Global Information Assurance Certification Paper

Cisco's Aironet 350 – An Enterprise-Level Wireless Security Solution

Executive Summary

Wireless local area network (WLAN) technology is one of the fastest growing areas in the information technology sphere, and with good reason. The benefits of using wireless include reduced move/add/change costs, the elimination of wire plant requirements in new workspace or older structures that pose challenges for traditional wiring, mobility of workers and data, and many others. While this growth is beneficial, it also provides new security challenges that the marketplace has not adequately addressed. This paper addresses security issues present in the WLAN environment, and how these issues are currently improved upon by Cisco's Aironet 350 series of wireless gear. A brief overview of some of the current technology implemented by Cisco and others is included, but is in no way comprehensive. Several of the sources included at the end of this paper are excellent reference material and much more can be found on the Internet.

Current Situation

The use of wireless technology is an attractive alternative to traditional wired local area networks (LANs) for many reasons including ease of use and improved employee efficiency. However, the current state of WLAN security is inadequate, or worse, nonexistent. The usual implementation of WLANs involves the use of the Institute of Electrical and Electronics Engineers (IEEE) 802.11b standard. Wireless clients can connect using two techniques: the first method uses an access point (AP) to connect to the wired portion of the network containing back-end services such as email, databases, and the Internet, and the second method creates an ad hoc network between two clients without the need for the AP. The most common method in an enterprise-level implementation is using an AP so the ad hoc will not be covered. The current 802.11b technology has three main techniques to address wireless security concerns, Service Set Identifiers (SSIDs), Wireless Equivalency Protocol (WEP) encryption, and Media Access Control (MAC) address access control.

SSID or Network Name

The wireless network is given a Service Set Identifier, commonly referred to as the network name, that restricts access to the network to clients that are using the same name. In other words the SSID acts as a basic "password" that is sent in packets that attempt to access the network. Unfortunately the SSID is sent is clear text, so it can be intercepted by an attacker and used with ease. SSID management in a large organization with multiple WLANs or offices is also a problem. Local areas can use different names to reduce the threat of a compromise, but management of a potentially large number of names is required. Mobile workers are also affected because they are required to manage multiple IDs or configure multiple profiles on the client utility. Employee turnover can be a problem as well because the SSID is usually configured on the individual APs, which can make wholesale SSID changes a frequent occurrence. These two issues present a catch-22 because multiple names reduce the change requirements when

employees leave the company, especially if they are not mobile workers, but also introduces management overhead due to multiple SSIDs.

Wired Equivalency Protocol (WEP) Encryption

WEP encryption has a number of flaws that have been exposed by various parties including researchers at the University of California at Berkeley and the University of Maryland. The basic function of WEP and its shortcomings are outlined below. A more comprehensive discussion can be found at **http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html** and **http://www.cs.umd.edu/~waa/attack/v3dcmnt.htm** as a start.

The WEP protocol offers two levels of encryption, 40-bit and 128-bit. The 128-bit encryption is weaker than it appears on the surface because of the limits of the Initialization Vector (IV) as detailed below. WEP uses a shared secret key on the client and access points for encryption purposes. A 24-bit IV augments the shared key and works with the Ron's Code 4 (RC4) algorithm to create pseudo-random key streams. The two important points to remember without having to resort to a cryptography lesson are that the IV remains a 24-bit value in both 40 and 128-bit encryption methods and the short length of the IV necessitates a value being used multiple times in a relatively short time period. This occurrence is known as an IV collision and means that two or more pieces of ciphertext will be encrypted with the same key stream and that if an attacker can obtain this ciphertext, he can recover the plaintext using a statistical attack.

The integrity of a packet using WEP is verified using an Integrity Check (IC) based on a 32-bit Cyclic Redundancy Check (CRC-32) checksum. Unfortunately, the CRC-32 method is linear and allows a hacker to correctly determine the bits that need to be altered in the checksum to correspond to bits that she altered in the actual message.

What this means in practical terms is that WEP presents a better level of protection than an absence of encryption, but it is far from robust. Calculations and tests have been performed that show that a single IV, key stream pair can be compromised in less than two hours, and an entire dictionary can be built in less than two days. While these statistics do not seem very impressive on the surface, it should be pointed out that these results are based on using one attacking host with reasonable levels of processor power, memory, and disk space, and are valid regardless of key size. Injecting traffic into the network or having a known message sent via email or some other means can accelerate the hacking process by enabling the hacker to know the plaintext at the outset of the attack.

