WIRELESS NETWORKING BENCHMARK

Version 1.0

April, 2005

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

TERMS OF USE AGREEMENT

Background.

The Center for Internet Security ("**CIS**") provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems, and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No Representations, Warranties, or Covenants.

CIS makes no representations, warranties, or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness, or completeness of the Products or the Recommendations. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties, or covenants of any kind.

User Agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**We**") agree and acknowledge that:

1. No network, system, device, hardware, software, or component can be made fully secure;
2. We are using the Products and the Recommendations solely at our own risk;
3. We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;
4. We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;
5. Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades, or bug fixes; or to notify us of the need for any such corrections, updates, upgrades, or bug fixes; and
6. Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of

use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of Limited Rights.
CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

1. Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;
2. Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of Intellectual Property Rights; Limitations on Distribution.
The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights."
Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this

paragraph.

We hereby agree to indemnify, defend, and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development, or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs, and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special Rules.

The distribution of the NSA Security Recommendations is subject to the terms of the NSA Legal Notice and the terms contained in the NSA Security Recommendations themselves (http://nsa2.www.conxion.com/cisco/notice.htm).

CIS has created and will from time to time create, special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules.

CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of Law; Jurisdiction; Venue

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions.

WE ACKNOWLEDGE THAT WE HAVE READ THESE AGREED TERMS OF USE IN THEIR ENTIRETY, UNDERSTAND THEM, AND WE AGREE TO BE BOUND BY THEM IN ALL RESPECTS.

1. INTRODUCTION

1.1 Wireless Benchmark Overview

Because of the wide range of environments and the often vastly differing functional and information protection requirements, the wireless technology security benchmarks will be divided into categories based on the characteristics of the environments to be configured.

Currently, this benchmark addresses the following levels:

- **Specialized Security-Limited Functionality:** These policies are appropriate for configuring a wireless network, which is part of an overall architecture for an enterprise level network. These networks often include wired networks, wide area network connectivity, and are administered by trained information technology staff. This type of Wireless Local Area Network (WLAN) is used to store, process, and/or transmit data that is highly valued, proprietary, or is protected by privacy laws. As such, accessibility and functionality may be sacrificed for security.

Future versions of the benchmark are being considered for the following levels:

- **Lower Sensitivity - High Functionality:** These policies are appropriate for configuring a wireless network that is part of an overall architecture for an enterprise level network. These networks often include wired networks, wide area network connectivity, and are administered by trained information technology staff. The requirements for this benchmark will focus on maximizing accessibility and functionality for the user while protecting the network from attackers. The additional expense in dollars and overhead is not merited. Security features such as Public Key Infrastructure (PKI) and high security encryption algorithms such as Advanced Encryption System (AES) are not needed based on a risk assessment.

- **Small Office/Home Office:** These policies are appropriate for configuring a wireless network that is part of a small office or home office environment. These networks may be purely wireless or may include wired networks. Highly specialized and dedicated information technology staff is often not available. The requirements for this benchmark will focus on maximizing accessibility and functionality for the user while protecting the WLAN from most attacks. The additional expense in dollars and overhead is not merited. Security features such as PKI and high security encryption algorithms such as AES are not needed based on a risk assessment. Protection is focused on using readily available and less expensive or free products whenever possible.

- **Hotspot Wireless Networks**: These policies are appropriate for configuring a wireless network, which is used as a public access to the Internet. Although available for public access, the backbone infrastructure and configuration must be protected from attack.

If you would like to see these environments addressed, please contact John Banghart at the Center for Internet Security. He can be reached via email at jbanghart@cisecurity.org or by phone at 703-716-0199.

1.1.1 Guide to Using the Wireless Benchmarks

Users of the wireless benchmark should, at a minimum, review the overall recommended architecture for the benchmark that most closely matches the functional requirements, data protection level, and other characteristics of their intended environments. The general policy tables will give general policies that should be implemented regardless of whether the technology used is wired or wireless—these policies are best practices that are accepted in the information protection industry. Finally, use the Wireless Policy Checklist and the Products Capability Matrix to help in your product comparison and selection research. The Center for Internet Security (CIS) document, *Assessing the Security of a Wireless Environment*, describes methods for conducting wireless site surveys and performing manual and automated monitoring.

