Global Information Assurance Certification Paper

Understanding Security Issues with Wireless LANs
Security Essentials v1.4b

Maria Caravaggio
October 2002

Abstract

IBM, COMAQ, and Toshiba to name a few are have begun delivering laptops with integrated 802.11b wireless cards. Gartner predicts that the cost of wireless cards and access points will drop by 2005[1]. Wireless devices are becoming the way of the future, especially in home environments. This paper will detail some of the security issues surrounding wireless networks, demonstrate the ease of eavesdropping and joining ill configured wireless networks and list some recommended best practices that will reduce the risk in deploying wireless networks within an organization and within a home environment as well.

Introduction

In 2001, most IT and telecommuncations markets were flat at best. But end-user spending on wireless LAN (WLAN) equipment grew by 40 percent year over year to $1.5 billion worldwide. Gartner Dataquest expects the worldwide market to grow at a compound annual growth rate (CAGR) of 22 percent through 2005[1]. The low cost, ease of deployment, and promises of productivity gains, makes wireless networks an attractive alternative to wired LANS. An employee can go from floor to floor and gain access to the network without the need to physically plug into the network. This convenience and ease of use, and promises of productivity gains brings with it many security challenges.

Wireless LAN vulnerabilities can be broken up into 3 categories. There are vulnerabilities that are inherent to the nature of wireless technology, there are vulnerabilities that stem from ill configured wireless devices, and then there are the vulnerabilities that stem from weaknesses in the protocol being used.

No network is completely secure, even wired networks, but there are some recommended best practices that can mitigate the risks posed by these vulnerabilities. Better management and configuration of access points, supplemental security protocols and practices, as well as a concise wireless security policy, together with employee awareness, will help reduce the risks in implementing wireless LANS.

---

[1] Rolfe, Andy, "Wireless LAN Market for Strong Growth Through 2005" March 11, 2002, Gartner Dataquest Research Brief

Background

Bluetooth

Bluetooth was introduced in 1988 as a standard for personal area networks[2]. It can support up to 80 devices within a range of 10 meters and speeds of up to 1 Mbps for data and voice. It runs on the same frequency band as 802.11b (2.4 GHz), therefore causing interference with devices running 802.11b protocol.

Bluetooth facilitates the creation of a peer-to-peer wireless network, with other Bluetooth enabled wireless devices, without the need of an intervening access point. This type of WLAN is called an **ad-hoc** network. Ad-hoc networks create a very high security risk. Wireless devices can connect to each other, without any prior authentication and without any controls. Any one who has their wireless device configured in ad-hoc mode could easily become part of this network, and gain unauthorized access to the wired network.

Bluetooth is most commonly used with devices that require low power consumption, short range, and when speed is not a requirement.

802.11

The IEEE 802.11 Working Group started to develop standards for 2.4GHz and 5GHz wireless networks in the early 1990s, and approved the first 802.11 standard in 1997. 802.11 standard provides 5.5Mbps or 11Mbps in the 2.4GHz band, also known as 802.11b and up to 54 Mbps in the 5GHz band, known as 802.11a[2]. Devices running 802.11b can also create ad-hoc networks, provided that they are within 500 feet of each other, but the most common deployment of this WLAN technology is with the use of an Access Point (AP). The access point converts airwave data into wired data, acting as a bridge between the wireless devices and the wired network[3]. When wireless devices are connected to a wired network via an Access Point, it is operating in **infrastructure mode**. Most access points are rated to support 60 to 70 simultaneous devices.

The 802.11 standard defined WEP (Wireless Equivalent Privacy) as the mechanism for protecting over-the-air data transmission. WEP was introduced with the 802.11 standard to deploy an equivalent level of privacy to wired LANS. Wired LAN are protected by the physical boundaries of a building, therefore not necessarily requiring encryption, but because data travels over airwaves with Wireless devices, physical security cannot be implemented, thus the 802.11

---

[2] Milanesi, Carolina "Bluetooth and 802.1X: Competition or Coexistence ?" December 3, 2001 Gartner Research

[3] Hiller, Kimberly, "Wireless LANs: An Overview" July 3, 2001 Gartner Research

standard implemented WEP encryption to provide a level of security that is similar to a physical boundary.

