have gone wardriving, identified target access points, and captured loads of packets, its time to start this next stage of the assessment process. You

[4] WarDriving – the practice of driving (or walking) through areas with an active wireless client running WLAN discovery software. The goal of wardriving is to discover open WLANs that can be tapped into or used to hijack network bandwidth.

will be able to examine every detail contained in a wireless frame. This includes source and destination MAC address, features enabled on the client, features enabled on the access point, supported transmit speeds, current transmit channel, encryption status, SSID, beacon interval, and more. In addition you can examine the data portion of the frame, seeing passwords and other data if no encryption is being used.

This phase of the assessment is to analyze if the wired network is as safe as possible from attacks originated from the wireless part.
To try to gain access to corporate resources, you can use AirSnort[5] to exploit WEP[6] weaknesses and crack the encryption. AirSnort is a packet capturing tool for wireless LAN's. It run's under Linux and all that is required is a wireless network interface card that is capable of running in promiscuous mode. AirSnort requires approximately 5-10 million encrypted packets to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password very quickly.

Be sure to save any log files or proof of access, capture screen shots of systems accessed, collecting and analyzing the kind of data transmitted when accessing these systems, and if there was any sensitive information observed.

Ps: This paper is not intended to show the techniques used to perform penetration tests but simple indicate that this can be a good evidence for the assessment to show that the WLAN is not hardened enough and need security improvements.

5) Wrapping Up

All the information you collect during the inspection process provides a foundation for understanding the security position of a company or organization. After gathering all the information in the above steps, spend some time thinking about potential gaps in security. This includes issues with network architecture, operational support, policy and other. Predict what a hacker would look for and bring to light any and all methods that would make it easier for someone to break in and control the company resources through the wireless LAN.

As you recognize flaws in the security of the wireless LAN, research and illustrate methods that will contradict the issues. Start by urging improvements to the policies, which dictate what the company requires in terms of security for the wireless LANs. This will build up the security system to a level that shields the company's interests.

[5] http://airsnort.shmoo.com/
[6] Wired Equivalent Privacy (WEP) is a mechanism that encrypts WLAN traffic to prevent unauthorized users from reading data captured in transit.

Here are several actions you can take to reduce the visibility of your wireless network to intruders, as well as make access more difficult to obtain. Some of these solutions require vendor-specific hardware, or may not be possible for certain network configurations.

- **Minimize propagation of radio waves in non-user area:** Using directional antennas, you can direct the propagation of radio waves inside the facility lessening your exposure to eavesdropping and also optimizing coverage. Consider setting access points and antennas near the edge of the building so you can lower transmit power and thus reduce range outside the facility.

- **Restrict access to wireless devices**. Don't leave access points within easy reach of a hacker who can replace a legitimate safeguarded access point with an unsecured, rogue access point that accepts access from any user. In fact, it's a good idea to keep them in a room with access control.

- **Change access points default settings**. Don't use default settings that come with the hardware. In most cases the security features are disabled. SSID, SNMP, Administrative passwords are widely known by hackers. Set strong passwords and SSID name for access points.

- **Disable SSID broadcasting.** Prevent the AP from broadcasting the network name and associating with nodes that aren't configured with the WLAN's unique SSID. While this will protect the network from rogue users, it will make WLAN deployment a more hands-on experience because WLAN clients will require that the network name be manually configured. This isn't foolproof, however, because someone can still monitor 802.11 association frames (which always carry the SSID, even if SSID broadcasting is turned off). At least shutting off the broadcast mechanism will limit access.

- **Use static IP address**. The use of dynamic host configuration protocol (DHCP) makes very easy for anyone to become connected to the network, since DHCP offers a convenient method to distribute valid subnet IPs to clients devices. Using static IP addresses increases the difficulty of a possible attack.

- **Enable Wired Equivalent Privacy (WEP).** Although it has weaknesses, and can be cracked, it requires a more knowledgeable and determined individual to do it. WEP does a good job from protecting many home and business networks from the general public. Better use WEP than nothing.

