Global Information Assurance Certification Paper

Cisco Aironet Wireless LAN Security
Stephan J. Kostyk
July 6, 2001

Introduction

Just today I received a letter from my local carrier offering the latest in wireless internet access. Soon, you'll be able to buy just about anything, just like the TV commercial where the a young woman buys a can of soda out of a vending machine with her wireless PDA. Access via wireless LAN from a Starbucks, the airport, or just about anywhere is just around the corner. Customers are pushing vendors to develop a high-speed wireless LAN standard which will reduce prices, provide interoperability, and provide additional bandwidth needed for applications.

Cisco Systems acquired the Aironet Corporation in March 2000 to enhance their portfolio for a complete end to end solution with wireless offerings. They currently offer the 340 series (radio transmitter rated @ 30mW) and the 350 series (rated @ 100mW). The security mechanism in the Cisco Aironet product lies in its compliance with the security standards as set forth by Wi-Fi (IEEE 802.11b standard) wireless products.

Wireless Background

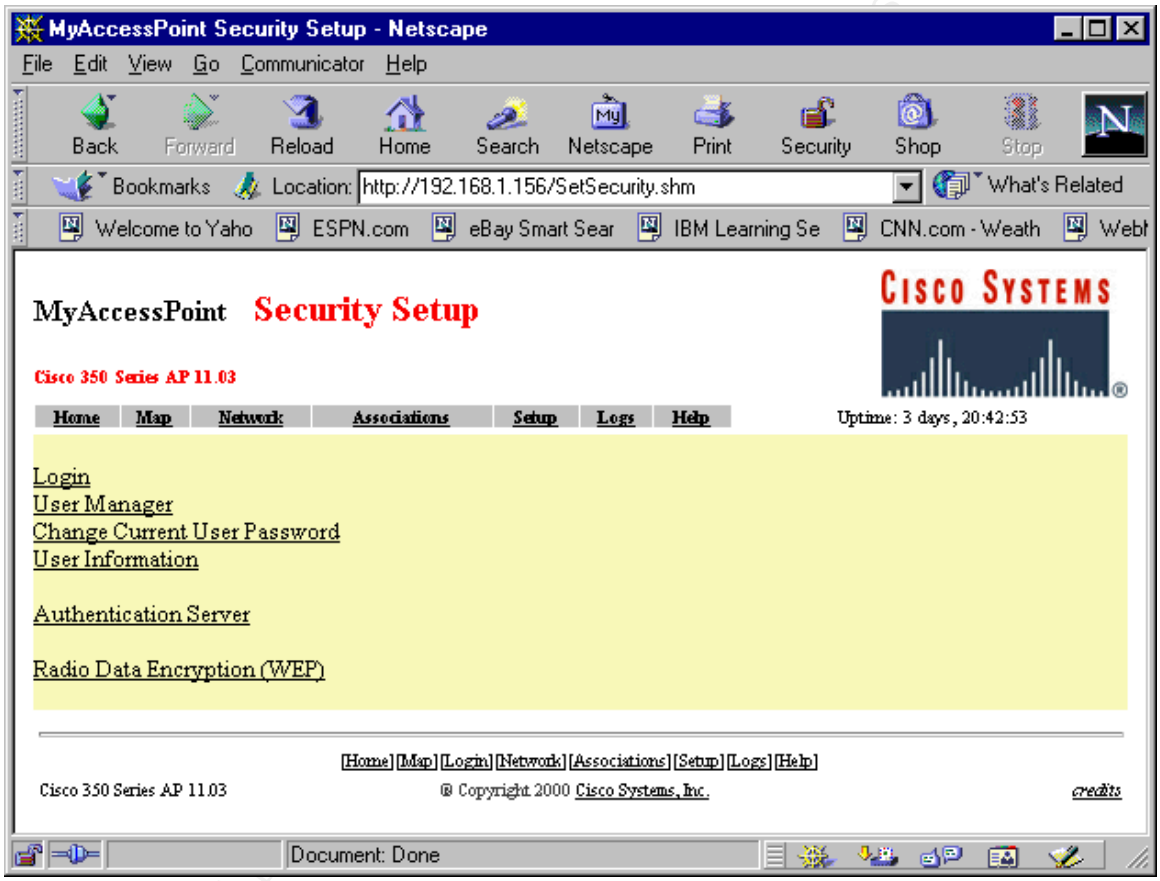
The Institute of Electrical and Electronics Engineers (IEEE) approved a modification to the wired ethernet 802.3 standard and defined the Wireless 802.11 LAN (WLAN) standard to operate at 11 Mbps. The growth of enterprise infrastructures and the need to setup "quick" networks without the premise wiring, triggered the wireless growth especially in the health care and education sectors. WLAN's use radio frequencies as a transmission medium at the 2.4 GHz frequency band, the only portion of the RF spectrum reserved around the world for unlicensed devices. The freedom and flexibility of wireless networking can be applied both within buildings and between buildings. By estimates, there will be a billion mobile devices (laptops and personal digital assistants) by 2003.

