Global Information Assurance Certification Paper

Wireless and Moneyless

Ryan Blake

GSEC Version 1.4b

February 20, 2003

Abstract

Wireless networks have recently become a topic of much discussion. Employees enjoy the freedom and independence associated with wireless. An employee with a wireless enabled laptop has the freedom to move around the building with the same ability to access the network resources as he/she would have sitting at their desk. On the other hand, security personal have been reluctant to implement wireless networks because of the security concerns associated with them. These security concerns have been further perpetuated by the inexpensive cost and ease of installation. Many workers feel that if the IT Department and/or management will not provide wireless networks, the employees will buy there own. This attitude compromises the overall security of the corporate network. The average user does not realize the "actual" cost to secure and implement a proper wireless local area network (WLAN). This case study covers two months of research, risk analysis, implementation, and improvements of a WLAN installation. This is not to be taken as a step by step approach to solve all security issues associated with WLANS. This is merely a study of how one organization met the challenge of deploying a reasonably secure WLAN with virtually no capitol.

Background

The organization that I work for is of a political nature and is a Constitutional State Agency. Therefore, to protect it's identity it will be referred to in this paper as the "Agency".

The Agency employs approximately 200 people in one centrally located office building that also houses other Governmental Agencies. The grounds are monitored by security however, a person could gain relatively close access to the external perimeter of the building. The Agency handles confidential information such as banking accounts, social security numbers, health care information, and personal employee data. Due to the information that our systems contain, we are bound by regulatory acts such as the Health Insurance Portability and Accountability Act (HIPAA) and the Gramm-Leach-Bliley Act (GLBA). Therefore, we must be able to provide a certain level of security and ensure that data is not compromised. My job, as the Information Security Officer, is to create a secure environment to protect our information assets.

Before

Wireless technology is increasing in popularity, mainly because of the decrease in cost and the ease at which it can be installed. In my office, wireless was not "officially" used. I knew that there were some instances of limited use but, wireless was not supported by the helpdesk.

In an effort to intertwine security with new technology, the Governor's Office of Technology mandated each agency to create a Wireless Information Technology Security (WITS) group. Each Agency's WITS group would be responsible for recommending, designing and maintaining a secure wireless network.

After the creation of this group, our WITS team tried to gain as much information as possible about the current, unauthorized wireless use. The first step of the evaluation process was to gain a thorough knowledge of the wireless assets that were owned and operated by the Agency. Table 1 details our findings.

Table 1: Wireless Asset Inventory

Wireless Asset Inventory				
Asset Type	**Quantity**		**Brand**	**Type**
	Authorized*	**Rogue±**		
Access Points	3	2	Linksys	N/A
Wireless NIC's	0	3	Linksys	USB
Integrated Wireless NIC's	85**	0	Orinoco	N/A
*Authorized by Administration (not ITS) **All integrated Wireless NIC's were authorized but disabled ±Anything not approved by ITS or Administration				

As the table shows, many employees are equipped with laptops that have integrated 802.11b wireless Ethernet cards. These cards are disabled by the IT networking group, before they are deployed, as part of the installation process. This provides only a minor roadblock because more experienced users can easily re-enable their wireless cards. The table also shows that there are three rogue USB wireless network interface cards (NICs) in use. After further investigation we determined that the administrational arm of the agency had previously purchased three Linksys wireless access points to use in the conference rooms for outside vendors to have the ability to connect to the internet for presentational purposes. All of the information in the Asset Inventory Table labeled "Authorized" was collected from the Agency Asset Management software and was purchased with Agency dollars. The equipment marked as "Rogue" was found during visual site inspections and was purchased by employees. It is important to understand that more rogue wireless devices are likely to exist.

After a meeting between the WITS group and the Executive Management of the Agency we collectively determined that simply "pulling the plug" on the

wireless network would not be a sufficient solution. The people, within the Agency, that had been using the WLAN did not want to see it dismantled. We also determined that there was a significant need to pursue a secure WLAN implementation. The next step would be to evaluate our options and make a recommendation to the Executive Management.

During

Once the WITS group had received approval from management, we began to evaluate the risks associated with wireless and the steps needed to implement a secure WLAN. WITS decided to take a risk management approach to identifying threats and vulnerabilities. Table 2 shows the risk metrics used to determine our top vulnerabilities.