This paper will focus on the 802.11 standard, as it is the most widely deployed wireless network protocol to date. The longer range and higher speed of 802.11 make it the protocol of choice for wireless LANs.

Wired LANs and its Vulnerabilities

Inherent WLAN Vulnerabilities

Wireless networks send data over the air and usually extend beyond the physical boundaries of a building. A hacker does not need to have physical access to an organization's network to wreak havoc with its resources. A hacker can eavesdrop or set in motion a Denial of Service attack (DoS) from a parking lot across the street. When WLANs are implemented, conventional security measures such as physical access to the building, or physical access to a device do not apply.

There are two main inherent vulnerabilities that come with wireless devices. The first one is the ability to eavesdrop on a data conversation, and the second is the ease of setting in motion a Denial of Service attack.

Eavesdropping on a wired network requires physical access on a port that is between the two endpoints, or gaining unauthorized access on one of the nodes and running a packet-capturing program like TCPdump[4]or Ethereal[5]. Ethernet networks implemented with hubs broadcasts all data to all nodes on the LAN segment, making it very easy to sniff (listen and capture data packets). Ethernet networks implemented with switches are more difficult to sniff because the switch is intelligent enough to only forward packets to the destined host. It does this by looking at the Media Access Control address (MAC) and sends the packet to the appropriate port on the switch. Sniffing packets on a switched network can be done, but it requires special configuration on the switch

Because data now travels over the airwaves, physical access to a device is not necessary to eavesdrop on a data conversation, nor is it necessary to be physically connected to a LAN segment. The same tools to eavesdrop on a wired network can be used on wireless devices.

Figure 1 is a screen capture of Ethereal running under Windows XP. The capture details the conversation of wireless devices deployed without WEP encryption. Ethereal is a free network protocol analyzer for Unix and Windows. It allows you to examine data from a live network or from a capture file on disk. You

[4] TCPdump can be freely downloaded from http://www.tcpdump.org
[5] Ethereal can be freely downloaded from http://www.ethereal.com

can interactively browse the capture data, viewing summary and detail information for each packet. Ethereal has several powerful features, including a rich display filter language and the ability to view the reconstructed stream of a TCP session.[6] Since the wireless communication was not encrypted, a hacker can recover passwords and can capture any confidential data submitted over the wireless LAN. With large enough traces, a hacker will eventually be able to identify many of the devices that are part of the wireless LAN and even some devices on the wired LAN. By analyzing the protocols being used, a hacker can deduce the types of operating systems and applications being used on the wireless LAN.