1.2 Wireless Local Area Networking Technology Overview

In the last decade, WLANs have changed from a few proprietary products servicing a small, specialized market, to a rapidly changing, user-friendly, scalable technology. Security solutions for WLANs have also greatly improved. It is now possible to sufficiently mitigate the inherent security risks, which were once considered an inevitable part of the Institute of Electrical and Electronics Engineering (IEEE) 802.11 protocol. As with other, more mature technologies, enterprises, home offices, and individual users can tailor the wireless architecture to meet the degree of risk and the level of protection needed for the information being protected. Wireless networks can be configured to maximize mobility, convenience, and functionality that are inherent in the technology, but users and businesses must understand the tradeoffs involved in the ability to protect sensitive enterprise data.

For the enterprise environment, we recommend a multilayered defense to protect the highly sensitive WLAN that includes 802.11i for wireless encryption using rotating encryption keys, virtual private networks (VPNs), Remote Access Servers (RAS), network monitoring, and strong security policies. In addition to a multi-layered encryption approach – mutual authentication via 802.1x and the Extensible Authentication Protocol (EAP) should also be addressed as part of a defense in-depth approach. For very specific contracts with some U.S. and Canadian government agencies, additional measures, such as Internet Protocol security (IPsec) VPNs with Federal Information Processing Standard (FIPS) 140-2 Level 2 certification may be required. Refer to http://csrc.nist.gov/publications/fips/ for more information.

For the Small Office/Home Office (SOHO) environment, a less costly solution will be recommended in a future wireless benchmark. Even the home user, must consider the need to protect banking and personal information when accessing the Internet via an open medium such as wireless radio transmissions. The SOHO user must specifically configure WLAN devices before processing sensitive information. Configuration in this environment should also take a defense in-depth approach by using simple techniques such as Media Access Control (MAC) address filtering, and turning off Service Set Identifier (SSID) broadcast. At a minimum, use of a dynamic encryption system is recommended. However, for an increased security posture, particularly in the sensitive small office environment, using Advanced Encryption Standard (AES) for layer 2 encryption and a Wi-Fi Protected Access (WPA)v2 pre-shared key for dynamic key generation would be more secure, particular if connecting to the corporate network.

This benchmark recommends that all wireless environments in any area other than residential and general public access (Commercial, Industrial, Governmental, Military, and etc.) perform an appropriate degree of risk assessment to determine what level of stringency above the minimum general benchmark recommendations are required to effectively protect information resources. Additional resources on information assurance standards, risk assessments, education, procedures and metrics can be found at the following web sites: http://www.cert.org/octave/ and http://csrc.nist.gov/nissc/2000/proceedings/toc.pdf

1.2.1 Wireless Standards

The following is a brief review of wireless technology with an emphasis on wireless security protocols. This section is not intended to be an exhaustive review of wireless technology, protocols, or wireless security standards. References are provided in Appendix A, *Publications*, to assist the user in furthering his wireless education and specifically research protocols and encryption methods recommended throughout the wireless benchmarks.

The IEEE 802.11 standards group defines the WLAN standard. There is a sub-committee or sub-group for each component of the 802.11 standard.

- IEEE 802.11a is the standard for high speed WLANs in the 5 GHz band. The standard defines data rates between 6-54 Mbps with 6, 12, and 24 Mbps required for any implementation. Most vendors have implemented either Wired Equivalent Privacy (WEP) or WPAv2 security services in 802.11a products.

- IEEE 802.11b is the standard for WLANs in the 2.4 GHz band. The standard defines 1, 2, 5.5, and 11 Mbps data rates. Most vendors have implemented either WEP or WPA security services in 802.11b products.

- IEEE 802.11e is a developing standard that will specify Quality of Service (QoS) for WLAN systems that require QoS support (e.g., Voice-over-IP (VoIP) WLAN systems).

- IEEE 802.11f is the standard for the Inter-Access Point Protocol – IAPP, defines roaming compatibility across access points from different vendors.

- IEEE 802.11g is the standard for high speed (up to 54 Mbps) WLANs in the 2.4 GHz band. Most vendors have implemented either WEP or WPAv2 security services in 802.11g products.

- IEEE 802.11h is a developing standard that specifies dynamic channel selection and transmission power control for WLAN systems. Its purpose is to minimize interference between IEEE 802.11a WLAN systems and other systems operating in the 5 GHz frequency band such as radar systems, Earth Exploration Satellite Service (EESS) systems, and Space Research Service (SRS) systems.

