Global Information Assurance Certification Paper

History and Best Practices of Wireless Network Security

Thomas Stripling

GSEC Practical Assignment Version 1.4b, Option 1

January 14, 2003

Abstract

Due to a lack of understanding of the risks and countermeasures involved, the majority of today's wireless networks are running without adequate security measures. Since wireless LANs are fundamentally less secure than wired ones, this creates huge security problems for organizations that could be targeted by hackers. WEP, the de facto encryption and authentication standard for 802.11 networks, has been proven to be fundamentally insecure and the industry has yet to produce a viable alternative standard. Despite this, wireless networks can be made to securely interface with the corporate intranet by implementing a company-wide policy detailing the implementation and use of wireless devices. This paper delineates some common forms of risk associated with wireless networks and provides some recommendations for improving their overall security.

Introduction

Wireless networks (or Wi Fi as they are commonly called) are becoming more popular, and for good reason. They are convenient, inexpensive, and can increase productivity. However, wireless networks create a new genre of security risks – an area with which most administrators are unfamiliar. Since the signal in a wireless local area network (WLAN) isn't confined to the physical components that make up a wired LAN, it is much easier for intruders to monitor traffic, disturb the transmission of data, and break into the network. This is particularly worrisome for businesses with sensitive data for which security is paramount.

Approximately 70% of the wireless access points in the world are currently running without encryption, and 27% are still using the default settings that came with the hardware (6). This is comparable to not only forgetting to lock your front door, but leaving it wide open as well. The only thing preventing an attacker from getting into these networks is to locate them. This isn't as difficult as one might think. Wireless access points must advertise their existence by necessity, so anyone with a laptop and a $100 wireless LAN card that comes within range of an access point can easily discover a it (1).

History and Pitfalls

The Institute of Electrical and Electronic Engineers (IEEE) defined a standard called 802.11 for wireless devices. Since wireless networks are inherently less secure than wired ones, an optional data encapsulation technique called WEP was built in to the standard. WEP (Wired Equivalent Privacy) was designed to provide both authentication and encryption. It was touted as being able to provide the same level of security as a wired LAN (11). However, it had some serious drawbacks.

The first problem with WEP was the overhead required to run it. Running WEP encryption can reduce bandwidth by 1 to 2 Mbs (8 page 342). This may not seem like much, but it produced a noticeable drop in performance in the wireless products of the time and as a result many products simply did not implement WEP at all. However, "when it became clear that wireless networks unprotected by WEP were extremely vulnerable, users were urged to select products that implemented WEP, and WEP became the linchpin of 802.11 network security" (1). Many companies still did not implement WEP, but those that did saw themselves as secure.

The second problem with WEP was the key length. Originally, WEP secret keys were limited to 40 bits due to U.S. government limitations on the export of products with longer keys (1). Unfortunately, this also made WEP keys much easier to crack than other forms of encryption, shortening the amount of time

before it was necessary to change keys. However, updating the keys had to be done manually on each access point and radio NIC (2). On larger networks, this made continually updating the secret keys prohibitively expensive. As a result, companies would often either not use WEP at all or "maintain the same keys for weeks, months and even years" (2). Currently, WEP is available with 128 bit keys, which take longer to crack.

The final blow to WEP came when Fluhrer, Mantin, and Shamir found a flaw in RC4, the encryption algorithm that WEP relies on. Because of the way WEP uses RC4, it became possible to recover the WEP secret key simply by collecting a sufficient number of packets (9). Depending on traffic load, gathering enough packets can be done within a single day (1).

As it became clear that WEP was "unsafe at any key length", the 802.11 working group adopted the 802.1x standard to provide authentication for wireless networks. 802.1x was designed for wired networks to require port-based user authentication before granting network access (1). These networks then had to rely on other encryption methods, such as IPSec, SSL, or SSH.

802.1x doesn't provide the actual authentication mechanisms, but rather relies on a protocol called EAP (Extensible Authentication Protocol) that resides on the authentication server and within the software on the client devices (2). Since no part of the authentication scheme lies on the access point itself, companies can update the EAP authentication type without changing the hardware.

The problem with using 802.1x for a wireless network is that it was "designed for a network with a fixed physical topology" (1). On a wired network, authentication is implicit in the connection to the network itself, and altering traffic as it traverses the wire is difficult and requires physical access to the company premises. On a wireless network, "it is much easier to inject messages into an authentication sequence or hijack authorized sessions in the absence of strong mutual authentication and integrity checks" (1).