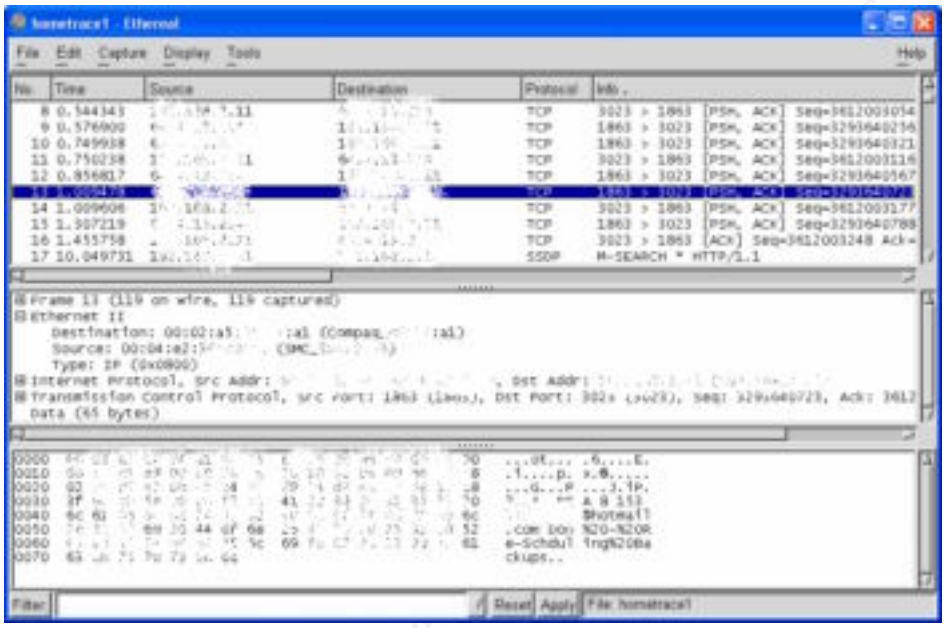

Figure 1. Ethereal screen capture running on Windows XP

There are many tools freely available to capture data packets on a network. There are also new tools designed specifically for WLANs that not only captures the data, but also provide decrypting mechanisms for WEP. Airsnort[7] and WEPCrack[8] are two such tools with this capability.

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. Cards known to do this are:

- Cisco Aironet

[6] http://www.ethereal.com
[7] Airsnort can be freely downloaded from http://airsnort.shmoo.com
[8] WebCrack can be freely downloaded from http://wepcrack.sourceforge.net

- Prism2 based cards using patched wlan-ng-0.1.13 drivers, or wlan-ng-0.1.14-preX drivers (no need for patch)
- Orinoco cards and clones using patched orinoco_cs 0.09b drivers

AirSnort requires approximately 5-10 million encrypted packets to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second.

Wepcrack was the first available code to demonstrate the weaknesses in the key-scheduling algorithm of RC4. It does not have the capability of capturing live data, but relies on the output of prismdump or Ethereal 802.11 saved captures.

To mitigate the ease of eavesdropping, IEEE developed WEP to provide a level of privacy on the airwaves. As we will see later on, WEP has its' own vulnerabilities. If an organization wants to ensure the privacy of it's communications, it should consider deploying a more sophisticated mode of encryption. Depending on an organization's requirements, they can implement 802.1X or implement IPSec and VPN technology. Both of these options will be discussed later in this paper when discussing the vulnerabilities in WEP.

The second inherent vulnerability to WLANs is that it is very easy to inject interference into the airwaves, causing the access point to stop responding (Denial of Service attack). Anyone with a strong enough transceiver can generate enough radio interference that it would make the access point unable to communicate effectively. This type of vulnerability if very difficult to reduce, unless an organization is willing to spend a fair deal of money fortifying its' walls.

Vulnerabilities with Access Point Configuration and Management

Most wireless devices are shipped with any security features disabled, and the capability of creating ad-hoc networks enabled. Access points are simple to install, all that is needed is a wired LAN connection and mobile devices with wireless capabilities. Due to the low cost of these devices, and simple installation of these APs, any employee within an organization can connect an AP to a wired network, creating a security hole into the organizations' wired network.

Discovery of organizations' WLAN network and sometimes-wired network is very easy. War driving is a term, which is similar in concept to war dialing, where one continuously dials a number to find an open modem port. War driving is accomplished by driving through a neighborhood, looking for ill configured Access Points. These tools are easily available on the Internet. One such tool is Netstumbler[9] by MariusMilner.

[9] Netstumbler can be freely downloaded from http://www.netstumbler.org

Figure 2 is a screen capture of Netstumbler running on Windows XP. Nine of these devices were discovered while riding a commuter train home one evening, the rest were discovered by driving through my neighborhood at approximately 40 km/hr. As can be noted from the screen capture, out of the 24 devices discovered, 23 wireless LANs were deployed using an AP, only 2 devices were using WEP encryption, and 12 devices were using a default SSID.

