

Implementing Wireless Security Using Cisco's SAFE White Paper. A case study.

Ray Carsey

November 1, 2002

GSEC - Version 1.4b - Option 2

Abstract

Mobile wireless laptops have become an essential support tool for the Information Technology Department of our company. Security concerns over wireless networking almost required the removal of the installed wireless equipment. Senior management was very concerned about sensitive customer information such as credit card and social security numbers stored on our corporate local area network. We needed to find a way to secure the wireless network from the corporate local area network and insure only authorized users are accessing sensitive information. If this task could not be accomplished we would be required to remove the wireless network.

All of our current routing, switching, firewall, VPN, and wireless equipment is manufactured by Cisco Systems. Cisco Systems has published a white paper describing the most effective way of securing wireless networks using Cisco equipment.¹ By following the white paper and implementing the security equipment and features outlined, a corporation can feel more confident that their wireless network has been secured. This case study will outline the implementation of Cisco security features on various devices that enhance wireless security shortcomings.

Before

Articles with titles like "Wireless Security: A Contradiction in Terms?"² caused to me to take a hard look at our wireless security configurations. While researching the vulnerabilities of wireless networks I found that a wireless network needed to be treated as an internet connection. 802.11b wireless LANs were not originally designed with security in mind. 802.11b access point's ship with default SSID (Service Set Identifier) and encryption turned off. Any hacker can use a wireless network card with a program such as Mini-Stumbler and AirSnort to "sniff" the wireless packets across a network and determine how to gain access to the network. This was demonstrated in my SANS GSEC class. We also learned about building a wireless device using a tin can and an antenna. It does not take a sophisticated person to learn to build and use these devices. This information is freely available through the internet.

There is a new type of hacker that uses a technique called "War Driving". A war driver drives in business and residential areas with a wireless antenna connected to a laptop using sniffer and packet filtering software. This enables the driver to collect any wireless communication detected by his antenna and

capture the data packets with the laptop software. This can then be used to determine how to gain access to wireless access points into network connections. If sound security practices are not followed unauthorized access into private wireless and local area networks can occur.

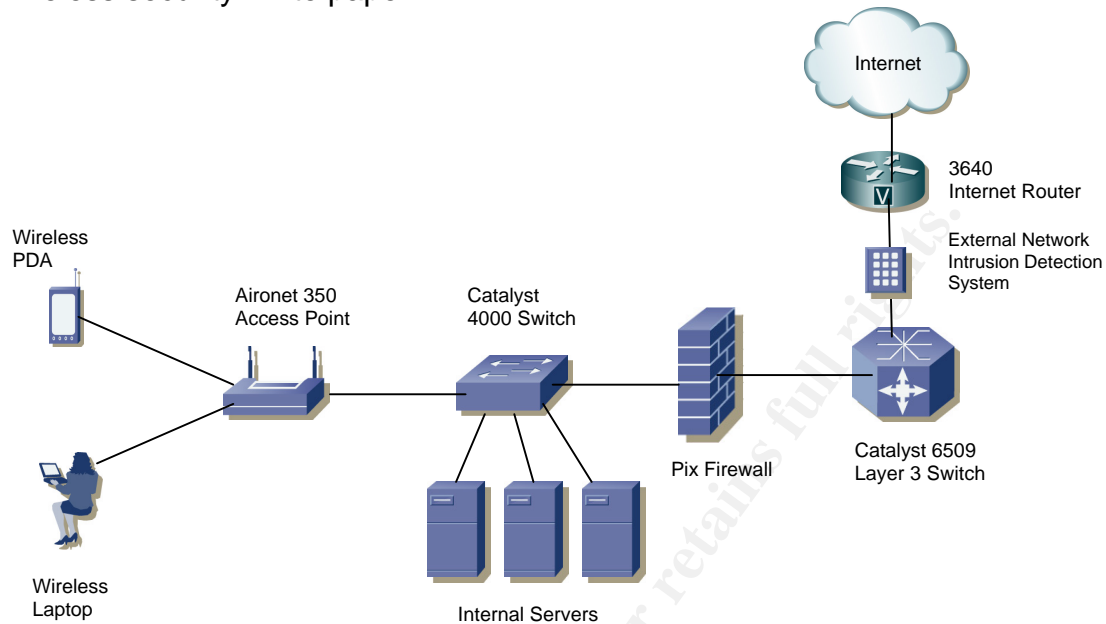
Our IT department supports 200 users located in various locations of our corporate office. Mobile wireless laptops have been used to enable our PC technicians and Network Administrators to help end users at their desks and still have access to the network resources necessary to perform their job functions. The wireless network was originally implemented without any security options enabled. We soon found that anyone with a wireless card could access our network with a default wireless card configuration. It became apparent that we needed to learn what steps to take to implement all security options available to us. Our IT staff has a sound understanding of Cisco's routing and switching devices. This was very beneficial in understanding Cisco's approach with their security devices. After some research we found that the security enhancements we desired were already part of the equipment we had purchased. They just needed to be implemented.