MAC Address Based ACLs

Access control lists (ACLs) that are based upon MAC addresses work by enabling the network administrator to enter the addresses that are allowed on specific APs throughout the network. Truly centralized control of the APs is not supported by all manufactures making this task difficult if not impossible with existing personnel, especially when factoring in mobile workers, employee turnover, new hires, etc. Most APs may be accessible remotely, but each one still has to be configured individually. The MAC ACL also suffers from many of the same problems that plague the SSID feature. The MAC address is sent in clear text so it can be intercepted. Many Network Interface Cards (NICs) enable the user to assign the MAC address manually as well

enabling a hacker to spoof a valid MAC address.

Traditional Workarounds

The most commonly suggested workarounds for 802.11b wireless security include security best practices such as defense-in-depth strategies. These techniques include placing WLANs outside firewalls, running a virtual private network (VPN), using the Remote Authentication Dial-In User Service, (RADIUS) and providing end-to-end encryption. Although these workarounds are good practices for all networks wireless or otherwise, in many circumstances they are practically impossible. Many factors including ease of use, workplace politics, and wholesale network redesign can come into play.

The Future

Fortunately, the IEEE is currently addressing the problems with WEP. There are two basic approaches that are being pursued, one has to do with improving WEP by releasing WEP2 and the second involves using the Advanced Encryption Standard (AES), a new encryption standard that is poised to replace the Data Encryption Standard (DES). The first approach is barely better than standard WEP, and is riddled with many of the same flaws, and the AES solution is not currently available.

Cisco's Aironet 350 Series

Cisco attempts to address and improve upon the same major areas that are addressed by other APs and WEP: authentication, encryption, and integrity. A few other handy features are covered at the end of this section as well. There are a few drawbacks to the solution as well as some areas that offer promise. The biggest drawback to the Aironet equipment is probably the fact that it is proprietary and expensive compared to most of the other 802.11b equipment on the market. All components are required to be Cisco products, right down to the NICs in the client machines. A great amount of time and money can be spent in configuration, firmware upgrades, and other areas if an existing infrastructure has to be replaced. Another problem is that WEP is still at the heart of the solution for encryption and integrity. The overwhelming benefit is that the architecture and unique methods used are a good stopgap measure for organizations using 820.11b that require a security solution that is superior to WEP until AES can be implemented.

Authorization

The industry standard RADIUS is used for authorization of clients as well as access points. RADIUS is a User Datagram Protocol (UDP) based authorization service that is widely implemented and understood. The service is usually setup to run on a centralized server that responds to requests for remote access. A secondary, backup server can be added if high availability is deemed necessary. This method allows the organization to manage all authorization at a central location without the need to configure individual APs. An added benefit is that AP authentication is two-way so the common problem of rogue access points can be avoided. The RADIUS implementation addresses both the SSID and MAC based ACLs normally used on access points. RADIUS processes authorization requests using

username/password combinations that can be stored in a password file, central database, or using a custom solution. Cisco's implementation can also authenticate against a Windows 2000 Active Directory or NT domain database thereby leveraging an existing investment for some organizations. Microsoft has built this authentication into the Windows login process for further simplification. Drivers are available for the Apple Mac OS and Linux for networks that are not solely Microsoft based. Another major benefit is that the username/password combination is encrypted on the wireless and wired links back to the RADIUS server using a Message Digest 5 (MD5) one-way hash. These messages are authenticated using an authorization key to prevent spoofing.

Encryption

Encryption on the 350 series network is handled in two ways. The RADIUS authentication process is encrypted as explained above, and the ongoing communication is encrypted using WEP. The WEP encryption is substantially improved upon, however, by using the Cisco Access Control Server (ACS). The method used is based on the IEEE 802.1x draft standard that includes the Extensible Authentication Protocol (EAP) and RADIUS protocol for wireless security. Cisco's ACS eliminates the need for shared secret keys throughout the network by creating WEP keys on demand. These keys are assigned to the individual user and are valid only for the current session. Because the key is no longer shared, the possibilities of IV collisions that make standard WEP so vulnerable are highly reduced.

Integrity

The area of integrity is still quite weak due to the fact that WEP is still at the core of the ongoing data encryption. Integrity attacks can still be undertaken in the same way as with standard WEP.

Additional Features

As previously mentioned, Cisco's solution is totally proprietary and can be quite expensive compared to other vendors. Many other handy options offer ease of use that may help to justify the price as well as improve security as related to eavesdropping.

Speed

Several tests at the time of the Aironet 350 series release show that the throughput was the fastest for wireless LANs at around 5-6 Mbps.