- IEEE 802.11i is the new security specification of the 802.11 standard. Consists of two components: IEEE 802.1x and Robust Security Network (RSN). The RSN is comprised of the following components – 802.1x, an EAP type (Protected Extensible Authentication

(PEAP), EAP- Transport Layer Security (TLS), EAP-FAST etc.) for mutual authentication and finally AES as the Layer 2 Encryption algorithm.

- IEEE 802.11j is the standard for WLAN systems operating in the 4.9 – 5 GHz frequency band in Japan.

- IEEE 802.11n is a developing WLAN standard that will provide data rates in excess of 100 Mbps.

- IEEE 802.1x is the Port Based Network Access Control standard. Included in the IEEE 802.1x standard is EAP, which provides multiple user-based authentication methods (smart cards, Kerberos, PKI, etc.). EAP provides a standard method for user authentication in WLAN systems.

- IEEE 802.16 is the WiMax Broadband standard. Broadband wireless access offers a high speed, high capacity, low cost, scalable solution that extends the fiber optic backbone currently used for broadband communications. The first IEEE 802.16 standard, published in April 2002, defines the wireless metropolitan area network (WMAN) Air Interface. These systems are meant to provide network access to homes, small businesses, and commercial buildings as an alternative to traditional wired connections.

1.2.2 Security Protocols

WLANs use radio frequency (RF) transmissions for communications between devices. Unlike a wired LAN, where one cannot connect to the network without physical access to the wired infrastructure, RF is an easily intercepted medium. When wireless networking was a young, expensive, proprietary solution implemented by only a few highly specialized organizations, it was not a priority to protect the WLAN from casual attack. However, the introduction of WLANs based on the initial 802.11b standard brought many vendors into the market, which decreased the cost of ownership and complexity of implementation. Soon, the technology attracted the attention of the hacker community and, with low cost hacking tools readily available, they reported that a single "drive-by" attack could quickly compromise both secured and unsecured WLANs and compromise all applications, data, and other resources on the enterprise or home network. A compromised WLAN often became the staging area for denial of service (DoS), Trojan, or other attacks on both the wired and the wireless network.

Most attacks were designed to target systems that use the still widely deployed WEP protocol which was built-in as part of the initial 802.11 protocol. New protocols and encryption methods were introduced to WEP; however, WLANs remained vulnerable to attack by other means.

To negotiate the WLAN security protocol discussion, it is essential that the user understand the somewhat confusing sequence of protocol development. The names and numbers are neither in sequence nor are they completely separate. The reader must also key in on the Wi-Fi certification name that indicates the product they are considering is compliant or implements the desired security standard.

Recognizing the weaknesses in the existing encryption and authentication mechanisms, the IEEE 802.11i working group was created to define solutions that tighten WLAN access controls and

improve the encryption techniques. Unfortunately, coming to agreement on a new protocol did not move quickly and the need was critical. Thus, another group was formed, known as the Wi-Fi Alliance. This industry group improved the security of WLAN products via a series of rapid steps. The first step was the release of the WPA definition, which was used as an intermediate solution until the ratification of the pending 802.11i standard. WPA defined an architecture as opposed to an encryption solution through the use of a security enhancement to WEP called the Temporal Key Integrity Protocol (TKIP), 802.1x and EAP a more secure wireless architecture was created. Due to the need for backward compatibility, WEP was still included in the WPA architecture. Currently, WLAN WPAv2 security solutions include:

- Using 802.1x authentication, access control, and base key generation for the TKIP and AES
- Using TKIP, which protects against known WEP attacks
- Replacing WEP with WPA on currently deployed equipment, whenever possible
- Setting WPA encryption scheme to AES in all new equipment

The following paragraphs are a more detailed discussion of each protocol. Table 1-1, Summary of WLAN Security Protocols, summarized the differences in the security protocols and gives the ready an opportunity for a quick reference.