Table 2: WITS Risk Metric

Risk Metric			
Issue	**Threat**	**Vulnerability**	**Risk**
Bandwidth Theft	Low	Low	Low
Data Loss	Medium	High	High
E-mail Theft	Medium	High	High
Loss of Confidential Data	High	Medium	High
Political Embarrassment	High	High	High
No Wireless Security Policy	Medium	Low	Medium
Denial of Service attacks	Medium	High	High
Loss of Proprietary Information	Low	Low	Low
Ad-hoc Mode	Medium	High	High

The WITS group listed our top vulnerabilities in the Table above. The biggest fear was the possibility of an attacker being able to access the scores of confidential data that resides on the Agency's wired network. Another concern was the confidentiality of the Agency's email that was being transmitted across the airwaves. The compromise of either the email system or confidential data would be political suicide for the agency's elected official and could cost all of us our jobs.

Another security issue stems from the mode of operation. Wireless equipment conforming to the 802.11b standard has the ability to operate in two modes, infrastructure and ad-hoc. Infrastructure mode is the most common. This is when a wireless client uses an access point to connect to a shared resource and exchange data. Ad-hoc is a lesser used mode of operation. Ad-hoc mode allows wireless enabled computers to communicate directly without the aide of an access point. Operation in ad-hoc mode can reveal the entire hard drive to an attacker who also has his wireless card in ad-hoc mode and is located within several hundred feet of the unsuspecting target. Adding insult to injury, some wireless manufactures ship their network cards in ad-hoc mode by default! This peer-to-peer communication introduces a new vulnerability that the WITS group must address in order to create a secure wireless network.

After reviewing the Risk Metric the WITS group decided that the two main features needed for a secure wireless implementation were authentication and encryption. The wireless client needed the ability to authenticate to the network before sending data and the data that flowed between its residing server and the client needed to be encrypted. We reviewed the Linksys AP's that we already had and found that there is no support for authentication. It was also discovered that the available encryption came in two flavors, 64 and 128-bit wired equivalent privacy or WEP. WEP is turned off by default and is inherently flawed. WEP uses an integrity check field to insure that the packet has not been modified in route and an initialization vector (IV) to augment the shared secret key and produce a different RC4 (encryption algorithm) key for each packet. The improper implementation of these measures contributes to the poor security associated with WEP.

Because we are mainly a Cisco shop we decided to turn to them for a solution. We began by looking into the Aironet Series client cards and access points. In doing so, we discovered the LEAP protocol. LEAP is Cisco's lightweight version of the Extensible Authentication Protocol. LEAP requires mutual authentication using shared secrets.

Table 3 (below) shows a comparison between WEP and Cisco's LEAP. This table was taken from the "Wireless LAN Security in Depth" whitepaper by Sean Convery and Darrin Miller. As you can see, LEAP and WEP are similar in many ways. They both use 128-bit key lengths and use the RC4 encryption algorithm. For message integrity both LEAP and WEP use the cyclic redundancy checksum (CRC32) and the message integrity check (MIC). Using MIC will keep attackers from employing a common technique of "bit-flipping" to uncover the encryption key. Cisco offers a warning that using MIC can reduce throughput by up to 80%, making it unsuitable for some applications.

Although similarities exist, there are several key differences that make LEAP superior to static WEP. One major difference is in user authentication. LEAP

uses the Cisco Secure Access Control Server (ACS) to verify usernames and passwords before permitting access to the wired network.

> *The Cisco Secure ACS is a high-performance, highly scalable, centralized user access control framework. Cisco Secure ACS offers centralized command and control for all user authentication, authorization, and accounting from a Web-based, graphical interface, and distributes those controls to hundreds or thousands of access gateways in your network. With ACS you can manage and administer user access for Cisco IOS® routers, virtual private networks (VPNs), firewalls, dial and broadband DSL, cable access solutions, voice over IP (VoIP), Cisco wireless solutions, and Cisco Catalyst® switches via IEEE 802.1x access control. (Cisco Secure, 1)*

The only user authentication available with WEP is MAC address filtering, which is easily spoofed. Other advantages of LEAP include per users keying and time-based key rotation. Each time a user authenticates to the access point the client is given a unique encryption key, this key is used for a specified time and then it is changed. Even if an attacker did uncover the encryption key, it would change before much information was divulged.