Power over Ethernet

The AP does not have a power connector on the unit itself but uses the IEEE 802.3af in-line power over Ethernet standard. Power is supplied over the Ethernet cable that connects the AP to the wired portion of the network. A power injector or one of Cisco's switches that has an option for in-line power can supply the necessary electricity.

Hot-Standby

Access points can be deployed in groups of two to provide for redundancy in critical applications.

Coverage Area

The RF power output of the Aironet can be adjusted to one of the highest levels available to improve coverage area. The best part of this feature is that the power can also be reduced so that the coverage area is drastically reduced as well. As more clients are added to a wireless network, performance is diminished. The wireless LAN functions in much the same way as older shared networks that use 10BaseT hubs. To reduce bandwidth sharing an area with a high user density can use many APs increasing bandwidth per user. The ability to reduce power can be a handy function for many small environments such as a field office or executive's home network as well. Many organizations have permitted access to their WLANs in parking lots, adjacent suites, and other undesirable areas unknowingly or because they had no choice due to the range of an installed access point.

Logging

Although RADIUS has been covered in some depth earlier it should be mentioned that Cisco's ACS server has logging features that do not directly concern authentication, encryption, or integrity but a log record can be beneficial for accounting purposes for legitimate users and for forensic type investigation after a suspected attack.

Scalability

The Aironet 350 series can supposedly scale to 250,000 users per server but this assertion has not been verified in the "real world".

Public Space Partnerships

Cisco has setup a limited number of partnerships in major metropolitan areas with wireless service providers. The current areas covered are airports and hotels located in the United States and select areas in the Asia Pacific region. Mobile clients will be able to use their Cisco wireless gear to connect to the Internet or company resources. Plans are under way to expand availability in the future.

Conclusions

The introduction of the wireless LAN has provided many benefits including ease of deployment, reduced infrastructure cost and maintenance, and worker mobility and efficiency; however, much of the progress has been overshadowed by a lack of forethought and planning for security. The assertion has been made that 802.11b security in the form of WEP was never supposed to be a robust security solution. The issue appears to be rooted in the fact that WEP was not permitted to be scrutinized by the cryptographic community, rather than its stated design goal to be equivalent to a wired network. WEP has since been proven to be weak in its implementation of basic cryptographic functions and popular opinion seems to reflect that WEP is not a viable protocol even with the improvements that will be added with the implementation of WEP2. The other open standards option is AES, but the problem is that AES will not be an available until sometime in the future. The only options for the security administrator are to not deploy wireless, wait for AES and use standard WEP in the meantime, or deploy the Cisco Aironet 350 series as a stopgap.

The Aironet 350 series of wireless gear does not solve all the problems of WLAN security, but it does mitigate the exposure of wireless data and systems to attack. The cost and proprietary nature of this solution can make it a difficult choice for many situations, especially if the installation will be large or an existing wireless infrastructure is present that will have to be replaced. However, some organizations demand a high level of security because of the sensitivity of their data, but also need to utilize wireless technology to address the business needs of a mobile workforce. Cisco provides the most robust solution currently available to support these installations.

While the Aironet 350 is not the perfect solution and is probably best considered a temporary fix until AES is available there is a good possibility that standards will develop around the Cisco implementation. Cisco and Microsoft are working closely with the IEEE on the 802.1x draft standard and the Aironet 350 series is the first implementation available. It is somewhat reasonable to assume that the final standard may be close enough that a few firmware upgrades to the current 350 series gear will bring it into compliance with the final draft and hopefully interoperability with other vendors. AES could potentially be on the horizon for the 350 series as well.

Glossary

ACL – access control list. A list used to control access to a network service or device
ACS – Access Control Server. Cisco's implementation of the RADIUS server as in the Cisco Secure ACS
AES – Advanced Encryption Standard. The latest open standard encryption method that will replace DES
AP – access point. The device that wireless clients use to access the network. The access point is the link between the wireless client and the wired network.
Ciphertext – data or text (plaintext) that has been encrypted to remove its original format and information structure so it is no longer directly meaningful.
CRC-32 – Cyclic Redundancy Check – 32 bit. A error checking/integrity technique where the sender of a frame calculates a numerical value based on the contents of a frame and the receiver verifies that the result of the calculation is identical after the frame has been transmitted by performing the calculation again upon receipt of the frame.
DES – Data Encryption Standard. A widely used public encryption standard. DES has been broken and will soon be replaced by AES.
EAP – Extensible Authentication Protocol. A standard security protocol used in the IEEE 802.11x draft standard for access control.
IC – integrity check. A method used to verify that the contents of a frame have not been altered. CRC-32 is an example of a method used to perform an integrity check.
IEEE – Institute of Electrical and Electronics Engineers. One of the organizations that seek to create open standards for networking, communications, and similar fields.
IV – initialization vector. A variable 24-bit value used in WEP to enhance the shared, secret key.
LAN – local area network. A network used to connect network devices over a relatively small area such as a room, building, or small campus.