Since there are no current standards that provide a total solution to the problem of wireless security, the IEEE is the process of defining a new one that will provide both authentication and encryption. 802.11i takes 802.1x as its base and adds several features for wireless networks, including the use of the AES encryption algorithm and a key distribution framework (1). Since AES uses a 128 bit key and has not yet been broken, it will not be possible to break the encryption just by listening to network traffic. Also, the inclusion of a key distribution framework makes it possible to dynamically update the keys without manually configuring each device, making it feasible to scale an 802.11i wireless network to many more users than was previously possible.

Unfortunately, 802.11i will not be fully approved as a standard until late 2003, which means that devices incorporating the standard may not start appearing

until 2004. In the meantime, the non-profit WiFi Alliance (the consortium behind interoperability standards and testing for 802.11-based networks) has created a temporary solution until 802.11i comes along. WPA (WiFi Protected Access) is a subset of 802.11i and is forward compatible with it. It will work similarly to an 802.1x network, using EAP for authentication to a server of some sort and using WPA for encryption (7). Furthermore each user has a different key and the keys are refreshed for each connection.

Since WPA is based on an unfinished standard, it will be missing the parts of the standard that "require a hardware upgrade or aren't ready, such as secure fast handoff, secure de-authentication and disassociation, and AES-CCMP enhanced encryption" (7). This could cause several problems, such as what happens when a machine is no longer allowed access to company resources in the case of theft or termination of employment. These cases will still have to dealt with manually. WPA will still be, however, the best choice for the overall security, manageability, and upgradeablity of a wireless network until 802.11i is released.

Commercial Solutions

There are several commercial products available that will increase the security of WLANs. These range from comprehensive, end-to-end solutions that attempt to incorporate all aspects of wireless security to smaller products that try to secure a particular issue. Unfortunately, like nearly all commercial security solutions, they can be very expensive and many companies simply cannot afford them.

One product, StillSecure Border Guard by Latis Networks, is a replacement for an Intrusion Detection System (IDS) for a wireless network (10). While an IDS is passive in the sense that it will only send out an alert when an intruder is detected, Border Guard won't let unauthorized users or machines on the WLAN in the first place. Border Guard actively detects wireless devices that come within range of any of the access points in the network, thus helping to prevent unauthorized snoopers.

The trouble with wireless devices, however, is the relative ease of spoofing the Media Access Control (MAC) address, which access points use to identify wireless devices. It does no good to only allow "authorized" MAC addresses if a hacker can easily change his MAC address to match one that has been approved. Furthermore, the Border Guard Wireless application costs $1,000 for the first network server and $2,500 for each additional one, and that's for the software alone (10).

Internet Security Systems offers a more comprehensive solution, including deployment, monitoring, updates, and emergency response (12). Their array of products include:

- *Internet Scanner*, a network vulnerability assessment product that probes networks to detect unauthorized or poorly configured wireless access points.

- The *RealSecure Protection System*, which is deployed between a wireless access point and the corporate network and helps to recognize and react to attacks.

- Managed Security Services, including network assessments and remotely managed intrusion protection services.

- Consulting and Education services that can help companies better understand their risks and how to manage them.

Of course, these services do not come without their price tag. They are effective and for some the peace of mind is well worth the cost, but for most companies a solution like this is completely out of the question.

Risks

The risks involved in maintaining a wireless network are somewhat more extensive than with a wired network due to nature of the transmission medium. Since network traffic is not confined to a wire, it is difficult to know who is connected and hard to secure the transmission against tampering. What follows is a list of several possible types of attack:

Insertion Attacks
An insertion attack is described as "deploying unauthorized devices or creating new wireless networks without going through security process and review" (12). There are two main types of insertion attacks:

- Unauthorized Clients – An attacker tries to connect an unauthorized wireless device to an access point. On access points that don't use any kind of authorization scheme, this is as easy as coming within range (12).
- Unauthorized Access Points – A wireless access point is connected to the internal network without company approval. This could be done by an attacker wishing to grant himself access or by an employee that doesn't understand the risks involved (12).

Interception of Wireless Traffic
In a wired network, an attacker must either be physically connected to the network or have already compromised a machine on the network to monitor traffic. Wireless traffic, on the other hand, can be monitored by anyone within range. 802.11b (a type of 802.11 wireless network) transmissions are advertised as working up to 300 feet, but what most users don't realize is that the use of equipment such as directional antennas can dramatically increase that range.