Cisco is a current member of Wi-Fi, who's mission is to certify interoperability of Wi-Fi products and to promote Wi-Fi as the global wireless LAN standard across all commercial sectors. Wi-Fi is a standard in wireless fidelity which has over 100 members including Ericsson, 3COM, HP, IBM, and Microsoft. The criteria by which Wi-Fi charters its members to compliance lies in its test matrix, which can be found at the URL www.wi-fi.org/downloads/test_matrix.PDF. Interoperability of wireless LAN products from different vendors is ensured by an independent organization called the Wireless Ethernet Compatibility Alliance (WECA). A more detailed description of the various wireless standards bodies, trade associations, and technology alliances can be found at the URL http://www.wlana.org/direct/matrix.htm.

Cisco Wireless Approach

The Access Point (AP) is a wireless LAN transceiver that serves as a focal point of a stand-alone wireless network or as the connection point between wireless and wired networks. The Cisco Aironet AP is configured via a terminal emulator thru an RS-232 port, web browser, telnet session, or SNMP. The security components of the AP are

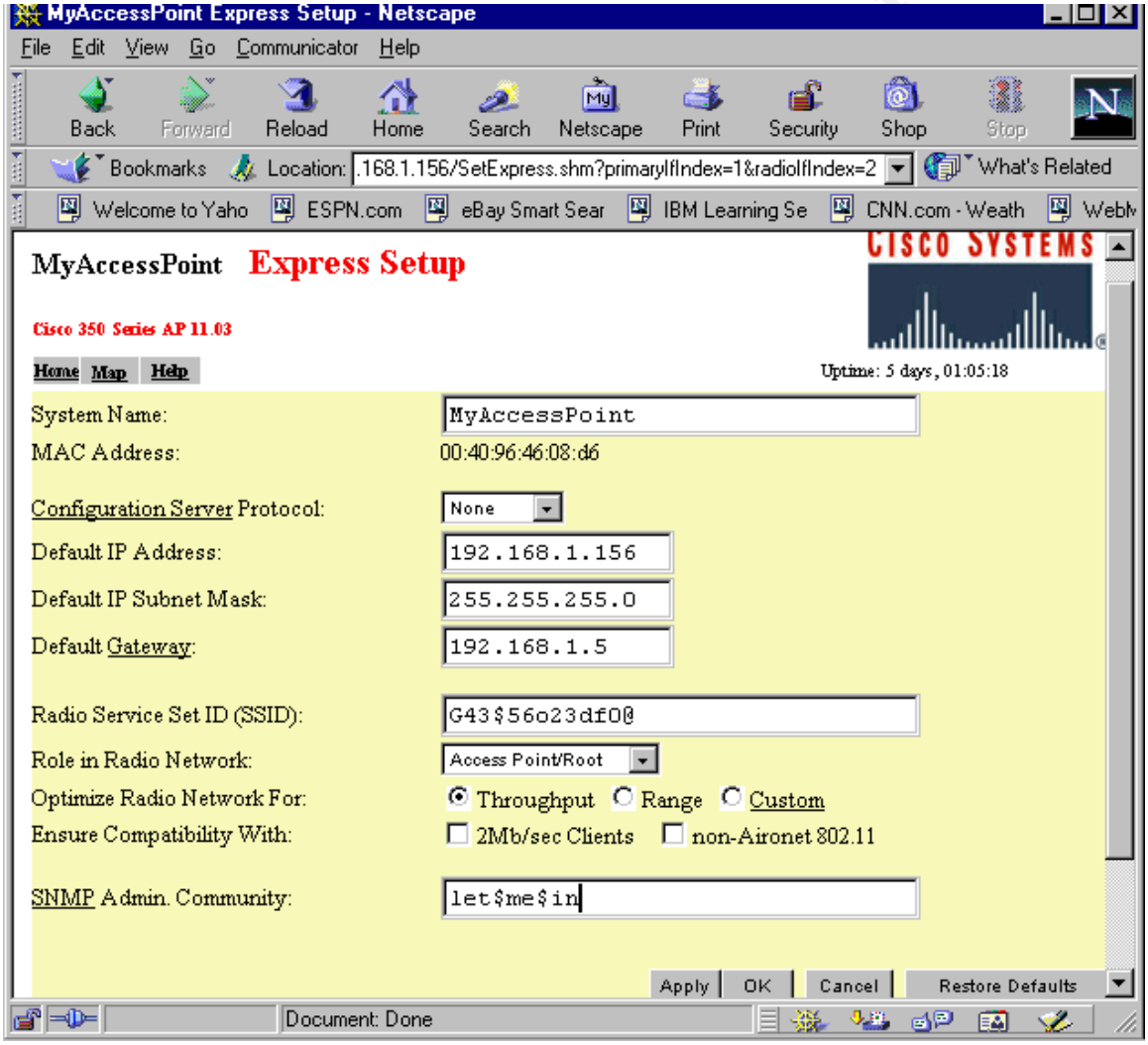
the Administrator Authorization, Radio Service Set ID (SSID), Wired Equivalent Privacy (WEP), and Extensible Authentication Protocol (EAP) with Authentication Server Setup (also known as Cisco Secure). It should also be noted that the browser default port is 80. To maintain a greater secrecy scheme you should choose an ephemeral web port >1024. This will prevent accidental detection of the AP web interface if the IP address is used. The default SNMP community string of *public* should not be chosen as well, since this is one of SAN's Top 10 security threats, http://www.sans.org/topten.htm. It is possible to manipulate configuration data if a clever attacker has the write community string. The appearance of the security configuration screen can be seen here through the web browser below.



The most elemental security feature is the User Manager for administrative authorization which is turned off by default. This should be enabled and a full administrator must be configured prior to enabling. There are 5 categories to choose;
Write- user can effectively change system settings (this should be very limited, 2 at most)
SNMP- designates username as an SNMP community name (do not use public or admin)
Ident- user to change AP identity settings (IP address and SSID) (again limit this to 2)
Firmware- user to update AP firmware, which should always be near the latest level to incorporate the most up-to-date patches and minimize security vulnerabilities
Admin- user can view sensitive system screens and with write capability can make