MAC address – Media Access Control address. The address of a physical device on the network such as a network interface card or access point. Often referred to as the hardware address.
MD5 – Message Digest 5. A one-way hashing algorithm used with RADIUS as well as many other common applications.
NIC – Network Interface Card. The hardware device used to connect a client to the network. NICs come in traditional wired and wireless versions.
Plaintext – The term used to refer to the data or text that is input to the encryption algorithm to derive encrypted ciphertext.
RADIUS – Remote Authentication Dial-In User Service. A common standard protocol used on the Cisco ACS server and others to provide authentication to remote devices. Often used for dial-up client access.
RC4 – The encryption algorithm used by WEP to produce the pseudo-random key stream.
SSID – Service Set Identifier. The name given to a particular 802.11b wireless network that acts as a password. Only packets with the correct ID are accepted. Also referred to as the network name.
UDP – User Datagram Protocol. The connectionless transport layer protocol used by RADIUS.
VPN – Virtual Private Network. A method of encrypting private network work traffic over a public, insecure network such as the Internet.
WEP – Wired Equivalency Protocol. The security protocol/architecture that forms the core of the 802.11b standard.
WLAN – A wireless infrastructure that connects network devices over a relatively small area. See also LAN

References

Arbaugh, William A. "An Inductive Chosen Plaintext Attack Against WEP/WEP2". May 2001 **http://www.cs.umd.edu/~waa/attack/frame.htm** (September 26, 2001)

Borisov, Nikita; Goldberg, Ian; and Wagner, David. "Security of the WEP Algorithm". January-July 2001
http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (September 26, 2001)

Cisco Systems, Inc. "Cisco Aironet 350 Series".
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap (September 26, 2001)

Cisco Systems, Inc. "Cisco Aironet 350 Series Wireless LAN Security". April 11, 2001
http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350w_ov.htm
(September 26, 2001)

Cisco Systems, Inc. "Cisco Internet Mobile Office Hot Spots".
http://www.cisco.com/pcgi-bin/cimo/Home (September 26, 2001)

Evans, William F. "RADIUS – A Protocol for Centralized Authentication".

October 27, 2000
http://www.sans.org/infosecFAQ/authentic/radius2.htm (September 26, 2001)

Garcia, Andrew. "WEP Remains Vulnerable". eWeek March 26, 2001
http://www.zdnet.com/eweek/stories/general/0,11011,2700806,00.html (September 26, 2001)

The IBM Corporation. "Wireless Security Auditor (WSA)
http://www.research.ibm.com/gsal/wsa (September 26, 2001)

McMurry, Mike. "Wireless Security". January 22, 2001
http://www.sans.org/infosecFAQ/wireless/wireless_sec.htm (September 26, 2001)

Mehta, Princy C. "Wired Equivalency Privacy Vulnerability". April 4, 2001
http://www.sans.org/infosecFAQ/wireless/equiv.htm (September 26, 2001)

Mobile Computing Online. "Comparison Report: Wireless LANs for All: Aironet 350".
http://www.mobilecomputing.com/showarchives.cgi?149:4 (September 26, 2001)

Molta, Dave. "Cisco Aironet 350 Series Tightens Wireless Security". February 5, 2001
http://www.networkcomputing.com/1203/1203sp1.html (September 26, 2001)

Nelson, Matthew G. "Untethered Doesn't Mean Unsecure". February 5, 2001
http://www.informationweek.com/shared/printArticle?article=infoweek/823/cisco.htm&pub=iwk (September 26, 2001)

Publications and Communications, Inc. "Cisco and Microsoft Collaborate on Wireless Networking Security". May 2001 Cisco World
http://www.ciscoworldmagazine.com/monthly/2001/05/microsoft.shtml
(September 26, 2001)

Ross, B. Justin. "Containing the Wireless LAN Security Risk". November 4, 2000
http://www.sans.org/infosecFAQ/wireless/wireless_LAN.htm (September 26, 2001)

Schenk, Rob. "Cisco Aironet 350 Series". February 15, 2001
http://www.zdnet.com/products/stories/reviews/0,4161,2682131,00.html
(September 26, 2001)

Wang, Sean. "Threats and Countermeasures in Wireless Networking".
December 20, 2000
http://www.sans.org/infosecFAQ/wireless/threats.htm (September 26, 2001)