The range of access points almost always extend beyond the territory they are intended to cover, and the signal can be intercepted outside buildings or on a different floor of the same building (12). There are several methods of intercepting traffic:

- Wireless Packet Analysis – An attacker captures unencrypted wireless traffic or decrypts encrypted traffic and reads packets from the initial connection of legitimate clients. These packets include the username and password of authorized users, allowing the attacker to sign on to the network (12).
- Broadcast Monitoring – Poor network configuration can have potentially nasty results. If an access point is connected to a hub rather than a switch, any network traffic across that hub can be broadcast out the access point. Thus, an attacker could listen to sensitive data not even intended for the wireless network (12).
- Access Point Clone – By setting up an unauthorized access point (see above) within range of the wireless network, an attacker can coax authentic wireless clients to connect to his network rather than the company WLAN. When users attempt to log into the fake access point, they can unknowingly give away passwords and similar sensitive data (12).

Jamming

Denial of Service (DoS) attacks also become easier over wireless networks. Since wireless networks operate over a particular frequency (2.4 GHz for 802.11b), an attacker can simply flood that band with useless noise or static, causing the wireless network to become unusable. Additionally, cordless phones and even baby monitors can send out signals on the 2.4 GHz range, degrading the overall signal (12).

Client-to-Client Attacks

Two wireless devices don't need an access point to talk directly to each other, and so even if the access points are secure, an attacker can get into the network by compromising an insecure client and using it to bypass the secured access points (12).

- File Sharing and Other Services – Wireless clients running certain services, such as a web server or file sharing can leave themselves particularly vulnerable (12). Users will often not realize that they can be at risk even when they are not in range of an access point as long as they have a wireless card enabled. Compromised machines can then be used to gain access to the corporate intranet at a later time.

Brute Force Attacks

Most access points use a single password that is shared with all connecting wireless clients. Unless this is changed frequently, a brute force attack could

uncover the password simply by trying all possible passwords. Additionally, attackers can search for combinations of known words and numbers to make the passwords easier to crack (12).

Attacks Against Encryption

As mentioned above, WEP is the de facto standard for 802.11 devices and it has been proven to be insecure. Access points that rely on WEP as their only means of security can be broken into within a day of monitoring the network (12). There are even tools available that do all of the work, so that the knowledge an attacker needs is minimal.

Misconfiguration

Many access points are shipped in an insecure configuration in order to allow neophyte users to set them up with ease. Unless administrators understand the risks associated with wireless networks and properly configure each unit prior to deployment, they will be leaving the door wide open for anyone within range to connect.

- Server Set ID (SSID) – The SSID is what identifies access points so that clients can connect. An attacker that knows the SSID will have a much easier time breaking into the network. Since the default SSIDs for different brands of access points are well known, it is vital that they be changed prior to deployment (12).
- WEP – Although WEP can be broken by a determined attacker, using it is much better than running without any encryption/authentication at all. Typically, wireless products are shipped with WEP turned off (12). Enabling WEP with 128 bit keys can deter casual attackers and provide the network with at least a layer of protection.
- SNMP Community Passwords – Many wireless access points run SNMP agents. If the community password is not configured prior to deployment, then an attacker that knows the default can connect and potentially write data to the access point (12).
- Configuration Interfaces – Different models of access points have different methods available to configure them. These include SNMP, serial, telnet, and Web servers (12). It is important for administrators to be aware of the different interfaces and protect them. (For example, don't leave the access point in a common area where a visitor could connect to it with a serial cable.)
- Client Side Security Risk – Clients connected to a wireless access point store the SSID of the access point and the WEP key locally. If the clients are not properly secured, an attacker could steal this information and use it to connect to the corporate network (12).
- Installation – Access points that are installed in insecure locations can be vulnerable to physical tampering. For instance, some access points have a reset button that will restore it to the factory default (insecure) settings (12).

Best Practices

Fortunately, the risks involved in operating a WLAN can be dramatically reduced though good practices and a competent network security team. Each of the risks mentioned above can be diminished by careful administration.
The goal of any complete wireless security policy is to ensure(8 p 11):

- Confidentiality – Controlling access to sensitive data
- Authentication – Validating a user's identity before allowing them access
- Integrity – Ensuring that data traversing the network has not been tampered with
- Access Control – Ensuring that users only see information for which they are authorized
- Theft and Employee Termination – Centrally disabling devices when the device falls into the hands of an unauthorized user

What follows is a checklist of important steps for securing your organization.

Wireless Security Policy
The company's security policy, procedures, and best practices should include wireless networking as a part of the overall security management architecture, and should clearly delineate what is and is not allowed with wireless technology (12). This should include access point configuration, installation, and placement in the network topology as well as authentication/encryption mechanisms and a method for centrally disabling unauthorized devices (5).