- **If available, enable WiFi Protected Access(WPA)**. WPA is a specification of standards-based interoperable security enhancements, which strongly increase the level of data protection (encryption) and

access control (authentication) for WLAN. Wi-Fi Protected Access is derived from the forthcoming IEEE 802.11i draft standard and is designed to be forward-compatible with that standard when it is published. It is a very strong wireless security enhancement, but while no security solution can ever claim to be “absolutely secure”, the protection that Wi-Fi Protected Access provides is significant and addresses all the known attacks on WEP. It also adds strong user authentication, which was absent in WEP.

- **Utilize IPSec based encryption and VPN (Virtual Private Network) technology on client devices**. In cases where confidential data must traverse a WLAN, the data can be protected by VPN and IPSec based encryption to provide the level of confidentiality required.

- **Ensure dissemination of security policies throughout the company**. Ensure that all employees and organizations within the company have knowledge and are in conformity with the security policies. Utilize methods to disseminate it to all employees.

- **Check NIC and access point firmware**. To fix security issues of devices, keep all NIC cards and access points updated with the latest patches to firmware. Make it a habit to always get the latest patches to a new device before making it available for use and keep checking for new ones that the vendors releases.

Conclusion

There is no such thing as perfect security. Rather, every security measure can be seen only as a deterrent, not as absolute prevention.
Wireless 802.11b networks are vulnerable to attacks and these attacks will undoubtedly increase in number and sophistication over time, and deterrence is only possible by performing regular assessments to keep tracking of security breeches that may appear in your wireless network.

References

1. "Wireless LAN Security 802.11b and Corporate Networks" 2001. URL: http://documents.iss.net/whitepapers/wireless_LAN_security.pdf (April 2003)

2. Griffith, Eric. “Mapping the Lack of Security.” 25 Oct 2002. URL: http://siliconvalley.internet.com/news/article.php/1488541 (May 2003)

3. Geier, Jim. “Identifying Rogue Access Points.” 6 Jan 2003. URL: http://www.80211-planet.com/tutorials/article.php/1564431 (May 2003)

4. Geier, Jim. “Wireless LAN Security Assessments Steps.” 20 Nov 2002. URL: http://www.80211-planet.com/tutorials/article.php/1545731 (April 2003)

5. Geier, Jim. “The Guts of WLAN Security Policy.” 12 Nov 2002. URL: http://www.80211-planet.com/tutorials/article.php/1499151 (April 2003)

6. Wi-Fi Alliance. “Wi-Fi Protected Access Q&A.” URL: http://www.weca.net/OpenSection/pdf/Wi-Fi_Protected_Access_QA.pdf (Jun 2003)

7. Signa Services "Best Practices for Deploying Wireless LANs". URL: http://www.signaservices.com/PDF's/security_audit.doc (May 2003)

8. WirelessCentral.Net (pictures of the antennas) URL: http://www.wirelesscentral.net (May 2003)

9. Kershaw, Mike “Kismet Documentation” URL: http://www.kismetwireless.net/documentation.shtml (May 2003)

10. O'Reilly Network: Where Are You, Exactly? A GPS Introduction [Dec. 08, 2000] URL: http://www.oreillynet.com/pub/a/wireless/2000/12/08/gps_intro.html (May 2003)

11. Packetattack.com “Sample Netstumbler Map using MapPoint and a short intro” URL: http://www.packetattack.com/wireless.html (May 2003)

12. Pulsewan.com “What is WLAN?” The Wireless Networking Industry’s Information Source [Dec, 2002] URL: http://www.pulsewan.com/data101/wireless_lan_basics.htm (May 2003)

13. McClure, Stuart / Scambray, Joel / Kurtz, George. Hacking Exposed Fourth Edition. McGraw-Hill Companies, The. [February 2003] (Chapter 10) (April 2003)