Global Information Assurance Certification Paper

Elements of Wireless Security

Gregory A. McGill

October 1, 2001

Introduction

A wireless LAN is a collection of devices connected via optical or radio technologies through open air. Wireless LANs, based on 2400 Megahertz radio transceivers have had an impact in many markets. Much has been written (Borisov, Goldberg and Wagner, 2001[1]; Posluns, 2001[2]; Mehta, 2001[3]; Ellingston, 2001[4]) about the inherent weaknesses in the Wired Equivalent Protocol (WEP). For their part, Cisco responded to these published weaknesses with new features (Meredith, 2001[5]; Cisco AP350 Product Bulletin, 2001[6]) to address many of the deficiencies in WEP.

The new Cisco strategy uses Extensible Authentication Protocol (EAP) to interact with an EAP-aware Radius Server, such as Cisco Access Control Server 2000 version 2.6. This "solution augments 802.11b WEP by creating a per-user, per-session, dynamic WEP key tied to the network logon[7]". Cisco's implementation of EAP is based on the 802.1x draft standard. The EAP approach does seem to address the primary weakness of static WEP keys. However, it does not address many of the other issues one encounters in a wireless environment, such as campus-wide VLAN deployment, ad hoc networks, physical security of the Access Points, deployment and management of wireless network cards, and radio footprints.

Components of a Wireless Network

Wireless LANs are typically built with Access Points, which Cisco describes as "wireless LAN transceivers that serve as the center point of a stand-alone wireless network or as the connection point between wireless and wired networks[8]". These devices are feature rich and some of the default behavior is not conducive to a good security posture. The access points are radio devices and proper consideration must be given to antenna selection and placement.

A wireless network designed to span one or many buildings will most likely rely on Virtual LAN (VLAN) technology to facilitate wireless roaming and reduce the amount of configuration on user workstations. It is impractical to build a stand-alone wireless network due to the low port count in any one location. The placement of existing switches in the company will likely be sufficient to handle the addition of access points in meeting rooms and break areas. Special cases like auditoriums and dining rooms may call for dedicated switches.

In this network, a decision was made to treat all wireless users as dial-in users, which means the device and the communication link is inherently un-trusted. This requires the

use of VPN technology, which in this design uses pre-existing components like the Cisco 3030 VPN Concentrator and the RSA SecurID server. The security policy for this site requires Intrusion detection on all network segments used for remote access so a sensor was added.

A DHCP server is needed to issue IP addresses and a RADIUS server is needed for authentication. Additionally, this site security policy calls for all network devices to use TACACS+ authentication for configuration access. An open firewall port was used to isolate the wireless VLAN from the TACACS and RADIUS servers and appropriate conduits for inbound authentication requests were defined.