Activate WEP
At the very least, WEP should be enabled on wireless access points. As mentioned above, WEP has a fault that makes it inherently insecure, but enabling it will deter many attackers, making them turn elsewhere to break into an easier network. For a network with a low risk of attacks, enabling WEP is a minimum (3). For higher-risk networks, the use of other options is a better solution, such as using an 802.1x-based network with EAP for authentication and IPSec, SSL, or SSH for encryption. 802.11i will have 128 bit encryption built into it when it comes out, and WPA will also include support and will be out somewhat sooner. To use these technologies, organizations must purchase WPA-compliant devices.

Create Access Lists
Compile a list of MAC addresses that have permission to access the network. Keep the list up to date, removing entries that, due to termination or loss, should no longer have access to company resources. An access list is not a foolproof authentication scheme, since it is relatively easy to change the MAC address of some wireless devices, but it makes it more difficult for attackers to proceed. Additionally, if the number of users is very large, this can require significant administration overhead and may not be possible to implement.

Utilize Dynamic Key Exchange Mechanisms
802.11i will include support for dynamic key exchange mechanisms, but until it is finalized, organizations will have to rely on vendor-specific technologies (3). The best policy is to check with the vendor before buying any hardware to determine its capabilities.

Keep Firmware Up-to-Date
Patches to firmware often include security fixes. Upgrade the firmware on a product soon after pulling it out of the box. Then, be sure to check regularly for updates and install them if there are any (3).

Properly Install Access Points
Access Points should be installed out of sight above ceiling tiles or high up on a wall where they cannot be easily tampered with. An access point that is within easy reach of a visitor could be reset via a button (in some cases) or the console port (in others). Alternatively, a visitor could simply swap the secured access point for an identical one that allowed him access (3).

Disable Access Points During Non-Usage Periods
If possible, shut down the access point when users will not be connecting to them. This will limit the window of time an attacker would have to break in and also force him to do his work during the work hours, when he can be more easily spotted. With just a few access points in a WLAN, simply pulling the power plug will work. With a larger network, consider using Power-over-Ethernet (PoE) equipment that allows you to power down all the access points centrally (3).

Assign Strong Passwords to Access Points
Never leave the factory default password on any device, wireless hardware included. They are all well known, making it easy for attackers to change the configuration of the access point. Also, be sure to change the passwords regularly and ensure they are encrypted if sent over the network (3).

Change the SSID
Changing the default SSID that comes with the hardware is important as well. SSID defaults are also well known and can be guessed easily if not altered. This will only protect a system from idle snoopers, however, as the SSID is always sent out in 802.11 association frames, which allow users to connect (3).

Don't Broadcast SSIDs
Most devices broadcast the SSID by default to anyone within range so that wireless devices will know they are in range of an access point and can connect to the network if they wish. Turning this feature off will help to discourage the feint of heart from penetrating the network. The SSID is always sent out in association frames when a user first boots their wireless device, but it takes more work to recover it if it is not being broadcast (3).

Reduce Propagation of Radio Waves Outside the Facility
Through the use of directional antennas, it is possible to direct the area of coverage for an access point to the interior of the facility and reduce the area outside the facility from which the network can be attacked. This can optimize coverage as well as diminishing the effectiveness of several of the attacks listed above, including interception and jamming (3). If an attacker must be inside or very near to the building in order to connect to the WLAN, it increases his chances of detection and makes breaking into the network less worth the risk.

Deploy Access Controllers
Access Controllers interface with an authentication server and provide strong access control to the network (3). There are many commercial solutions available, such as ReefEdge (13), Bluesocket (14), and Nomadix (15). For administrators on a budget, a similar effect can be obtained by using an 802.1x-capable network with EAP and an authentication server. 802.11i and WPA networks will also be able to be configured this way.

Implement Personal Firewalls
Installing personal firewalls and disabling file sharing and other services for WLAN users will prevent the client-to-client attacks described above, as well as protect user machines if an attacker does manage to compromise an access point (3).

Use a Virtual Private Network (VPN)
For the encryption of sensitive data, implementing a VPN using IPSec or similar technology is the best way to ensure confidentiality. This requires the installation of VPN software onto each user's machine, however (3). 802.11i and WPA will include support for 128-bit encryption when they are released.

Utilize Static IP Addresses for Clients and Access Points
Dynamic Host Configuration Protocol (DHCP) is a convenient way to assign IP addresses and it is tempting to install it on wireless access points. Using it, however, makes it much easier for an unauthorized user to connect to the WLAN (3). Static IP addresses produce yet another roadblock that an attacker must overcome before he gains access.