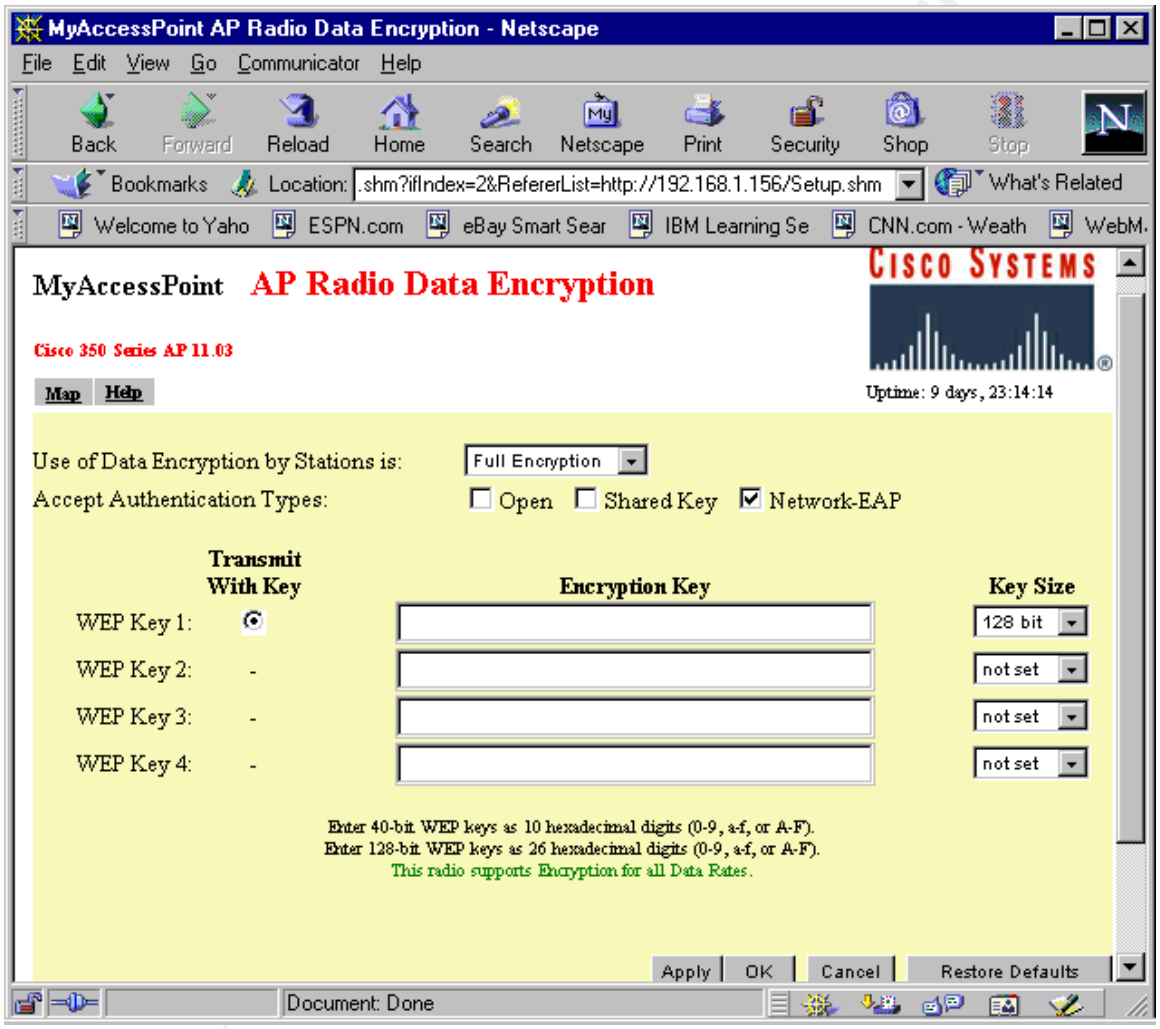
changes to the system.(give view admin to users in group, but limit write to just 2).

The SSID is a unique identifier that the client devices use to associate with the AP. The SSID allows client devices to distinguish between multiple wireless networks in the same vicinity by matching case-sensitive alphanumeric entries from 2 to 32 bit characters long. By default, Cisco uses the SSID string tsunami. This string should immediately be changed since it is a default configuration for all Cisco AP's. The principle of least privilege should be applied here to minimize vulnerabilities. Choosing non-dictionary lookup strings aids in the blanket of security. Below is an example of how this is configured through a browser.



The WEP protocol is used to encrypt data signals sent from the AP to the wireless client device and to decrypt data signals sent from the client devices to the AP. Up to 4 WEP keys can be defined using WEP 40-bit (10 hexadecimal digits 0-9,a-f) or WEP 128-bit (26 hexadecimal digits 0-9,a-f). WEP keys are not case sensitive. The default setting is no encryption, whereby the AP can communicate only with the client devices that are not

using WEP. Once a WEP key is defined (recommendation-here should be a 128 bit key WEP set to prevent link-layer eavesdropping or man in the middle attacks, where the basic idea is to stymie the potential attackers since it's been found that 64 bit keys can be cracked in 30 seconds or less) the other settings can then be chosen; *Optional* - client devices can communicate with the AP either with or without WEP. *Full Encryption*-client devices must use WEP to get to the AP (recommended). This menu configuration is shown in the web browser view below.