The only authentication method many vendors employ on wireless networks is a SSID (Service Set Identifier). The SSID of an access point is usually announced to the network by default. The SSID can easily be captured by means discussed previously. A solid authentication system should be employed to ensure that only authorized users are allowed into the wireless network. As of yet, a standard has not been developed to insure proper authentication across all vendors.

Many wireless access devices use an encryption method know as WEP (Wired Equivalent Privacy). Cryptographers' have mathematically proven that there are flaws in the WEP algorithm. WEP can be cracked if a hacker can gather enough wireless traffic and passes the traffic to WEP deciphering tools downloaded from the internet. These deciphering tools are able to "crack" the WEP keys and then use them to gain unauthorized access to wireless network resources. This weakness in the WEP algorithm has been widely publicized in many networking magazine articles. The IEEE committee has been working to develop a new standard for 802.11 wireless encryption. As of yet they have been unable to issue a new standard.³

The main security features required for our implementation dealt with authentication and encryption. Cisco's wireless access points have the ability through Cisco's Secure Access Control Server (ACS) to authenticate users to a Microsoft Active Directory Domain. This is accomplished through a proprietary encryption method known as LEAP (Lightweight Extensible Authentication Protocol).⁴ Cisco's LEAP takes wireless authentication and encryption to the next level.⁵

The Following diagram shows the network configuration before the implementation of LEAP and the other recommendations from Cisco's SAFE wireless security white paper:



Wireless users have unsecured access directly into sensitive network resources. Most of our security efforts have been directed to traffic coming to and from the internet. An external network intrusion detection system was installed to send alerts of improper internet traffic. This system was also configured to send TCP re-sets to clear improper internet connections. The tuning process for the IDS took quite a lot of time and effort. If wireless connections are treated as internet connections the same time and effort must be exerted to secure them.

During

A wireless networking policy was developed before implementing any security enhancements outlined in Cisco's white paper. The policy outlined those users authorized to use the wireless network and the information they had access to. The policy also described all hardware and software required to access the wireless network. The issue of auditing and detection was also addressed. An incidence and response section was written to describe steps necessary if unauthorized network entry was detected. The use of network security policies were discussed at great length at the SANS security class.

The first step outlined in Cisco's wireless security white paper required was to implement Cisco's LEAP authentication system. Cisco has published a step by step guide to implement Cisco Leap.⁶ This guide shows all hardware

and software upgrades and configurations necessary to complete the LEAP installation.

The current firmware on our Aironet 350 series access points and wireless network interface cards needed to be upgraded. The ability to upgrade to current firmware revisions is an important feature for any wireless access point or wireless network card. This allows for system enhancements without purchasing new equipment. It would be quite expensive to purchase new wireless hardware whenever a new security feature was released. The firmware upgrade was started by downloading the upgrade for the 350 Access Point and following the firmware upgrade guide provided by Cisco.⁷ We needed to upgrade the firmware on the wireless network interface card as well as upgrading the Microsoft network drivers and the wireless client software (ACU). In order to incorporate Cisco's Secure Access Control Server (ACS) to authenticate users, an upgrade to release 3.0 was performed.⁸

It was now time to configure the access points for LEAP authentication. A detailed installation guide is provided on Cisco Systems web site. Configuring the Cisco Wireless Security Suite (Revision 2.0). An entry was added to the ACS for a RADIUS server with a key that would be shared between the ACS and the access points. The ACS server had previously been configured to allow users to authenticate to a Microsoft Active Directory Domain Controller which allows a user to authenticate using their Microsoft username and password.⁹ The configuration of the access points required a little more work. An entry for the ACS server was entered with the shared key previously entered in the ACS configuration into the access point. The root radio data encryption was then set to Full Encryption and the Network-EAP box was checked. We also disabled the announcement of the SSID to conceal this information from any hacker trying to gather wireless information as described previously.

