Global Information Assurance Certification Paper

Implementation of 802.11b Wireless LAN with Cisco 350/WEP

Dave Marks

October 1, 2001

Introduction

My organization is experiencing rapid growth, and needed a solution to inventory management. The challenge was to provide a wireless network that met the users need for mobility and did not compromise the security of the network. Management wanted to utilize the new 802.11b standard, and was most impressed by the Cisco Aironet 350 Series Access Point. Also of interest, was the Cisco Aironet 350 Series Workgroup Bridge. This device brings the flexibility of wireless connectivity to any Ethernet-enabled device.

Security for any wireless network is a challenge. The Cisco 350 utilizing WEP (Wired Equivalent Privacy) along with EAP (Extensible Authentication Protocol) seemed to be the right product to provide both the mobility and security we were looking for.

Background

Before setting up my lab for testing of the wireless equipment, I wanted to gain a better understanding of both WEP (Wired Equivalent Privacy) and EAP (Extensible Authentication Protocol). I utilized the following internet sites to research both security protocols.

WEP is used to encrypt and decrypt data signals transmitted between Wireless LAN (WLAN) devices. WEP provides data confidentiality that is equivalent to a wired LAN, not providing encryption. WEP makes a wireless LAN link as secure as a wired link. WEP supports both 40 bit key and 128 bit key encryption. Cisco WEP is implemented at the hardware level, causing minimal performance issues.

EAP enables wireless users to authenticate to a Radius Server (ACS) with a network login capability. The Radius Server authenticates username and password of the client and transmits the authentication key to the access point.

WEP and EAP appeared on the surface to meet the minimum requirements of protecting the confidentiality, integrity and availability of the wireless network. As with any implementation, caution will need to be utilized during the installation as to not create vulnerabilities in the network during testing and deployment.

I also was introduced to one commonly used feature in wireless LAN's called the SSID. The SSID (Service Set Identifier) is used to logically define and separate the users and access points that form the wireless network. The SSID is advertised as periodic beacons sent over the wireless network by the access points. Although SSID's can be used as a minimum level of security to deny access to unauthorized users, I would recommend

against using only SSID's to maintain the security of your network. Many available wireless sniffer products can be utilized to determine the SSID's from the beacons being broadcast over the wireless network.

Authentication and Association

The next challenge was to emulate the wireless network in a lab environment. Authentication and association of the access points are the next step. Authentication is the process of verifying the client credentials to join the wireless LAN. Association is the process of associating the client with the access point.

The 802.11b spec calls for three states:

1. Unauthenticated and Unassociated
2. Authenticated and Unassociated
3. Authenticated and Associated

There are two types of authentication – Open System Authentication and Shared Key Authentication

The Open System Authentication is done in clear text. The process is done unencrypted. A client will be able to associate with the access point with no WEP key or an incorrect WEP key. The client will still be unable to send or receive data, because it does not have the correct key to process the packet.

The Shared Key Authentication sends a challenge test packet, if the client has no key, or the wrong key it can not be authenticated and will not be allowed to associate with the access point.

The default setting is Open System Authentication, and is a good place to start your testing. A client will first send request packet out all channels, the access points that hear the request will send a response packet back to the client. This packet contains the SSID. The client uses the SSID to determine which access point to maintain the association with. After the client determines the access point it will maintain an association with, it will begin the authentication process. The client will then send an authentication request to the access point. The AP and the client will then exchange response packets based on a pass/fail from the access point.

The Shared Key Authentication environment sends an authentication request to the access point, and the access point sends a challenge packet to the client. The client will encrypt the packet using the WEP key, and send the packet back to the AP. The access point will then decrypt the packet and send a pass/fail response in the return packet. Once the client completes the authentication it will proceed to the association process If the packet passes the access point it will add the client to its' association table, and returns the packet to the client.

Cisco LEAP Authentication allows the client and Radius Server ACS (Access Control Server) to exchange shared secrets, and determine an encryption key independently of each other. The access point sends only the key length and the key index, the key value is not sent since to client knows the key.

Cisco 350 Workgroup Bridge

The workgroup bridge offers support for a wide variety of products and applications. Any Ethernet device can terminate to the workgroup bridge and access the wireless LAN. This product offers tremendous flexibility in regard to locations that will be used temporarily and sites with physical cable installation issues. The workgroup bridge has a range of 40 meters at 11mps, or 107 meters at 1mps.

The Cisco 350 Series Workgroup Bridge supports Wired Equivalent Privacy (WEP) security architecture and provides up to 128-bit encryption. The workgroup bridge also supports the (EAP) standard. The devices on the workgroup bridge will be able to authenticate to a RADIUS server through the access point it is associated with.

Wireless LAN Network Vulnerabilities

Security on wireless LANs offers many new challenges.

One of the primary concerns is protecting the privacy of the WEP key on the access points and NIC cards. Security breaches based on hardware theft are very common. Central key management, and user based identification, authentication and accounting make it possible to detect security violations. I will be utilizing ACS (Cisco Secure) to provide this central management.

Client impersonation is a commonly seen attack. 802.11b does not identify users, MAC address based security schemes are a vulnerability. An attacker can change his MAC address to a client authorized to gain entry to the network.

Access point impersonation also presents a concern. There is no mutual authentication between the client and the access point. This allows denial of service attacks from unknown access point emulating members of the wireless LAN subnet.