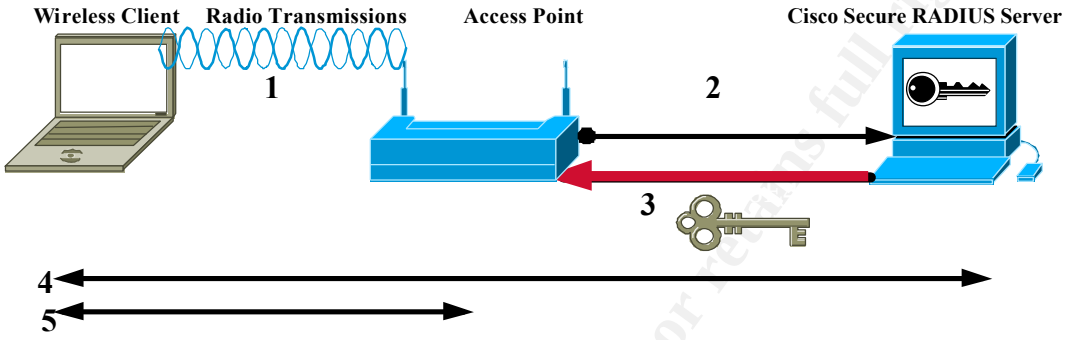


Lastly, to enable WEP, you must select the type of authentication the AP will recognize; *Open*-default, allows client (regardless of its WEP) to connect to AP(not recommended) *Shared Key*-AP sends plain text shared key query to any device trying to connect. This is a serious security risk and should not be used, since it gives intruders a chance to access. *Network EAP*- the recommended method whereby the AP uses EAP (RFC 2284) on a Remote Authentication Dial-In User Service (RADIUS) server on the internal network to provide authentication service for wireless client devices. Server based authentication can be enabled on the wireless client in one of two ways;

1)Through a host device and code built into its operating system (EAP)

2)Through client's firware and Cisco software, referred to as LEAP (Lightweight Efficient Application Protocol to alleviate eavesdropping and man-in-the-middle attacks through mutual authentication)

Once EAP is enabled on the AP and on the client devices, authentication to the network occurs in this sequence, as demonstrated by the diagram below.



1)Wireless client device uses EAP to provide a network login of username and password to associate with the Access Point, otherwise they are blocked out.
2) AP communicates with the EAP-compliant RADIUS server to authenticate username and password across a wired ethernet LAN physically connected.
3) If username and password are valid, RADIUS server sends a dynamic, session-based WEP encryption key to the Access Point.
4) Radius server and wireless client negotiate a dynamic session-based WEP key if the RADIUS server authenticates the user of the wireless client.
5) The AP and client activate the WEP and use the key for all transmissions during the session. The key is unique for the session and provides network access.

By default, the RADIUS server port setting is 1812 which is used on many RADIUS servers. The port 1645 is Cisco's RADIUS server, the Cisco Secure Access Control Server (ACS v2.6) which can run on Sun Solaris or Windows NT.

Another security feature that can be introduced on the Cisco AP is the filtering of the data based on protocols and MAC addresses. The filtering of the protocols for wireless client devices or users on the wired LAN via IP protocol, IP port, and ether-type. This can be thought of as the access control lists (ACL's) on routers or firewalls.

Recent Security Concerns

The goal of IEEE 802.11 and wireless LANs was to mirror the privacy achieved by a wired network and to simulate physical access by denying access to unauthenticated stations. A number of papers have been written to critique the vulnerabilities of the security in a wireless LAN. From a chronological perspective, 3 researchers identified here have had a significant impact on diagnosing IEEE 802.11 security vulnerabilities. To fully comprehend the theoretical concepts presented in these research documents, one must have a deep understanding of abstract mathematical concepts and cryptography.