Configuring the ACU client is a relatively easy task. A profile is created by entering the wireless network SSID and selecting the LEAP option in the network security section. There is also an option to authenticate using a windows user name and password. The LEAP authentication is now ready to be tested. We were able to use the process listed to configure our wireless PDA's to securely access network resources as well.

Let me describe how the basic LEAP authentication works:

1. A wireless client connects to an Aironet 350 Access Point.
2. The client sends a start message to the Access Point.
3. The Access Point sends a request from the client to the ACS authentication server.
4. The client sends a user name to the Access Point which is forwarded to the ACS authentication server.

5. The ACS authentication server sends a challenge back.
6. The Access Point sends the challenge to the client as an EAP message over 802.11.
7. The client runs the challenge through the LEAP algorithm and responds with a value that is derived from a mixture of the challenge and the user password and is sent through the Access Point to the ACS authentication server.
8. The ACS authentication server run the user password through the LEAP algorithm and determines the values sent from the client. If they match the ACS sends a successful message through the Access Point to the client.
9. The client then sends a challenge to the ACS to authenticate the Access Point (wireless network) and goes through a reverse LEAP process.
10. If the Access Point (wireless network) is authenticated the client sends a successful message through the Access Point to the ACS which opens a port to the inter network.
11. The ACS holds a WEP key for the session and stores it on the Access Point.
12. The client derives the WEP key locally.
13. The ACS generates a new dynamic WEP key at an interval that can be changed on the ACS.¹⁰

Once the authentication was verified we were able to move on to the MAC (Media Access Control) authentication. Using the MAC address of a device to authenticate a user is another level of security available through the Aironet 350 access points. The MAC Address is located on the under side of the Cisco wireless card. This twelve digit hexadecimal number is entered in the Address Filters configuration page of the wireless access point. Implementing this layered authentication gives us an added layer of security an intruder must pass through to access company information. This layered approach was shown in the week long SANS security classes. We should not rely on a single security method to secure a network. MAC filter authentication should not be used exclusively as a security deterrent. Many wireless cards can be configured with any MAC address entered. A hacker can “spoof” or take on an allowed wireless card’s MAC address and gain access to internal LAN resources.

Another important aspect described in the SAFE wireless security white paper was the implementation of a VPN (Virtual Private Network) to further encrypt and tunnel wireless traffic. Wireless traffic that is properly authenticated through secure means and encrypted through a VPN tunnel is difficult if not impossible to decipher.

A separate VLAN (Virtual LAN) was created that would segment all wireless traffic from other network traffic. VLANs are a powerful tool in segmenting sensitive network traffic. This exercise helped us become aware that our

network was overly “flat” in nature. This means that we have too many workstations and servers located on the same TCP/IP network. We saw that this flat network should be logically broken-up into smaller data specific areas. VLANs in and of themselves are not considered a security measure. If they are used in conjunction with security measures they are an effective tool. If VLANs are employed in your network you must have a switch that is capable of processing VLAN traffic as well as being able to route information between VLANs. This routing of switched traffic is accomplished through a layer 3 switch device. Access lists were also created to only allow wireless VLAN traffic to access other VLANs with sensitive information. The use of VLANs was another topic discussed at the SANS GSEC security class.

The use of a DHCP (Dynamic Host Configuration Protocol) server to dynamically assign wireless devices IP addresses was discontinued. All wireless devices IP addresses are now statically assigned. An unauthorized wireless user can no longer obtain an IP address automatically.