Table 3: Wireless Encryption Technology Comparison

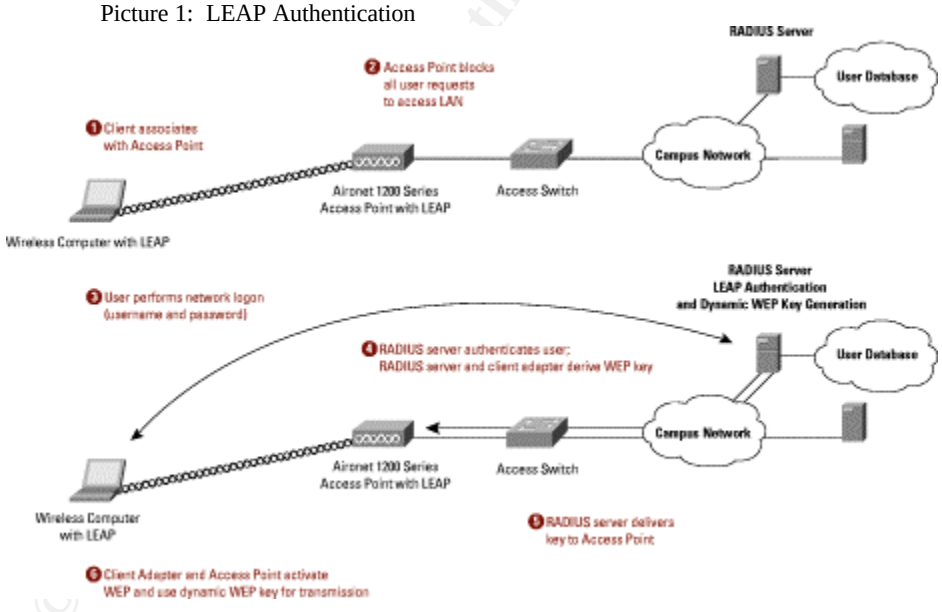
	LEAP	IPSec	Static WEP
Key Length (bits)	128	168	128
Encryption Algorithm	RC4	3 DES	RC4
Packet Integrity	CRC32/MIC	MD5-HMAC/SHA-HMAC	CRC32/MIC
Device Authentication	None	Pre-shared secret or Certificates	None
User Authentication	Username/Password	Username/Password or OTP	None
User Differentiation *	No	Yes	No
Transparent user experience	Yes	No	Yes
ACL requirements	None	Substantial	N/A
Additional Hardware	Authentication Server	Authentication Server and VPN Gateway	No
Per users keying	Yes	Yes	No
Protocol Support	Any	IP Unicast	Any
Client Support	PCs and high-end PDAs. Wide range of OSs supported from Cisco	PCs and high-end PDAs. Wide range of OSs supported from Cisco and Third-Party Vendors.	All clients supported
Open Standard	No	Yes	Yes
Time-based key rotation	Configurable	Configurable	No
Client hardware Encryption	Yes	Available, software is most common method	Yes

Additional Software	No	IPSec client	No
Per-flow QoS Policy Management	At access switch	After VPN gateway	At access switch

The following picture (Picture 1) from the "Cisco Aironet Wireless LAN Security Overview" paper shows how the client adapter, access point, and access control server work to authenticate the user. First, a wireless computer with LEAP associates with a LEAP enabled Cisco access point. The access point blocks the client machine from accessing the wired LAN. The user is then prompted to enter their logon credentials. After successful authentication, the RADIUS server and the client card derive the initial WEP key. Communication between the client and the wired network begins.

There were a couple of problems with the Cisco solution. Since LEAP is a proprietary version of the EAP protocol we would have to replace all of the integrated wireless network interface cards that came with the laptops with Cisco brand cards. This interoperability issue would increase the cost by approximately one hundred fifty dollars per user. Though cost was already an issue, replacing the network cards significantly increased the overall cost. However, the benefit of utilizing the Cisco equipment far out weighed the expense of implementation.

Picture 1: LEAP Authentication



After reviewing Cisco's wireless equipment and suggested implementation we were ready to present our recommendation to the Executive Management. The WITS team's preferred solution was to use Cisco equipment. The Cisco Aironet 350 series client adaptor, the Aironet 1200 series Access Point, and the Cisco ACS server would be recommended. All three support 802.1x authentication types, including Cisco's LEAP. 802.1x is a port-level access control standard for network security." Cisco Secure Access Control Server (ACS) would be used for user management and authentication.

The WITS group took the proposal to the Executive Management. Then they hit us with a curveball. We were told that there was not enough general revenue funding to purchase the Cisco Solution. We were also told that any solution we proposed would have to make use of the current wireless equipment and that no new equipment purchases would be permitted. We were informed that with the financial position of the state and the budget cuts in affect, there would not be any purchases for this type of equipment for at least 3 years.