In January 2001, Nikita Borisov, a research PHD candidate at the University of Berkeley along with 2 peers, explained a number of vulnerabilities of WEP. These included passive attacks such as eavesdropping which can intercept wireless traffic to reveal potential keys and active attacks which require radio transmissions that are more difficult to launch that can potentially allow injection of malicious traffic (ie. programming of firmware for reverse engineering). The WEP protocol is intended to enforce three main security goals; *confidentiality* (prevent casual eavesdropping), *access control*, and *data integrity* (prevention of tampering of data with integrity checksum). The WEP encryption algorithm provides data confidentiality using a symmetric stream cipher called RC4. Stream ciphers operate by expanding a secret key and a public per packet key (a 24-bit Initialization Vector -IV concatenated to a pre-shared key) into an arbitrarily long keystream of pseudo-random bits. Encryption is performed by using the boolean algebra exclusive OR (XOR) between the keystream and the plaintext to generate ciphertext. Decryption occurs by generating the identical keystream based on the IV and secret key and XORing it with the ciphertext. A huge breach of security occurs when encrypting two messages under the same IV and key which can reveal information about both messages (by XORing both ciphertexts together causes the keystream to cancel out, and the result is the two plaintexts- a well known pitfall of stream ciphers)! Thus, the keystream reuse can also lead to a number of attacks including the building of decryption dictionaries but this is for the most persistent type of attacker who is willing to invest time and resources to defeat WEP security. It was also found that CRC checksums were not cryptographically secure authentication code. CRC's were designed to detect random errors in the message, however they are not resilient against malicious attacks. Thus, message modification or message injection can occur. In conclusion, the point of the WEP cryptographic protocol is to be able to communicate securely over an insecure medium, which it fails to do, at least by itself.

At the University of Maryland, there has been a researcher named William Arbaugh who has been poking holes into the IEEE 802.11 standard, and maintaining an ongoing website of recent submittals by himself and other researchers to help fortify the wireless LAN endeavor (http://www.cs.umd.edu/~waa/wireless.html). The overall discussion focuses on the vulnerabilities of 802.11 wireless LAN authentication methods and protocols for access control like the shared key authentication method. Another attack described in detail is the "Parking Lot Attack", whereby a disgruntled former employee uses a laptop to bypass corporate firewall security and authenticate with an AP since all AP's transmit a beacon management frame at a fixed interval. The detailed authentication attacks describe the open systems authentication (essentially a NULL authentication process), shared key authentication pitfall, closed network access control (knowledge of the SSID or a shared secret), access control lists, and key management. Also examined is the weaknesses in the current access control mechanisms of AP's provided by Lucent's proprietary access control mechanism and their ethernet MAC address access control lists. The seriousness in this lies in that a MAC address can easily be sniffed by an attacker via eavesdropping and then subsequently masquerade as a valid address by programming the desired address into the wireless card and bypassing the access control to the protected network. Another concern is the "Man in the Middle" attack whereby an attacker can insert himself between a client and AP to obtain the

session key, which is using an unauthenticated Diffie-Hellman.

Jesse Walker of the Intel Corporation has been pushing the envelope of 802.11 in quite a number of different ways. His work has been including detailing the current 802.11 pitfalls today and proposing enhanced encapsulation along with options for bettering authentication, authorization, and key management. In short, his overall pitch is that data encryption itself offers no protection from attack and that cryptographic schemes should be reviewed by professionals. The last portion has to do with the fact that the 802.11 standard was only reviewed by internal IEEE members and not been reviewed from the "outside" specialists in cryptography such as the researchers at the University of Berkeley.

Cisco Security Enhancements

Cisco, Microsoft, and other companies have jointly proposed a baseline security framework IEEE 802.1x modified from IEEE 802.11b to incorporate EAP and RADIUS. Future wireless needs could potentially support authentication schemes including biometrics, certificates, and one-time passwords (ie. Secure-ID cards).