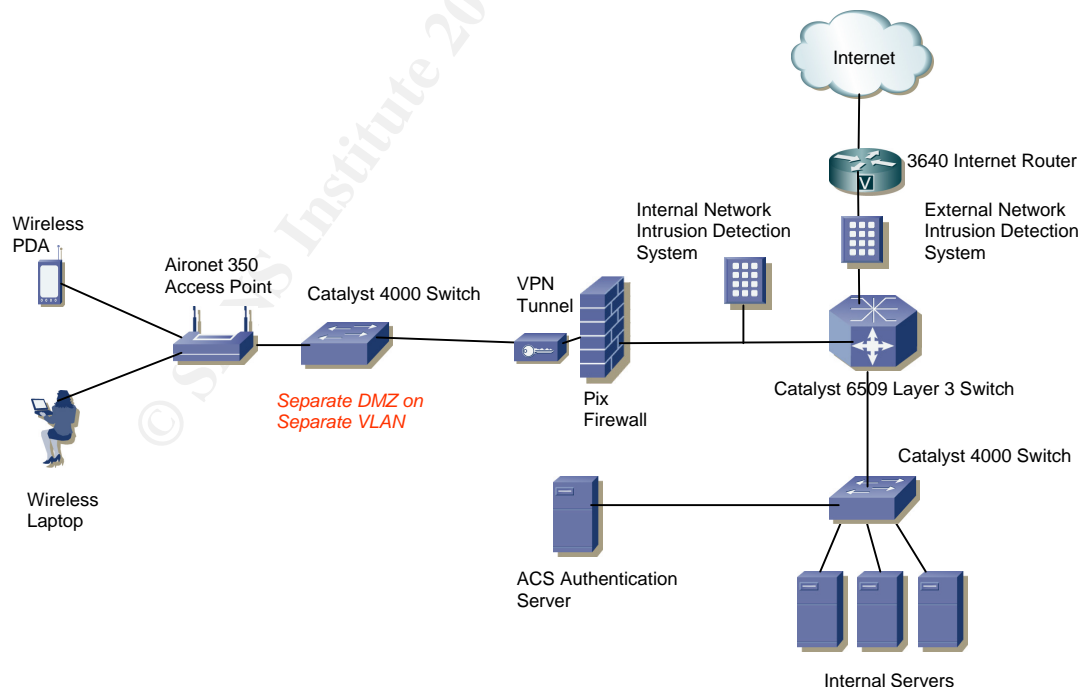
A separate DMZ (Demilitarized Zone) was configured to bring wireless traffic through. This DMZ was connected to a port on our PIX Firewall. Since we have a relatively few number of wireless users it was decided to use the Pix firewall to terminate our VPN connections. If the wireless VPN connections generate a high utilization on the firewall the VPN functions will be move to a hardware device called a VPN concentrator that is specifically designed to terminate VPN connections. The VPN concentrator would be placed between the firewall and the wireless access point. We implemented strict access lists on the firewall to only permit necessary network traffic through the VPN connection. Filters were constructed to only allow wireless traffic to access less sensitive server data. This network traffic segmentation shows another layering approach used to make a network more secure.

We learned that it was necessary to perform a site survey to determine the best placement of the Aironet 350 wireless access points. Access points should be able to receive radio transmissions to the exterior walls and windows but not beyond that point. If the access point signal radiates outside the building, it is easier for someone “War Driving” to intercept wireless network traffic. The next wireless access points we purchase will be equipped with directional antennas. These will be placed to further lessen the amount of wireless traffic leaked outside our building. There was a discussion in our SANS class about wireless transmissions being contained inside a companies building. Most of the class members were military personnel. A story was related about a government building that was built with materials and engineering that would act as a faraday cage and not allow radio waves to enter or leave the building. I decided that these measures would be rather cost prohibitive.

The last enhancement that needed to be implemented was an Internal IDS (Intrusion Detection System). We purchased a Cisco IDS blade for our Catalyst 6590 Layer 3 switch. This IDS blade will enable us to monitor wireless as well as internal network activity. Tuning the internal IDS was much harder than the external IDS. Our internal network produces many more false positives than the external web segment. We had to be very careful not to block valid network traffic. The IDS has been configured to alert network administrators to any inconsistent network traffic. We found that several workstations had Back Orifice root kits and a couple of Trojan Horses loaded on them. They somehow were able to bypass our virus protection software. These systems were re-imaged and are now being monitored for any suspicious activity. The internal IDS have become one of our most effective tools in monitoring internal network traffic.

An external penetration audit was performed by a well respected security firm which included penetration tests from the internet, internal LAN, as well as the wireless network segment. All recommendations of the security firm have been recently implemented. We have also contracted with this firm to perform quarterly network risk assessments to help strengthen our level of network security.

The diagram below describes the security enhancements outlined and implemented in the previous paragraphs. The diagram shows the additional security features of a separate DMZ and VLAN, VPN, Firewall, and internal IDS that work in conjunction with Cisco's LEAP authentication.



After

Enabling these security features outlined in Cisco's SAFE white paper on network security have increased our overall network security and enabled us to continue to use wireless technology without leaving unnecessary security holes.