Table 1-1. Summary of WLAN Security Protocols

WEP	WPA	WPA2
Rivest Cipher 4 (RC4) for confidentiality	RC4 by default for confidentiality	AES by default for encryption and confidentiality (RSN) TKIP for encryption and MIC for integrity also supported for less capable equipment
64 or 128 bit encryption	128 bit encryption 64 bit authentication	128 bit encryption
Concatenated packet key	Mixing function packet key	Packet key not needed
CRC-32 for data integrity	Michael used for data integrity	Counter-Mode/CBC-MAC Protocol (CCMP) used for data integrity
No header integrity check	Michael used for header integrity check	CCMP used for header integrity check
No protection against replay attack	Uses initialization vector to protect against replay attack	Uses initialization vector to protect against replay attack
EAP-based (optional)	EAP-based	EAP-based

1.2.2.1 WEP

WEP was the included in the original 802.11 specifications in 1999. It uses the Rivest Cipher 4 (RC4) algorithm to encrypt portions of the data transmitted between the Access Point (AP) and the station. Most WLAN products offer both 64-bit and 128-bit WEP encryption. The WEP

encryption key is comprised of a shared key and a 24-bit initialization vector (IV). Combining a 40-bit shared key and the IV forms the 64-bit WEP key. Combining a 104-bit shared key and the IV forms the 128-bit WEP key. Some WLAN products allow the IV to be changed dynamically as often as after every transmission.

The primary security flaws of WEP are because of the method by which the initialization vector is used and transmitted. Any station that can receive the packets on the WEP encrypted WLAN, could see the IV, which is transmitted in clear text. By using low cost, readily available equipment, a small amount of traffic can be intercepted, analyzed, and deduce the encryption key. Then using the IV and the key, an attacker could easily gain access to the shared secret key. Additionally, since the original WEP specification required the same key be hard coded into all stations, it followed that all stations were now able to read the data being transmitted regardless of destination station. Finally, a known security issue with all shared key systems is that an attacker can gain access to the entire network if on AP or station is lost, stolen, or hacked.

For the enterprise, particularly the highly sensitive network, WEP alone, is never an acceptable option. However, if legacy equipment that does not have the processing capacity to be upgraded to the more demanding protocols, WEP or WPA in conjunction with 802.1x authentication with dynamic key generation and key rotation, and a sound security policy could provide an acceptably secure solution with a longer term goal of upgrading to better equipment.

For the small office network WPA in personal mode (does not require 802.1x server) is the best option. This configuration will allow for the use of Pre-Shared keys. The initial PSK is used as the keying material for the dynamic keys used with TKIP or AES.

For the home office network WEP may be used, even with shared secret keys. With layered security and proper configuration, even WEP can be adequately secured.

1.2.2.2 WPA1/WPA2/TKIP

In 2002, the Wi-Fi Alliance defined a security architecture that resolved the issues with the original 802.11 WEP specification. WPA1 was released and, after obtaining feedback from industry, the final version was released and is known as simply WPA. It is important to note that WPA is based on the work being done by the 802.11i working group. WPA became widely available in 2003 and is a subset of the final 802.11i standard. WPA is a combination of authentication and encryption (802.1x, EAP and TKIP) and mitigates nearly all WEP security concerns. Wireless products shipping after Aug 2003, particularly enterprise level devices must comply with the WPA standard and have the Wi-Fi certified seal. Although WPA using TKIP is the standard, WEP is still included in Wi-Fi equipment for backward compatibility for legacy equipment.

WPA is often referred to by its key integrity protection protocol name, TKIP. WPA (TKIP) uses the RC4 algorithm by default, however, some products may allow use of pre-standard AES in WPAv1 deployments. The major differences between TKIP and AES are the implementation of the encryption and decryption layers. TKIP uses four keys and AES uses three keys, but both protocols use the same key management scheme.

1.2.2.3 WPA2/802.11i/AES

The 802.11i standard, ratified in June 2004, updates the IEEE 802.11 standard by incorporating WPA (TKIP) with improved data and header integrity. The standard also incorporated AES as the default cipher, which provided advanced encryption and security features.

CCMP is used to handle both packet authentication and encryption. CCMP uses AES to provide confidentiality and encryption. Cipher Block Chaining Message Authentication Code (CBC-MAC) is used for improved message authentication and integrity.