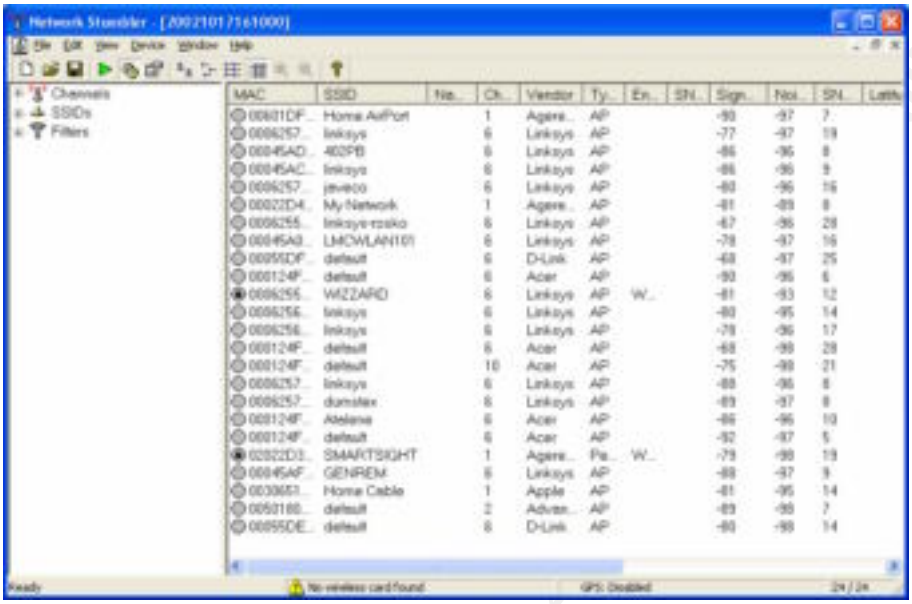

Figure 2. Netstumbler screen capture showing 24 discovered wireless LANs.

Nestumbler scans for networks roughly every second and logs all the networks it runs into--including the real SSIDs, the AP's MAC address, the best signal-to-noise ratio encountered, and the time you crossed into the network's space. If you add a GPS receiver to the notebook, the program even logs the exact latitude and longitude of the AP[10].

All this reconnaissance information helps a hacker gain unauthorized access to a wireless LAN or launch a DOS attack. A Service Set Identifier (SSID) identifies access points. Vendors usually default these names; for example, Cisco always uses tsunami, whereas Linksys defaults to linksys. Figure 2 confirms this, and as can be seen, *default* is a very common default SSID for the other access points. These access points were discovered because they are configured to send out a broadcast beacon. This beacon usually contains the access point's SSID, supported data rates, and whether it supports frequency hopping or direct frequency. Once a client wireless device knows the SSID, all that is needed to gain access to the wireless LAN is to guess on a valid IP address. Many times, a hacker need not even guess on a valid IP address, because users configure their

[10] Santalesa, Rich "The war over 802.11x security" July 10, 2001, http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2783681,00.html

access points to give out an IP address from a pre-defined pool without requiring any authorization. One of the access points discovered with Netstumbler happened to be approximately 200 meters away from my house. With no manual configuration of my Compaq WL110 card, I became part of my neighbors wireless LAN and was surfing the Internet within seconds of locking into their signal. (After my discovery, I proceeded to inform my neighbor of my findings and helped him with the proper configuration of his home wireless network).

Windows XP facilitates configuration of many devices, wireless NICs included. One can set up the wireless NIC to have Windows XP automatically configure it upon detection of a wireless LAN.