Cisco recently released a firmware upgrade (12.00T) for their Aironet wireless access points. One of the new features in this firmware release will alert a network administrator if an access point is inserted into the network with a SSID that does not match other valid network access points. This release also allows an administrator to configure multiple SSID's that will correspond with separate VLANs configured on the switch connected to the access point. This feature allows us to create a separate VLAN whose traffic is directed to the internet bypassing any internal server resources.¹¹ Once we implemented Cisco LEAP our vendors could no longer access the internet while they were completing projects at our office. We created a vendor VLAN that allows our vendors and any other users that require wireless internet access to the internet. The vendors have internet access without allowing them access through our internal network which has sensitive information. The release also incorporates quality of service metrics that will eventually be used for wireless IP phones.

A new authentication method called PEAP (Protected Extensible Authentication Protocol) has been announced by Cisco. PEAP provides strong security using user database extensibility, and will support one-time token authentication and password aging. LEAP is unable to support these features. The implementation of PEAP follows the same upgrade process described above. As soon as Cisco releases the 3.1 version of their ACS server we can implement PEAP.

We are trying to upgrade to the most current security features available on all network devices. This can be a very difficult task. We have been able to leverage our investment in Cisco equipment by shortening the learning curve of new equipment and feature releases. The configurations of Cisco equipment are very similar across product lines. It is fairly easy to use our current knowledge to configure and use new security products and features. Cisco has done an excellent job with their product upgrade paths. They also have a vast amount of well written implementation and administration guides for their products. Cisco will probably not be the cheapest security solution a company can find. Our experience has shown us the old adage "You Get What You Pay For". Cisco continues to be a leader in the development of new networking products. We have been impressed with Cisco's economic stability. Any security vendor we choose must be in good financial condition. This is a requirement for any company equipment purchase.

The implementation of the security devices and features described in this case study has had a significant impact on our company's network infrastructure. The understanding I received in my SANS security class was invaluable in the design and configuration of the security devices and wireless network topology. We will continue to seek out new security technology issues and implement any necessary changes to insure a secure network into the future.

References

¹ CISCO - SAFE: Wireless LAN Security in Depth:

http://www.cisco.com/en/US/netsol/ns110/ns129/ns131/ns128/networking_solutions_implementation_white_paper09186a008009c8b3.shtml

² Networking Magazine - Wireless Security: A Contradiction in Terms?:

<http://www.networkmagazine.com/article/NMG20011203S0008>

³ COMPUTERWORLD - Wireless LAN Install Leaves Corporate Net Wide Open:

<http://www.computerworld.com/mobiletopics/mobile/story/0,10801,71448,00.html>

⁴ NetworkWorldFusion - Wireless LAN security: Cisco LEAPs past the competition: <http://www.nwfusion.com/reviews/2001/1217rev.html>

⁵ INTERNETWEEK.com - Security Flaw Isn't Death Knell For WLANs:

http://www.internetweek.com/printableArticle?doc_id=INW20010827S0009

⁶ Configuring the Cisco Wireless Security Suite:

http://www.cisco.com/en/US/products/hw/wireless/ps458/products_white_paper09186a00800b3d27.shtml

⁷ Firmware upgrade release notes for Aironet 350 Access Points:

<http://ftp:ftp@ftp-sj.cisco.com/pub/wireless/aironet/350/AP-BR-v1123TReleaseNotes.pdf>

⁸ Firmware upgrade release notes for Aironet 350 PCMCIA Network Interface Adapters:

<http://ftp:ftp@ftpsj.cisco.com/pub/wireless/aironet/firmware/350/PCMCIA-LMC-PCI-v42530ReleaseNotes.pdf>

⁹ Software: Cisco Aironet and Cisco Secure Access Control Server Security Implementations for the Cisco Wireless Security Suite:

http://www.cisco.com/en/US/customer/products/hw/wireless/ps458/products_qanda_item09186a008010018c.shtml

¹⁰ Under the Hood: Wireless Authentication:

http://www.cisco.com/en/US/about/ac123/ac114/about_cisco_online_exclusive09186a00800a5cab.html

¹¹ Firmware upgrade release notes for Aironet 350 Access Points to Release 12.00T: <http://ftp:ftp@ftp-sj.cisco.com/pub/wireless/aironet/350/ap/AP-BR-v1200TReleaseNotes.pdf>

© SANS Institute 2003, Author retains full rights