The CCMP protocol uses a 128 bit-key and a 128-bit block size for a 256-bit block-cipher encryption mechanism replacing the 40 and 128-bit stream-cipher mechanisms used in WEP and WPA. The 802.11i standard requires the use of a 128-bit key but larger key sizes are possible to enhance the security of a system using AES encryption. Although larger key sizes are possible, in most cases they are not required and may impact performance of low power handheld devices. WEP and WPA use the RC4 algorithm that operates using a stream-cipher mechanism. The result is a more vulnerable protocol with a key stream that is the same length as the data stream, making it possible to use a brute force attack to break the cipher.

Key caching and pre-authentication provide for improved roaming between APs. These processes were not included in the original 802.11 standard, but are now increasingly needed to support application such as Voice over WLAN and videoconferencing where seamless data streams are needed. The Wi-Fi Alliance certifies 802.11i products as WPAv2 compliant.

1.2.2.4 802.1x

The 802.1x protocol is an authentication standard that can be used for wired as well as wired as well as wireless networks. This standard provides for user and device authentication as well as distribution and management of encryption keys. Individual client sessions use different keys and keys are changed dynamically, thus addressing two of the major security flaws of WEP. Use of 802.1x authentication has been made mandatory by the 802.11i WLAN security standard, thus products meeting the WPAv2 requirements will be compatible with enterprise level 802.11i authentication servers, such as the Remote Access Dial-in User Service (RADIUS) server. The RADIUS server can then pass off the backend authentication to enterprise authentication services such as Active Directory, Lightweight Directory Access Protocol (LDAP), or Novell NDS. WEP and WPA installations may also install 802.1x solutions to mitigate the shared-secret authentication security issues.

The use of 802.11i configured to use AES encryption, 802.1x authentication services along with the EAP provides the best solution for the enterprise level network, particularly a high security environment. Additional 802.1x can be used to provide some protection from unauthorized APs on the wired network, as all devices are required to provide authentication credentials to the network switch port prior to obtaining access.

1.2.2.5 Extensible Authentication Protocol (EAP)

The use of EAP provides support for centralized, user-based authentication with the ability to generate dynamic encryption keys. Several 802.1x authentication types exist, each providing a

different approach to authentication while relying on the same framework and the EAP for communication between a client and an access point. Supported types include: Cisco LEAP, EAP-FAST, EAP-Transport Layer Security (EAP-TLS), and types that operate over EAP-TLS, such as Protected Extensible Authentication Protocol (PEAP), EAP-Tunneled TLS (EAP-Tunneling TLS (TTLS)), and EAP-Subscriber Identity Module (EAP-SIM).

The EAP method chosen as the authentication type for their 802.1x deployment is dependent on multiple factors. Areas to evaluate when selecting an EAP type include the following: security mechanism used for security credentials; the user authentication database; the client operating systems in use; the available client supplicants; the type of user login needed; and RADIUS or Authentication, Authorization, and Accounting (AAA) servers.

Each EAP type has advantages and disadvantages. Trade-offs exist between the security provided, EAP type manageability, the operating systems supported, the client devices supported, the client software and authentication messaging overhead, certificate requirements, user ease of use and WLAN infrastructure device support. Multiple EAP types might also be used within a network to meet specific authentication, client device, or end user needs.

2. WLAN: SPECIALIZED SECURITY-LIMITED FUNCTIONALITY ENVIRONMENTS

This wireless benchmark addresses recommended policies for securing wireless networks when used to process highly sensitive information such as HIPPA, FISMA, Grand Jury Material, company confidential, proprietary, trade secret, Sarbanes-Oxley, Grahm-Leach- Blaly, and military classified. Outside of the U.S, look into the applicable laws that are similar to those listed here. Using wireless to store, process or transmit highly sensitive data is generally not considered a best practice, however, we recognize that there may be overriding business reasons which may make an acceptance of risk necessary. In this case, the following policies address actions for establishing and maintaining a highly secured WLAN, which protects these highly sensitive resources while in transit and at rest.

2.1 Network Architecture

Specialized security, limited functionality environments are often embedded within large enterprise networks. Enterprise networks are usually complicated; often large in scale; are distributed geographically; and store and transmit information of various sensitivity levels. This benchmark recommends the following:

- Secure integration of the wireless network with the internal wired network. One example of integration uses the existing switch infrastructure to create separate virtual local area networks (VLANs) for the wireless network. Another example uses a central switch to tunnel all AP traffic to a single point without Layer 2 VLANs spanning the network—which may be a better solution for the extremely large network.