We knew that we had to find a viable solution for new equipment without a budget. After several meetings within the WITS group we came to a unanimous decision, complete segregation! The wireless access points would be setup on their own network, completely separate from the wired network. Under an existing contract we could order a 1.5 megabyte pipe from our cable internet provider (we already had suitable cable drops) for $45 per month. Because this was a purchase that would be added to a pre-existing account, we were not bound by the budget restrictions. We would then connect our wireless AP's to the cable connection and require all employees, who have a true business need for wireless, to use this connection. If the mobile employee needed to access the wired network, they would be required to connect using the existing VPN solution. This provides a form of authentication and encryption for the Agency's wireless network.

We also took the appropriate and necessary steps to "lock down" the wireless AP's. We followed and expanded on Konstantinos Karagiannis' article in PC Magazine entitled "Ten Steps to a Secure Wireless Network". Karagiannis' ten recommended steps are as follows:

1. Control Broadcast area.
2. Lock Each AP.
3. Ban rogue access points.
4. Use 128-bit WEP.
5. Use SSIDs wisely.
6. Limit access rights.
7. Limit the number of user addresses.
8. Authenticate users
9. Use Radius.
10. Call in the big boys.

The steps that we actually used when installing our wireless equipment are listed below.

1. MAC address filters are used to limit the computers that connect to the AP.
2. Wireless users must register their MAC address with the WITS group to be allowed access to the APs.

3. Enable 128-bit WEP. We will rotate four different WEP keys based on an easy to remember formula.
4. The number of available DHCP addresses will be limited to the number of authorized wireless users. If any authorized user could not access the AP because of a lack of DHCP addresses, we would know that an unauthorized user has accessed the AP.
5. The default SSID was replaced with a cryptic SSID that did not divulge any ownership information.
6. SSID broadcasting was disabled.
7. Default password changed to a strong password that made use of the mixed case characters A-Z, numbers 0-9, and characters such as !,@,#, etc.
8. Installed the APs in places where their signal leakage was minimized.

The final step taken was to require that all laptops have an Agency approved personal firewall installed and configured by the helpdesk. Wireless network cards have the ability to operate in ad-hoc mode. Ad-hoc mode allows wireless clients to communication without the use of an access point. This peer-to-peer communication could expose sensitive data stored on the hard drive. The personal firewall would block this type of communication and mitigate the risk.

It is important to understand that following the above steps will not keep a determined hacker out, but it will make it more difficult to obtain access.

After security measures were put in place the WITS group wrote a comprehensive Wireless Security Policy. This policy detailed acceptable use, monitoring, expectation of privacy, and user awareness. The Wireless Policy was then molded to fit into our existing security program. We also provided user training that showed live demonstrations of a hacker attacking an improperly configured wireless computer. This provided a deeper level of user awareness which is the key to any security program.

After

The Agency WLAN now has a reasonable level of security. All critical data is accessed using a VPN which requires authentication and provides encryption. The APs have been "hardened" to prevent accidental or intentional access by the average person or "war driver" and to make it more difficult for a hacker to connect to. We have also implemented a wireless security policy to establish guidelines for accessing the WLAN. Table 4 shows the WITS Risk Mitigation Metric.

Table 4: WITS Risk Mitigation Metric

Risk Mitigation Metric	
Issue	**Mitigation Procedure**
Bandwidth Theft	Segregation of Network
Data Loss	Encryption Through VPN

E-mail Theft	Encryption Through VPN
Loss of Confidential Data	Encryption Through VPN
Political Embarrassment	Encryption Through VPN
No Wireless Security Policy	Implement Policy
Denial of Service attacks	Segregation of Network
Loss of Proprietary Information	Segregation and Encryption
Ad-hoc mode	Personal Firewall

The issue of bandwidth theft and denial of service (DoS) attacks have been mitigated by segregating the wireless network from the wired network. There are no mission critical applications running on the wireless network. If an attacker does leverage a DoS attack on the wireless network, we will power down the AP and advise the users to switch to the wired network. This is feasible because of the limited number of users on the wireless network. Loss of proprietary information is of little concern to our agency, though this threat has been removed by the segregation and encryption of network traffic. The threats of data loss, email theft and political embarrassment due to a security breech have been minimized by encrypting all sensitive data through the VPN concentrator.

The Future

We are continually looking for new technology to improve our wireless security as funding becomes available. We are currently evaluating wireless "honeypots". One product we are reviewing generates thousands of counterfeit 802.11b access points, confusing the attacker and making the real AP more difficult to find. The AP becomes the proverbial needle in a haystack.