Putting the Pieces Together

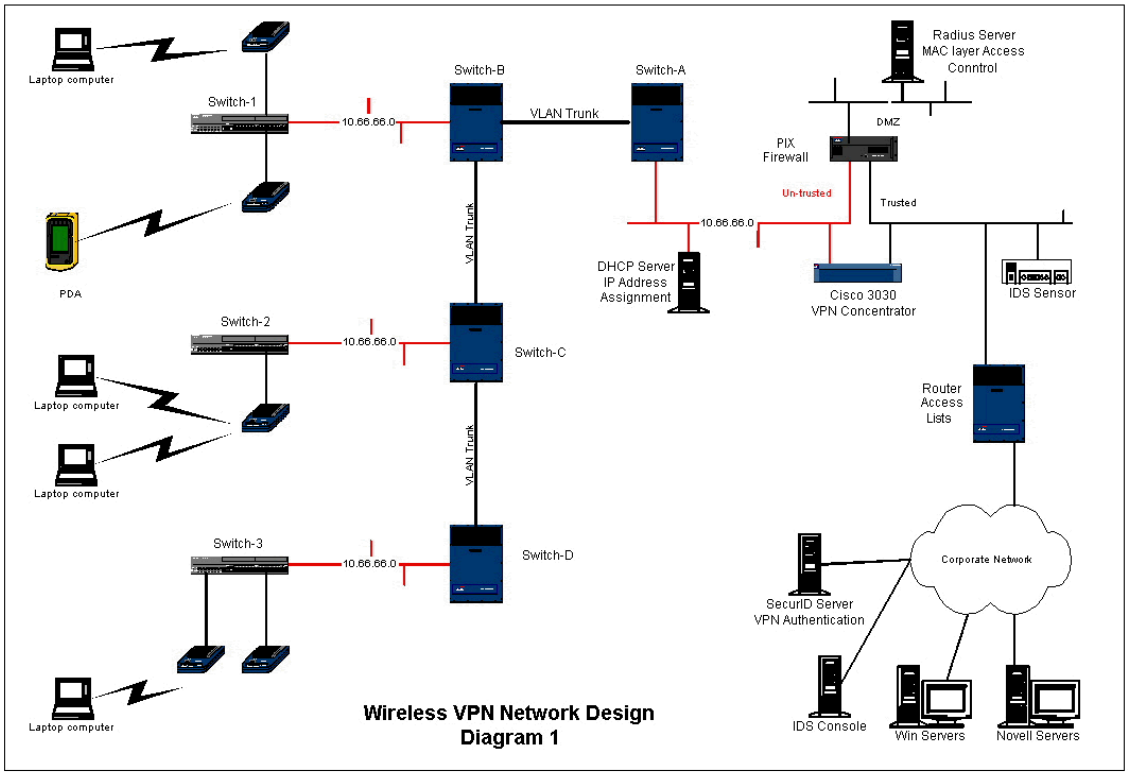


Diagram 1 shows a single un-trusted VLAN deployed in a campus environment using Cisco's Inter-Switch Link (ISL) trunk encapsulation protocol on switch-A through switch-D. In Cisco's words, "a trunk is a point-to-point link between one or more Ethernet switch ports and another networking device such as a router or a switch. Trunks carry the traffic of multiple VLANs over a single link and allow you to extend VLANs across an entire network[9]." The ISL protocol was chosen because there have been some concerns about the 802.1Q specification[10].

While the security of VLAN schemes is outside the scope of this paper, there are some physical security issues related to VLANs that should be discussed. It is strongly suggested that the port security feature of switches be used to limit which wireless Access Points can be connected to the wired network and where they can be connected. This feature would be implemented in Switch-1 through Switch-3 as shown in Diagram 1. It is also suggested that the wireless VLAN be defined in each switch with one port for each access point, resisting the temptation to define ports for future expansion. These steps offer some protection from mistakes in the wiring closet and the clandestine addition of new access points.

Using Cisco's EAP-aware Radius server (Cisco Access Control Server), one can control access to the wireless access point by MAC address. While this may represent an added administrative burden, it is necessary to protect against unauthorized users and rogue access points. Since many companies allow small purchases, such as wireless cards, to be purchased at a departmental or personal level, it becomes even more important to control access by MAC address. Another feature of Cisco's RADIUS server is that one can establish access by time and date. It is strongly suggested that implementers disable their wireless LANS during off hours where practical. One may consider a zoned approach where public areas are disabled and other, more controlled areas are left enabled.

One possible approach to managing wireless network cards is to have the Security Administrator record the wireless card MAC address, have the employee read and sign the appropriate security policy, enter the MAC address into the Radius Server, and lastly, affix a serial-numbered approval sticker on the wireless card.