- Wireless users connect “remotely” using a VPN to provide needed security.

VPNs provide a secure path or tunnel for communications between the enterprise and remote users connecting. A recent trend for wired enterprises has been the use of VPNs with any device not directly wired to the enterprise, whether that device is connected through the Internet or through a local WLAN. This configuration is particularly important if 802.11i is not used. However, the introduction of the 802.11i standard with its advanced security mechanisms has eliminated the need for the VPN, particularly for stations that exclusively use the enterprise WLAN. Some organizations still prefer to use the VPN for all remote users to simplify network management. Figure 2-1 and 2-2 illustrates these two WLAN implementations.

Note that secure architectures may exist which use gateway/switch products. These architectures may also meet benchmark requirements and may be included in a future version of this benchmark.

Figure 2-1, *VPN Implementation of a Specialized Security WLAN*, illustrates the main components of this architecture. Though the functions of the client device (e.g., laptop, Personal Digital Assistant (PDA), notebook, voice handset) and AP are clear, the underlying network requires additional components to manage and secure the enterprise network networks.

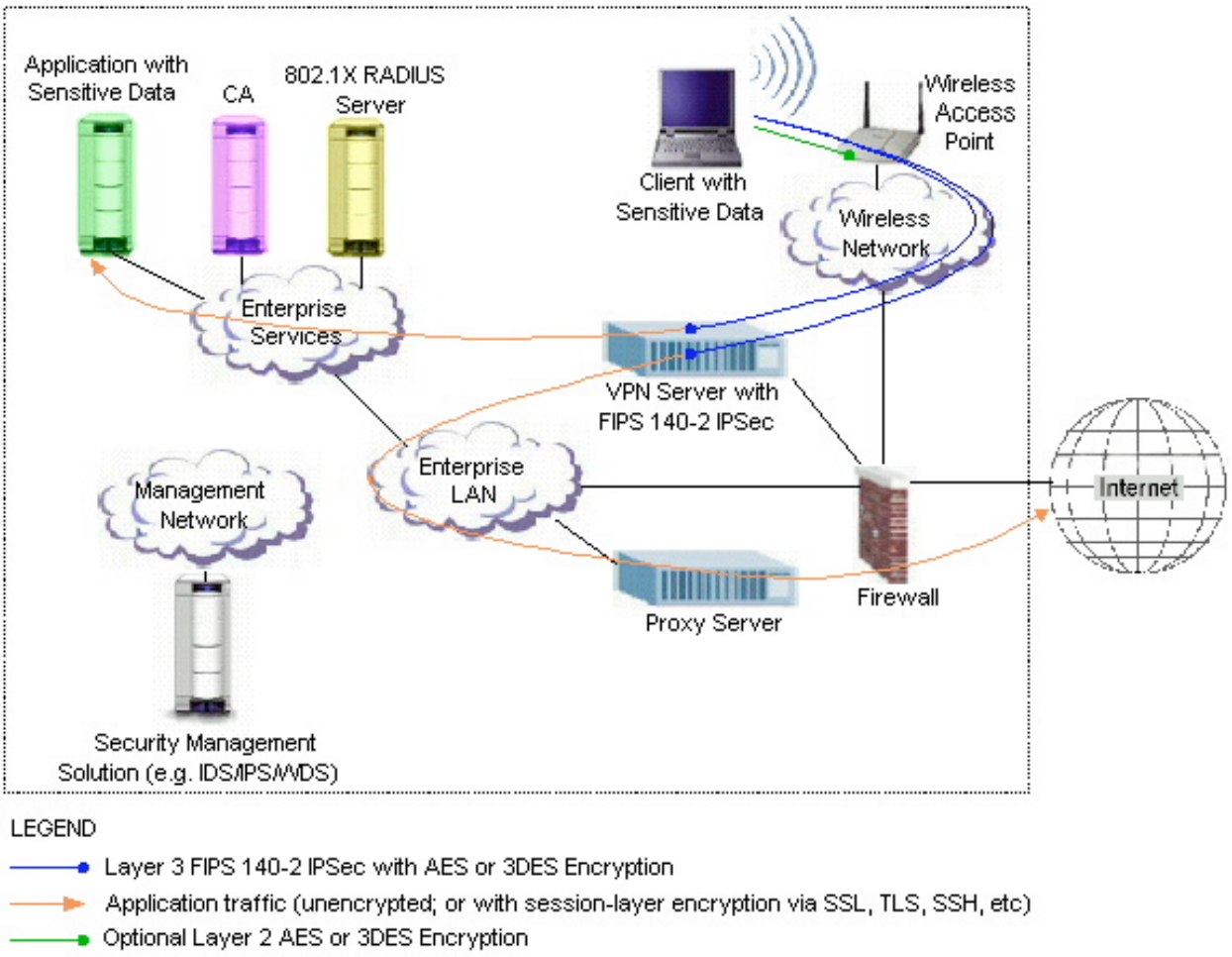

Figure 2-1. VPN Implementation of a Specialized Security WLAN

Alternatively, organizations may use a network architecture without a DMZ, if the wireless device is FIPS 140-2 certified. Federal Information Processing Standard (FIPS) refers to standards and guidelines developed and issued by the National Institute of Standards and Technology (NIST) for government-wide use in the United States. FIPS 140-2 specifies minimum cryptographic requirements to be used to process sensitive information. Refer to http://csrc.nist.gov/publications/fips/.

This alternative architecture, depicted in Figure 2-2, *Alternative Architecture for a Specialized Security Network*, does not adhere to the "defense-in-depth" principle, but it is sometimes necessary where a DMZ architecture is not feasible or is too expensive. It is important to note that, even with the use of FIPS 140-2 compliant encryption, this architecture remains vulnerable to layer 2 threats such as man in the middle and ARP attacks. The need for a robust security management solution, such as a wireless intrusion detection system (WDS), is imperative to guard against layer 2 attacks, which may slow or stop the network.