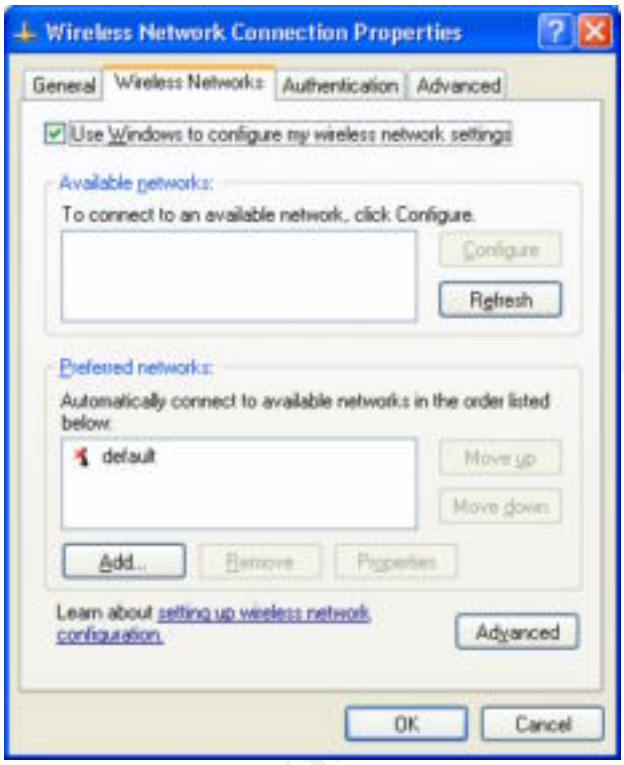

Figure 3. Screen capture of Wireless NIC configuration screen

Knowing the model of AP helps a hacker further investigate the features (or lack of) and any know vulnerabilities associated with the AP. Manuals can be freely downloaded from the Internet, which contains information on the pre-configured password to initially set up an access point.

Many times a hacker takes advantage of such WLANs to gain access to the Internet, at other times; a hacker may be seeking to gain unauthorized access to the wired network when they are having difficulty using the conventional access via the Internet.

If the Access point is configured with no access controls or security, a hacker can easily become a trusted device on the WLAN network, gathering information such as passwords to further gain access into an organizations' wired network.

Service Set Identifier (SSID), access control mechanisms and WEP all come standard with 802.11b standard access points. Unfortunately, these devices come pre-configured with default settings that make an access point vulnerable to attack.

To minimize the risk of unauthorized devices joining your WLAN, the SSID of an access point should be set to a meaningless name, therefore making it very difficult for hackers to join the WLAN, and the beacon broadcast should be turned off.

Access control mechanisms limit access to the access point based on a wireless device Media Access Control (MAC) addresses. Enabling this feature would make it difficult for unauthorized access to the WLAN network from devices that have guessed the SSID and assigned itself a valid IP address belonging to the WLAN network.

Making sure of the identity of the wireless device connecting to the access point is not a trivial task. Even though you filter wireless devices based on the MAC address, it doesn't help when there are WLAN cards that can be loaded with firmware that doesn't use the built-in MAC address. Anyone eavesdropping on the WLAN can spoof a valid MAC address and gain unauthorized access to the WLAN network.

Authorization alone cannot guarantee that your WLAN network is safe from hackers. Authentication mechanisms should be implemented hand in hand with authorization. Authentication mechanisms have not been implemented with the 802.11b standard. Cisco Systems, Microsoft and other organizations have jointly submitted a proposal to the IEEE for an end-to-end framework for 802.1X and the Extensible Authentication Protocol (EAP). 802.1X provides a standard for port based access control, whereas EAP allows client devices to communicate with different back-end authentication servers such as Radius[11].

Enabling WEP encryption will also reduce the initial impact on the wired network. Without encryption enabled, anyone with a wireless device and tool like Ethereal can passively monitor the wireless traffic and gain knowledge of the WLAN network and the LAN network as well. WEP comes with its' own vulnerabilities which we will touch upon in the next section. For organizations that do not require strict confidentiality of the data traveling over the airwaves, WEP along with 802.1X serves the purpose.