Security Policies for the Wireless Environment

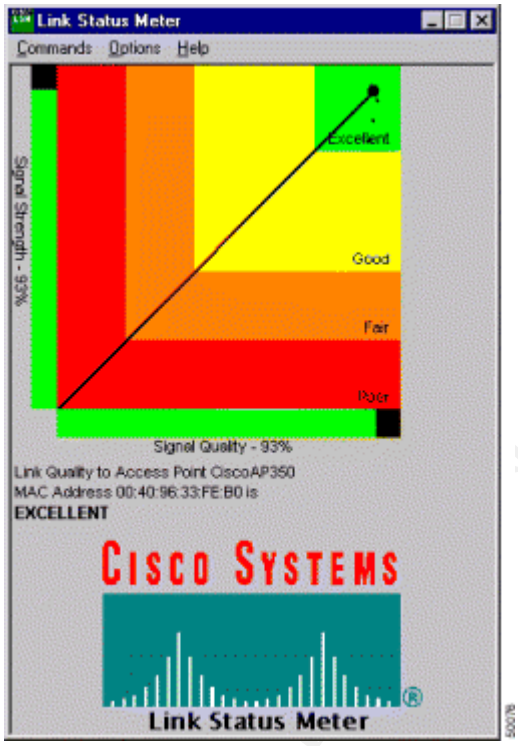
Security policies must be developed or enhanced to accommodate the new wireless environment. Primary issues will be ownership and control of the wireless network, controlling access to the network, physical security of access points, encryption, auditing, and the procedures for detecting and handling of rogue access points or networks. This last issue is particularly disturbing since the necessary equipment can be easily purchased.

Wireless networks are similar to remote access networks in that the end devices are an unknown quantity. The client device may not even belong to the company. These technologies need a central point of control and will often share some resources with the campus network such as switches and authentication servers. Consider the wireless device as another remote access device and determine how it may fit into existing security policies. A combination of strong two-factor authentication, virus scanning and host-based intrusion detection is almost mandatory.

The wireless security policy should encompass situations where users may find themselves using wireless access outside the office. Some hotels, airports and conference centers are currently offering wireless access. There is a potential vulnerability from other

users on the network and, in some cases, from the Internet. The consistent use of VPN technology is the best protection against eavesdropping when connecting over public networks.

It is a good idea for someone to periodically check the radio footprint by using the vendor-supplied signal strength tools. Too often radio engineers, who may have complete coverage as their goal, perform this task during installation. Public areas, which should not have coverage, are sometimes included. Be prepared to pay for expert advice on antenna placement and installation. Cisco adapters ship with a tool called Link Status Meter, which can be used to spot check signal quality. There is also a version for Windows CE devices. A screen print of the Windows version is shown here.



The security policy should emphasize the potential for interception of wireless signals and notified that routine audits of wireless usage will be performed. If all network cards are registered, activity can be traced back to an individual. There are some commercial wireless eavesdropping products from Network Associates and Wild Packets. The AiroPeek product from Wild Packets is less expensive and appears to have a complete feature set[11]. The Network Associates product comes from a fine heritage and is suited for those companies that have unlimited budgets.

Implementation

The network shown in Diagram 1 utilizes SecurID for positive authentication of users and IPSec tunnels with triple-DES encryption between the wireless device and the internal

network. This implementation uses the Cisco 3030 VPN Concentrator, which has native support for SecurID token authentication. This network had previously deployed SecurID and had upgraded to version 2.6 of Cisco Access Control Server. This same methodology is used for remote access so user impact is minimal.

This is an application of Defense-in-depth. An intruder must first obtain access to the wireless LAN with an authorized network card, then authenticate to the VPN server using a SecurID token before attaining any access to the corporate network. The IDS sensors will detect any attempts to scan the wireless network or penetrate the VPN, RADIUS or DHCP server. The IDS sensor on the inside was already present and is used to detect unusual traffic going to a wireless device. The RADIUS and DHCP servers should be protected with host-based intrusion and should have all web access disabled, if not uninstalled.

Cisco has tried to make the access point devices simple to deploy and manage but some of these features may cause concern for security professionals. One of these questionable features is related to SNMP and allows a username to be added as a SNMP community name, which means all SNMP community names must be defined as users. The WEP encryption level can be set via SNMP, so this may be cause to disable SNMP write capability.