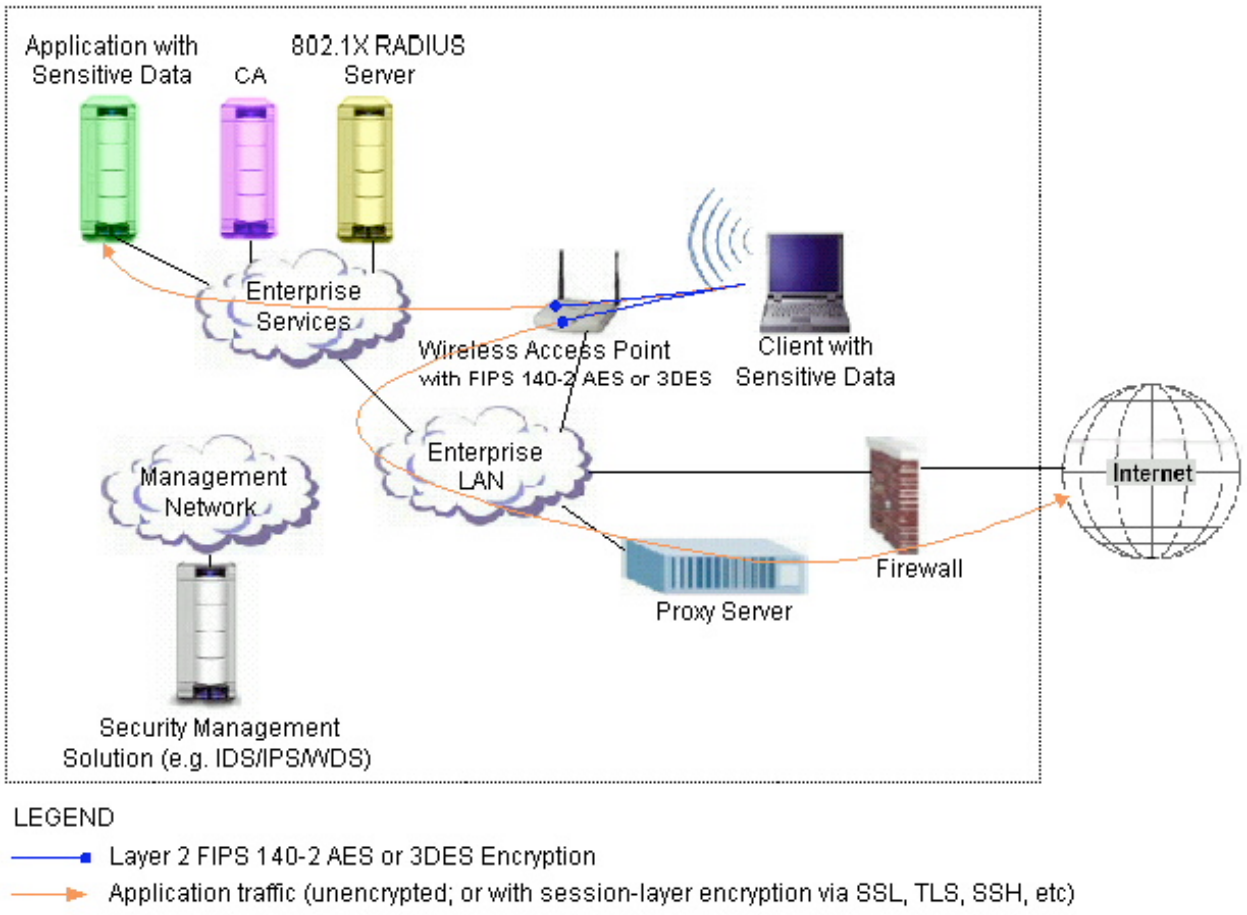

Figure 2-2. Alternative Architecture for a Specialized Security Network

Both architectures recommend using a network level security management solution (e.g., intrusion detection system (IDS)/intrusion protection system (IPS)/WDS) to monitor traffic traversing the WLAN. Both wired and/or wireless security management products can be used to monitor network traffic. There are a variety of methods available, depending on enterprise needs.

The enterprise airspace must be monitored, either periodically or continuously, for rogue (unauthorized) wireless devices, such as unauthorized access points connected directly to internal networks with sensitive information (thus creating a vulnerability for bypassing the enterprise firewall protections). High sensitivity environments may require 24x7 electronic screening using a wireless security management solution (e.g., IDS/WDS/IPS). A requirements-based evaluation should be performed to determine the best tool or tools for the environment as with all IA products. See the Appendix A, *Publications*, for a more complete list of references.

Table 2-1. Definitions of Architecture Components

Architecture Component	Component Function
Firewall	A firewall separates and protects networks. It may include VPN features.
VPN Server with a FIPS 140-2 certification	A VPN server provides access for devices outside the firewall through a secure tunnel. FIPS 140-2 certification provides the assurance required for specialized security requirements.
AP	A wireless AP bridges wireless client traffic to/from a network.
Management Systems (e.g. AP Manager)	An AP manager monitors and manages the configurations of APs.
Security Management Solution	This is a broad term which indicates use of one or more network level monitors such as a Radius Server, LDAP, wired IDS, wireless IDS, or etc.
RADIUS Server	802.1x authentication and encryption key management