[11] Convery, Sean and Miller, Darrin "SAFE: Wireless LAN Security in Depth" http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

Albeit that most of these mechanisms are not considered strong security features, enabling them is sufficient enough to deter the casual intruder.

WEP

As mentioned earlier, WEP was developed to deploy an equivalent level of privacy to the wired LANs. WEP uses RC4 encryption algorithm, which is a symmetric stream cipher that supports variable length keys. The original standard was developed with 40-bit static encryption keys, and has already been cracked, a newer version of WEP now supports 128-bit static encryption keys, but on a busy network, and with the help of software like Airsnort, the 128-bit encryption keys have already been cracked in as little as 15 minutes. The plaintext itself is not run through the RC4 algorithm; instead the base key along with an initialization vector is run through the RC4 algorithm to produce stream cipher. The stream cipher is then XOR'd with the plaintext data to produce the cipher text data.

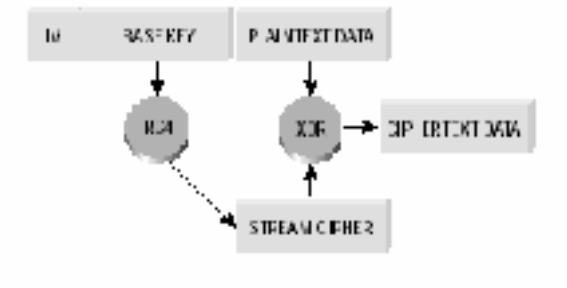

Figure 4. Wep Encryption Process[12]

One of the inherent weaknesses of WEP is that it uses an Initialization Vector (IV) to ensure that no two ciphertexts are encrypted with the same keystream. The IV is used to augment the shared key secret and produce a different key stream for each packet.[13] The IV is implemented as a 24-bit field which allows for 16,777,216 different possible values. Because of its size, the vector guarantees the reuse of the same key stream. For example, it has been noted that a busy access point, which constantly sends 1500 byte packets at 11Mbps, will exhaust all possibilities of the IV after 5 hours. This amount may be even smaller, since many packets are smaller the 1500 bytes.

11Mbps ÷ (1,500 bytes per packet x 8 bits per byte) = 916.67 packets per sec. (pps)
16,777,216 IVs ÷ 916.67 pps = 18,302.3509 seconds to use all IVS
18,302.3509 seconds ÷ 3600 seconds per hour = 5.084 hours to use all IVS

[12]Convery, Sean and Miller, Darrin "SAFE: Wireless LAN Security in Depth" pg. 46. http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm
[13] Borisov, Nikita, Goldberg, Ian and Wagner, David "Security of the WEP algorithm" http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Another weakness in the 802.11b standard is that it does not account for authentication and key management. Even if the RC4 encryption algorithm were stronger, the 802.11b standard does not provide a mechanism for dynamically changing or managing encryption keys. Since RC4 is symmetric, both the access point and the wireless device need to know the secret key. Manageability problems arise when an employee leaves an organization, requiring the WLAN administrator to change the secret keys on all the access points and each client wireless device to change the matching secret key on their device.

A short explanation of stream ciphers will help depict the vulnerability in the WEP protocol. A stream cipher is a process in which the entire stream is encrypted bit by bit by XORing the plaintext with the keystream. XOR returns 0 if the two bits are the same and 1 if the two bits are different. By applying the same algorithm to the ciphered text, one retrieves the plain text. If an eavesdropper intercepts two ciphertexts encrypted with the same keystream, it is possible to derive the XOR of the ciphertext. Having this knowledge, the hacker can enable statistical attacks to recover the plaintexts. Once one of the plaintexts becomes known, it is trivial to recover all of the others.