In support of the work done by the researchers at the University of Berkeley, University of Maryland, and Intel, Cisco agreed to the inherent weaknesses in WEP as defined in 802.11b and that these weaknesses exist regardless of the length of the encryption key used. Each of the researchers referred to flaws in Lucent's Orinoco AP. The Cisco Aironet solution is using a more sophisticated key management technique and recently has introduced several innovations, such as dynamic per-user, per-session WEP and integrated network logon, which will greatly diminish the applicability of certain attacks. The key enhancements to the 802.11b WEP standard made by Cisco include(these are all included in the 802.1x proposal);
Mutual Authentication- a new authentication scheme called LEAP between the wireless client and RADIUS server which eliminates "Man in the Middle attacks"
Secure key derivation- hash values sent over the wire are useful for one-time use only at the start of the authentication process, and not ever again (prevents back-dooring).
Dynamic WEP keys- this eliminates the vulnerabilities due to lost or stolen client cards.
Reauthentication policies-RADIUS server can have new policies set for reauthentication.
Initialization Vector changes- Cisco Aironet wireless solution changes the initialization vector on a per-packet basis to prevent attackers from exploiting messages.

Although it is not a new enhancement, but Cisco had developed Cisco Discovery Protocol (CDP) a proprietary protocol to help administrators collect information about locally attached neighboring devices. The Cisco Aironet AP's have the capability to enable CDP for troubleshooting and in effect can monitor the devices to trigger SNMP alarms to a management console such as HP Openview or Tivoli Netview. These tools have the ability to aid security administrators real-time for potential threats. There are other utility programs in existence such as Network Stumbler , written by Marius Milner which can pinpoint and catalog any AP in an area. Such a tool is valuable for wireless network installs and to test coverage for AP's. It is not intended to be used as a "war driver". This is a new term coined for laptops equipped with a wireless card in pursuit of scanning for AP's while driving around by potential attackers.

Conclusions

Do not use default configurations or out of the box configurations with wireless devices. That is just an open invitation to a potential attacker, as seen in the recent internet explosion with home computers possessing cable modems (always on) and their lack of security (even a simple firewall) can lead to possible damage without the knowledge of the user. The concept of defense in depth must be applied here, just like the layers of an onion as you peel it, you must plan ahead and layer your wireless security scheme. Wireless LAN's should be coupled with additional higher-level security mechanisms such as access control, end-to-end encryption, EAP/LEAP & RADIUS servers, and VPN's, especially in enterprise environments. Best practices in network design and deployment, and standards efforts on an open security framework, such as IEEE 802.1x will stimulate new interoperability to better meet customer needs. WEP alone does not provide an end-to-end security solution. Perhaps when the new AES encryption scheme becomes commercially available, this may help solidify future designs. Network security is dynamic, what did work today, might not tomorrow and will need constant attention to changing needs.

References

Arabaugh, William. "Your 802.11 Wireless Network has No Clothes."30 March 2001. URL: http://www.cs.umd.edu/~waa/wireless.pdf

Borisov, Nikita. "Security of the WEP Algorithm." January 2001. URL: http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

Daemon J./Rijmen V. "AES Algorithm (Rijndael) Information." URL: http://csrc.nist.gov/encryption/aes/rijndael

Harris, Daniel/Cole, Eric. Level One SANS Security Essentials Part 1. SANS Institute, Baltimore Maryland ,May 2001.

Milner, Marius "Net Stumbler". URL: http://www.personaltelco.net/index.cgi/NetStumbler

Walker, Jesse. "Overview of 802.11 Security" March 2001. URL: http://grouper.ieee.org/groups/802/15/pub/2001/Mar01/01154r0P802-15_TG3-Overview-of-802-11-Security.ppt

Walker, Jesse. "Unsafe at any key size, An analysis of the WEP encapsulation." Oct. 2000. URL: http://grouper.ieee.org/groups/802/11/Documents/DocumentHolder/0-362.zip

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

URL: http://www.wi-fi.org

URL: http://www.wlana.org