Unintended data exposure can occur through control and data channel monitoring, important information can be obtained about the access point and the client. (MAC addresses)

In implementations were WEP keys are taken from passwords or phrases, your network becomes vulnerable to pre-computed and offline dictionary attacks.

Having completed the lab and beta testing of the Cisco 350 Access points and workgroup

bridges, it was determined this product met all of our requirements for functionality and security. We aggressively moved forward with the implementation to our company, knowing we had provided to right solution. The rollout was completed as scheduled.

What a surprise when I read this article:

http://www.newsbytes.com/news/01/168883.html

The article referred to researchers from Rice University and AT&T labs successfully breaking the Wireless Encryption Protocol (WEP). In a published paper at their WEB site, in was determined that " WEP is totally insecure".

My first impression was that a high powered, fully funded university team had been working for months on this project. I was surprised to find out two researchers with minimal financial resources, were able to crack the WEP key security in just a little over 2 hours. This of course meant that users that were using a minimum level of security would be vulnerable to attacks from less knowledgeable individuals, and wireless networks utilized by banks, credit card and retail establishments would be vulnerable to attacks by sophisticated professionals.

The attack against WEP, was described as an exploitation of the use of RC4 IV s being improperly designed within the WEP standard. The RC4 consists of two parts, a key scheduling algorithm and an output generator. The key scheduling algorithm in WEP uses either a 64-bit packet key(40-bit secret key plus 24-bit IV) or a 128 key (104-bit secret key plus 24-bit IV). Based on this design it was simple for the researchers to determine that the first output byte leaks information about the key bytes.

Once the WEP key was determined, capturing the encrypted packets was more difficult than the researchers had expected. The attackers had access to NAI "sniffer" and Wildpackets " airopeek", but in an effort to show the capture could be successful using low cost tools they were not used. Instead, a Linksys wireless card ($100.00) was used. It took them just under one week to resolve the delivery, software and hardware compatibility issues with the Linksys card.

TCPDUMP was utilized in the attack to determine the true value of the first plaintext byte of each packet. A large number of packets were collected from the wireless network by flooding a wireless node with ping traffic. It was determined that even a lees sophisticated attack would yield the same results in a short period of time, a couple of days.

The research team concluded 802.11 network should be considered as insecure, and the following recommendations were made:

Assume the link layer offers no security
Use higher level security, Ipsec and SSH instead of WEP

All 802.11 systems should be connected as external. Access points outside a firewall
Assume anyone who can acquire the physical proximity can access the network
In response to the security breaches of the WEP security protocol, Cisco has published enhancements to the 802.11b WEP security solution. Please note, the following enhancements will not solve all potential security issues, but do increase the time that will be required to "crack" to network.

Mutual authentication- Communication from the access point and RADIUS server is via a secure channel, and will prevent "man in the middle" attacks.

Secure key derivation- the original secure key undergoes "one way hashes" eliminating password reply attacks.

Dynamic WEP keys- The weakest link in the WEP protocol is the static WEP key. By using dynamic WEP keys, session keys are unique to the users and not shared. This solution also deals with the issue of stolen or lost cards.

Reauthentication policies- Policies can be set requiring reauthentication at the RADIUS server. The attack window is greatly minimized.

Initialization Vector changes- Initialization Vector (IV) changes on a per packet basis so no predetermined sequence exists. This enhancement not only minimizes the attack window, and decreases the ability to create table based attacks

Conclusion

When I joined the team assigned the task of implementing the 802.11b Wireless LAN, my experience in wireless networking was at the novice level. I had been involved in network troubleshooting and router administration for a about one year. I learned a great deal of technical knowledge in regard to 802.11b and WEP/EAP. The installation team I worked with was well supported by experienced network staff and vendor staff to insure the installation was not only completed on schedule, but met all the security requirements. I felt confident throughout the process, that all involved were experts in their field of expertise.

What I learned in retrospect, after completing the GIAC Security Essentials modules, is that the engineering that goes into the design and implementation of any new technology needs to be scrutinized from a security perspective. I was surprised at the level of expertise of the Rice University researchers, and the depth of complexity of the issues in breaking the WEP key standard. I have learned that security issues covered in the vendor supported training classes I received in networking and system administration, merely scratched the surface of security and were inadequate. Until I read the article detailing the WEP attack, I lacked the realization that individuals are constantly looking at weaknesses in all security protocols. Many times by the security community themselves. I am sure the engineering team that developed the WEP standard was convinced the product was

secure from attack.

I have learned the importance of having a strong security policy, that is reviewed on a regular basis. A constant review is necessary to guarantee that as new issues are discovered, as happened with the WEP key security breach they can be addressed immediately. It is clear to me that if you are serious about protecting the integrity of your data and your company's assets that having experts who specialize in protecting the network from outside and internal attacks is imperative.

References:

http://www.cisco.com/warp/public/102/confwep.html#intro

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350c_ds.htm

http://www.cs.rice.edu/~astubble/wep/wep_attack.html

http://www4.gartner.com/DisplayDocument?doc_cd=99228

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/a350b_ds.htm

http://www.cisco.com/univercd/cc/td/doc/pcat/350wgbr.htm

http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1281_pp.htm

http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf

http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Last Updated: May 29th, 2017

Upcoming Training

Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event