Ad Hoc networking can be a useful tool but many corporations may choose to disable that capability due to the unrestricted shared environment it creates. Cisco has added a new feature to the Model 350 to address this concern. "Publicly Secure Packet Forwarding (PSPF) prevents client devices associated to a bridge or access point from inadvertently sharing files with other client devices on the wireless network. PSPF provides Internet access to client devices without providing other capabilities of a LAN. With PSPF enabled, client devices cannot communicate with other client devices on the wireless network[13]." This should eliminate all inter-device traffic except that which has been encrypted via IPSec tunnels.

Cisco Access Points are web-enabled for management functions, which could be a concern. The previously mentioned PSPF feature will not prevent users on the wireless network from accessing an Access Point's web page. Implementers should consider disabling this feature and limiting management access to telnet and console interfaces by replying NO to the *Allow Non-Console Browsing* configuration question. All Cisco products are configured to use Cisco Discovery Protocol (CDP) and this can be disabled entirely or just on the radio port via the management web page. Look for the *AP Radio* selection beneath the *Individual Port Enable* option on the *CDP Setup Page*.

The Radio Service Set ID (SSID) should be set to a unique value. Choose this value as one would choose a good password. Avoid default SSID values like Cisco's *tsunami*.

MAC-Based Authentication is enabled via the *Address Filters Page* below the *Setup* page. Check the Yes button for the *Lookup MAC Addresses on Authentication Server if*

not in Existing Filter List question. Note that *Authentication Server* is a link to the *Authentication Configuration Page* where the RADIUS server address and shared secret are entered. Be sure to select *MAC Address Filtering*.

Under the *AP Radio Hardware Page*, respond No to the *Allow Broadcast SSID to Associate* question. This forces client devices to have an exact SSID match. If this option is left enabled, devices can learn the SSID and associate with the Access Point.

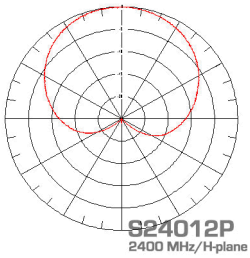
If a syslog server is available, navigate to the *Event Notifications Setup Page* and enter the address in the *Syslog Destination Address* box.

Since Access Points are sometimes placed in publicly accessible areas, it may be necessary to physically limit access to the console port. This can be done by purchasing 9-pin D-shell connectors (Radio Shack part #910-4001for $1.40) and attaching them with tamper-resistant screws.

Antennas

Antenna selection can greatly affect the security of a wireless network. Enterprise and campus networks may not desire omni directional coverage such as that found in hotels, airports and similar public areas. Many companies would benefit from the use of directional, patch antennas to control the radio footprint. The antenna footprint is usually shown in a Rose diagram but is also sometimes described as a coverage angle. Technical specifications may refer to E-Plane and H-Plane, which we can simplify to vertical and horizontal, respectively. A typical patch antenna might have a coverage angle of 65° in the horizontal plane and 70° in the vertical plane. Obviously an omni directional antenna will have a 360-degree coverage area. The specification will also state an indoor and outdoor range. When planning antenna placement, floor plans and a protractor, along with rose diagrams from the manufacturer, will help in finding, or creating, dead spots and overlapping coverage areas.

As shown in the following diagram[14], patch antennas can focus the radio energy into a fixed area. In the case of this 2400 Megahertz patch antenna from Cushcraft, the radiation pattern is slightly more than 180 degrees; complete coverage in front of the antenna with some coverage behind the antenna on either side. Imagine this antenna mounted on an exterior wall (the horizontal line in this diagram) with the large lobe directly in front.



By placing selected antennas properly, one can limit the amount of radio energy available to eavesdroppers outside the company walls. For additional protection, one may note that Cisco has posted a warning that "chain link fence, wire mesh with 1 - 1 1/2" spacing, acts as a 1/2" [harmonic] wave that will block a 2.4 GHz signal [15]".

VPN Clients

Cisco has released VPN clients for Windows, Linux, PocketPC and has announced support for Macintosh later this year. Certicom has enhanced its Movian VPN product for Palm, WinCE and PocketPC[16]. The Movian clients are positioned for modem users since their flagship platform is Palm, which currently has no Ethernet capability. The new Palm 500 and 505 have expansion slots, which Palm has stated are for 802.11b and GPS expansion cards.