Control the Deployment of WLANs
Ensure that any installation of a wireless access point is coordinated with the appropriate administrators. Forbid the installation of unauthorized access points in the company's security policy (3). Regular security audits should be performed to ensure that existing wireless access points are in conformance with regulations (12).

Treat Wireless Stations as Untrusted
Access points need to be identified and evaluated on a regular basis to determine if the configuration of each is secure. This determination should include appropriate placement of firewalls and the use of VPNs, IDSs, and authentication (12). If at all possible, all access points should be placed outside of a firewall that will only allow VPN traffic to pass. Thus, all traffic between the wired and wireless network would take place through a VPN tunnel and would therefore be encrypted.

Monitor for Unauthorized Access Points
There are several methods of finding unauthorized or "rogue" access points. The cheapest is to simply walk though the facility with a wireless device using a WLAN sniffing tool, such as AirMagnet, AiroPeek, or NetStumbler (5). Keep a list of authorized access points and compare it to the ones that you find. Track down any suspicious access points by measuring the signal strength of the point and following in the direction it increases. If you find an unauthorized access point that is connected to the corporate network, immediately shut it off (11).

With larger wireless networks, the "walk-through" method isn't feasible. In these cases, use a centralized detection scheme. This method uses a central console attached to the wired side of the network and maintains a list of authorized access points. These access points then listen for rogues that come within range. If a rogue access point enters the area covered by any of the existing points, the system alerts security personnel (11).

As an alternative, there is an inexpensive albeit fairly crude approach for finding potential rogues. Since nearly all access points maintain a Web interface, the use of a port scanner can detect most rogues by looking for devices listening on port 80 (HTTP). This will unfortunately uncover a large amount of false-positives as well, including all Web servers and some printers (11).

Conclusion

There is no such thing as perfect security. Rather, every security measure can be seen only as a deterrent, not as absolute prevention. Following these steps will not ensure that a network will not be attacked or broken into, but it will drastically reduce the risk of such a break-in. Wireless networks can be extremely useful and can dramatically increase productivity in some environments. If used correctly, they can be made as secure as the rest of the corporate network.

References:

1. Gast, Matthew. "Wireless LAN Security: A Short History." 19 April 2002. URL: http://www.oreillynet.com/pub/a/wireless/2002/04/19/security.html (14 Jan 2003).

2. Geier, Jim. "802.1X Offers Authentication and Key Management." 7 May 2002. URL: http://www.80211-planet.com/tutorials/article.php/1041171 (14 Jan 2003).

3. Geier, Jim. "The Guts of WLAN Security Policy." 12 Nov 2002. URL: http:// www.80211-planet.com/tutorials/article.php/1499151 (14 Jan 2003).

4. Geier, Jim. "Identifying Rogue Access Points." 6 Jan 2003. URL: http:// www.80211-planet.com/tutorials/article.php/1564431 (14 Jan 2003).

5. Geier, Jim. "Wireless LAN Security Assessments Steps." 20 Nov 2002. URL: http://www.80211-planet.com/tutorials/article.php/1545731 (14 Jan 2003).

6. Griffith, Eric. "Mapping the Lack of Security." 25 Oct 2002. URL: http://siliconvalley.internet.com/news/article.php/1488541 (14 Jan 2003).

7. Griffith, Eric. "New Protection for 802.11." 31 Oct 2002. URL: http://www.80211-planet.com/news/article.php/1491771 (14 Jan 2003).

8. Nichols, Randall K., Panos C. Lekkas. Wireless Security. New York: McGraw-Hill, 2002.

9. Stubblefield, Adam, John Ioannidis, Aviel D. Rubin. "Using the Fluhrer, Mantin, and Shamir Attack to Break WEP." Revision 2. 21 Aug 2001. URL: http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf (14 Jan 2003).

10. Wagner, Jim. "Wired Security Mentality for WLANs." 18 Nov 2002. URL: http://www.80211-planet.com/news/article.php/1502271 (14 Jan 2003).

11. "WEP." 5 Aug 2002. URL: http://www.pcwebopaedia.com/TERM/W/WEP.html (14 Jan 2003).

12. "Wireless LAN Security – 802.11b and Corporate Networks." 2001. URL: http://documents.iss.net/whitepapers/wireless_LAN_security.pdf (14 Jan 2003).

Additional Information:

13. http://www.reefedge.com
14. http://www.bluesocket.com
15. http://www.nomadix.com