Following is an example of a passive attack to decrypt traffic. A hacker passively listens on the airwaves and intercepts all wireless traffic with a packet capturing software like TCPdump. Since the IV is transmitted in clear text, the hacker waits until an IV collision occurs. By XORing the two packets that use the same IV, the attacker obtains the XOR of the two plaintext messages. IP traffic is very predictable because it contains a lot of redundancy. This redundancy is used to eliminate many possibilities for the contents of the messages. The hacker can now begin to do statistical analysis on the data. If the statistical analysis is inconclusive, the attacker can look for more collisions with the same IV. Once the attacker is able to decrypt one message, the decryption of all future messages will follow. The following example shows how two ciphertexts using the same IV cancels out the keystream:

	Plaintext for the letter “x”	0111 1000
XOR’d	Keystream for the letter “n”	0110 1110
	---	---
	ciphertext for the letter “x”	0001 0110
	plaintext for the letter “y”	0111 1001
XOR’d	keystream for the letter “n”	0110 1110
	---	---
	ciphertext for the letter “y”	0001 0111

XOR’ing the ciphertext “x” with the ciphertext “y” produces the following result.

	Ciphertext “x”	0001 0110
XOR’d	ciphertext “Y”	0001 0111
	let’s cal this “z”	0000 0001

Now if a hacker has successfully retrieved the contents of one cipher text, let’s say he knows “x”, it would be very easy to retrieve the plaintext of another message that is using the same keystream.

Plaintext “x”	0111 1000
Unknown plaintext	
“z”	0000 0001

Using the rules of XOR, one can deduce that the unknown plaintext results to 0111 1001 which is the binary representation of plaintext “y”.

This is a simple representation of the inherent weakness in WEP. Hackers today are using tools like Airsnort to capture and decrypt WEP keys on the fly.

Supplemental Security Considerations

802.1X

The 802.11b standard did not provide for a strong authentication method and a method to distribute dynamic encryption keys. The proposed 802.1X standards try to address this weakness. When this feature is implemented, a wireless client cannot gain access to the network until the user performs a network logon. Both the client and the radius server perform a mutual authentication. The steps involved in this authentication is detailed below:[14]

1) A wireless client associates with an access point.
2) The access point blocks all attempts by the client to gain access to network resources until the client logs on to the network
3) The user on the client supplies a username and password.
4) Using 802.1X and EAP, the wireless client and a radius server on the wired LAN perform a mutual authentication. One of several authentication methods or types can be used. With the Cisco authentication type leap, the radius server sends an authentication challenge to the client. The client uses a one-way hash of the user-supplied password to fashion a response to the challenge and sends that response to the radius server. Using info from its user database, the radius server creates its own response and compares that

[14]. Convery, Sean and Miller, Darrin “SAFE: Wireless LAN Security in Depth” http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

to the response from the client. When the radius server authenticates the client, the process repeats in reverse, enabling the client to authenticate the radius server.
5) When mutual authentication is successfully completed, the radius server and the client determine a WEP key that is distinct to the client.
6) The radius server sends the WEP key called a session key over the wired LAN to the access point.
7) The access point encrypts its broadcast key with the session key and sends the encrypted key to the client, which uses the session key to decrypt it.
8) The client and access point activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session.
9) Both the session key and broadcast key are changed at a regular intervals as configured in the radius server.

Implementing LEAP provides 2 significant benefits. It eliminates "man-in-the-middle attacks" that are introduced by rogue access devices, because it requires both the client and the access point to authenticate, and enables centralized management of the encryption keys used by WEP.

Use of VPN and IPSec to further reduce the weaknesses in the 802.1X protocol

IPSec ensures confidentiality, integrity, and authentication of data across public networks such as the Internet. It can be equally applied against wireless networks as well. It provides confidentiality by encrypting the data with Triple DES (3DES) encryption algorithm. This algorithm encrypts the data three times with up to three different encryption keys.

IPSec would require that an IPSec client be installed on all wireless client devices and a tunnel would be built between the client and the VPN gateway.