Microsoft is preparing to release a download for their operating systems that will increase wireless security. The upgrade introduces a new standard, Wi-Fi Protected Access (WPA). This is a new standard that is dubbed as the replacement for WEP. WPA uses a built-in Extensible Authentication Protocol (EAP) and is similar to Cisco's LEAP. EAP will provide user authentication using a RADIUS server. WPA also uses dynamic encryption keys by implementing the Temporal Key Integrity Protocol (TKIP) and uses a message integrity check known as michael. TKIP's dynamic keys which, are automatically rotated every 10,000 packets, will be much more difficult to crack than the static encryption keys associated with WEP. One problem remaining in WPA is the RC4 algorithm that is used, by TKIP, for encryption. RC4 is the same encryption algorithm used in WEP and it introduces the same vulnerabilities in WPA. TKIP is not being advertised as the ultimate fix. It is simply a quick fix that will be replaced with the Advanced Encryption Standard (AES) protocol which is a stronger form of encryption that will require a hardware upgrade.

Vendors are expected to release WPA certified wireless equipment in the third quarter of 2003. It is also anticipated that older equipment will be upgradeable to the WPA standard by a firmware flash update. Because of the non-proprietary

nature of WPA it will not require vendor specific hardware and will be interoperable between other WPA certified vendors.

Our plan for the immediate future is to find funding to replace our current system with either the Cisco or a WPA certified solution. This will ease the administrative burden associated with our current installation and provide increased security.

We continue to explore ways to provide "defense in depth" to properly secure our wireless infrastructure and to ensure the integrity of our information assets. We have learned that it is much easier to integrate security in the planning stage than it is to secure a product after it has been deployed. In the future we will consider security during the product evaluation and design phases.

Conclusion

Securing a network is a painstaking and time consuming process. Don't get in a hurry and jump to a quick fix. Before you begin, be sure to meet with the executive management and setup a budget. This will save you time in the long run and in our case keep you from test driving the Cadillac when you can only afford the Dodge. The first step, after the preliminary meeting, is to conduct a thorough assessment of all wireless assets. Secondly, conduct research on the latest protocols and security threats. Next, consult with a trusted research firm, such as The Gartner Group. Don't forget the Policy. It is impossible to have a successful security program without a policy. Finally, find the solution that is right for you. It doesn't make sense to spend thousands of dollars creating a secure network to surf the web with. On the other hand, spending thousands of dollars may just be a start to securing your corporations most classified information. Keep in mind, security is a dynamic concept. What may be secure today may be vulnerable tomorrow.

References

Borisov, Nikita. "Security of the WEP Algorithm". URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (20 February 2003).

Brooks, Jason. "Wireless LAN Lockdown". eWeek. 3 February 2003. URL: http://www.eweek.com/article2/0%2C3959%2C865592%2C00.asp (20 February 2003).

Cisco Aironet 350 Series Client Adapters. Data Sheet. URL: http://www.cisco.com/en/US/products/hw/wireless/ps4555/products_data_sheet09186a0080088828.html (10 February 2003).

Cisco Aironet 1200 Series Access Point. Data Sheet. URL: http://www.cisco.com/en/US/products/hw/wireless/ps430/products_data_sheet09186a00800937a6.html (9 February 2003).

Cisco Secure Access Control Server Software for Windows. Data Sheet. URL: http://www.cisco.com/en/US/products/sw/secursw/ps2086/index.html (9 February 2003)

Cisco Aironet Wireless LAN Security Overview. URL: http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm (20 February 2003).

Convery, Sean. "Wireless LAN Security in Depth". SAFE Blueprint Whitepaper. URL: http://www.cisco.com/en/US/netsol/ns110/ns170/ns171/ns128/networking_solutions_white_paper09186a008009c8b3.shtml (15 February 2003).

Fisher, Bret. "Wireless Security: 802.11i, TKIP, AES". 24 October 2002. URL: http://www.cawnet.org/pipermail/rfmon/2002-October/001901.html (18 March 2003)

Karagiannis, Konstantinos. "Ten Steps to a Secure Wireless Netwok." PC Magazine. 25 February 2003. URL: http://www.pcmag.com/article2/0%2C4149%2C844020%2C00.asp (27 February 2003).

Klaus, Christopher. "Wireless LAN Security FAQ". 6 October 2002. URL: http://www.iss.net/wireless/WLAN_FAQ.php (26 January 2003).

Lawson, Stephen. "Wi-Fi group lays out better wireless security". InfoWorld. 31 October 2002. URL: http://archive.infoworld.com/articles/hn/xml/02/10/31/021031hnwifi.xml?s=IDGNS (12 March 2003)

The Unofficial 802.11 Security Web Page. URL: http://www.drizzle.com/~aboba/IEEE/ (12 February 2003).