Conclusion

The user community, based on coverage in trade journals and the popular press, has already accepted wireless networks. Now, it is up to network and security professionals to implement them in a responsible manner. Although this paper has concentrated on Cisco solutions, other vendors should have similar solutions.

While weaknesses in the WEP protocol have been covered in detail elsewhere, little attention has been given to the physical security problems associated with wireless networks. A simple guideline for deployment is that if there is no signal, the signal cannot be intercepted. Use the vendor-supplied tools for display of signal strength and limit the signal appropriately. Most importantly, know where your wireless signal can be intercepted. Be sure that the footprint is under your control. If the signal is detectable outside your property, be sure to install a surveillance camera to record activity in that area.

Use care when configuring the Access Points since the default behavior may not meet your security policy. If VLANS are used to connect the Access Points, use access lists on the switches and isolate the wireless VLAN from all other VLANs. Consider MAC address authentication as a first layer defense and do not allow Ad Hoc networking. Consider VPN clients on wireless devices to enforce strong encryption and require positive authentication via hardware tokens. Protect your authentication servers with firewalls if possible, and with host-based intrusion detection in all cases.

Consider the use of Network-based Intrusion Detection on the wireless LAN. During initial deployment, the sensor can be set to log all activity. This can be very helpful when explaining potential vulnerabilities to senior management.

References

1. Borisov, Nikita; Goldberg, Ian; and Wagner, David, "Security of the WEP Algorithm." May 23, 2001. http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html (October 1, 2001).
2. Posluns, Jeffrey, "Wireless Communications Technologies: An Analysis of Security Issues." April 26, 2001. http://www.sans.org/infosecFAQ/wireless/sec_issues.htm (October 1, 2001)
3. Mehata, Princy C., "Wired Equivalent Privacy Vulnerability." April 4, 2001. http://www.sans.org/infosecFAQ/wireless/equiv.htm (October 1, 2001)
4. Ellingson, Jorgen, "Layers One & Two of 802.11 WLAN Security." August 3, 2001. http://www.sans.org/infosecFAQ/wireless/WLAN_sec/htm (October 1, 2001)
5. Meredith, Gail, "Securing The Wireless LAN", Packet, Cisco Systems Users Magazine, Volume 13, No 3.
6. Cisco Product Bulletin No. 1327, "Cisco Comments on Recent WLAN Security paper from University of Maryland." http://www.cisco.com/warp/public/cc/pd/witc/ao350ap/prodlit/1327_pp.htm (October 6, 2001)
7. Cisco Product Bulletin, "Cisco Aironet Security Solution Provides Dynamic WEP to Address Researchers' Concerns." http://www.cisco.com/warp/public/cc/pd/witc/a0350ap/prodlit/1281_pp.htm (September 28. 2001)
8. Cisco Systems. "Cisco Aironet Access Point Software Configuration Guide." http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350ch1.htm (October 5, 2001)
9. Cisco Systems, "Catalyst 6000 Family Software Configuration Guide (5.4)." http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/sw_5_4/config/e_trunk.htm (October 5, 2001)
10. Bugtraq Archive, http://www.securityfocus.com/archive/1/26008 and http://www.securityfocus.com/archive/1/27062 (October 6. 2001)
11. Wild Packets, Inc., http://www.wildpackets.com/products/airopeek (October 5, 2001)
12. Cisco Systems. "Cisco Aironet Access Point Software Configuration Guide." http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350ch1.htm (October 5, 2001)
13. CushCraft Corporation, http://www.cushcraft.com/support/s2307amp/2400hp.jpg (October 6, 2001)
14. Cisco Systems. "Cisco Aironet Access Point Software Configuration Guide." http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/accsspts/ap350scg/ap350ch1.htm (October 5, 2001)
15. Certicom Corporation, http://www.certicom.com/products/movian/movianvpn.html (October 6, 2001)

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
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
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
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
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
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
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