Install a firewall to protect the wired LAN from the wireless LAN

Most organizations consider their LANS as trusted networks. The same cannot be said for WLANs. WLANs should be considered as public network, because they are easily accessible by the public. Another security extension that should be implemented with WLAN is a firewall sitting between the access point and the wired network. A firewall will allow explicit defined protocol through to the wired network, in the same way that a firewall protects the wired network from the Internet.

Recommended Best Practices for a Secure Wireless LAN infrastructure

Lock Down all Access points

Make sure all access points are configured with the broadcast beacon turned off and with an SSID that is difficult for anyone to guess. This helps mitigate the risk of being discovered by hackers searching for ill-configured devices.

Implement and Enforce a Strong Wireless Security Policy

A wireless security policy should be added to an organization's security policies to reduce the possibility of a security breach. The policy should include information on how to secure and lock down the Access points, enable WEP and authentication mechanisms and prohibit the creation of ad-hoc networks. To ensure compliance to the security policy, tools like Netstumbler can be used to do regular audits of the air space.

Employee awareness of the vulnerabilities of WLANs will also help enforce the Wireless Security policy. Many users are attracted to ease of use and deployment of wireless equipment and the promise of productivity gains that they do not take the time to realize the implications to an organization's wired network.

Implement Security Extensions when warranted

Depending on the level of privacy an organization needs on their wired network, security extensions should be implemented. Some organizations may find it sufficient to implement 802.1X to overcome the vulnerabilities in WEP, whereas other organizations may wish to implement IPSec to ensure the confidentiality, integrity and authenticity of the data over the wireless network. Weighing out the risks and costs of implementing security extensions will help an organization decide on whether to implement 802.1X or IPSec.

Conclusion

Even though WEP is not secure, the biggest problem with wireless networks is with users installing it without any control mechanisms. As can be seen from my wardriving experiment, the majority of access points did not have WEP enabled and are configured with factory default values. These ill-configured devices give hackers a wealth of information that they can use to gain unauthorized access to the wireless network. Everyone requires different levels of security. The majority of home networks can be secured by using the available security features that come with an AP. Organizations need to assess the cost of implementing a stronger encryption, authorization and authentication mechanism to secure wireless networks against the cost of losing valuable company information. Stronger security measures alone will not eliminate all the security risk introduced by wireless networks. No network will ever be secure enough, but user education and concise policies with regards to wireless networks will help reduce the proliferation of rogue access points within an organizations' network.

6.0 References

"5 Pratical Steps to Secure Your Wireless LAN" AirDefense Whitepaper

Borisov, Nikita, Goldberg, Ian and Wagner, David "Security of the WEP algorithm"
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Convery, Sean and Miller, Darrin "SAFE: Wireless LAN Security in Depth"
http://www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm

Craiger, J. Phillip, "802.11, 802.1x and Wireless Security" June 23, 2002
http://rr.sans.org/wireless/80211.php

Geier, Jim, "802.11 WEP: Concepts and Vulnerability"
http://www.80211-planet.com/tutorials/article/0,4000,10724_1368661,00.html

Hiller, Kimberly, "Wireless LANs: An Overview" July 3, 2001 Gartner Research

Janszen, Eric, "Understanding Basic WLAN Security Issues"
http://www.80211-planet.com/tutorials/article/0,,10724_953561,00.html

Milanesi, Carolina "Bluetooth and 802.1X: Competition or Coexistence ?" December 3, 2001 Gartner Research

Rolfe, Andy, "Wireless LAN Market for Strong Growth Through 2005" March 11, 2002, Gartner Dataquest Research Brief

Santalesa, Rich "The war over 802.11x security" July 10, 2001,
http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2783681,00.html

Stubblefield, Adam, Ioannidis, John and Rubin, Aviel D "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP"
http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf

Sutton, Michael, "Hacking the Invisible Network" July 10, 2002, Idefense paper

"WIRELESS LANs: Risks and Defenses" AirDefense Whitepaper