LDAP Directory	Directories are databases for lightweight data (e.g. identification and authentication data) that are accessed using the LDAP protocol.
Intrusion Detection Systems (IDS)	Wired (IDS) or Wireless (WDS) intrusion detection (e.g. to detect rogue APs) as well as wired network intrusion detection systems are recommended for specialized security requirements.
CA	Certification Authorities (CAs) and related services are used to sign digital certificates that may be used for strong authentication or other security requirements. CAs are a key component of a Public-Key Infrastructure (PKI).

2.2 General Organizational Policies

Table 2-2. Security Best Practices

SECURITY BEST PRACTICES		
Policy Number	Requirement	Discussion
2.2.010	Establish configuration management procedures	This process should include: hardware and software architecture upgrade and patch management; architecture drawings, and a configuration control process.
2.2.020	Written information assurance policy and user agreement	This policy should train and inform users of the organization's security policies and the proper use of company-owned equipment. Require users' obtain approval to install, reconfigure, and operate **all** computing devices from the organization's designated approval authority.
2.2.025	Consider physical security as a part of your implementation.	AP and other wireless network devices must be physically secured or protected by an alarm to prevent tampering or theft. Users must be trained on physical security protections for wireless mobile equipment to prevent compromise or theft of WLAN clients.
2.2.030	Prohibit or control use of personally owned wireless devices	Do not allow use of personally owned wireless devices for storing or processing sensitive organizational information.
2.2.040	Maintain a list of wired and wireless network and client level devices used throughout the organization	Include AP and Client configuration settings such as: MAC addresses; IP addresses; channels used; Dynamic Host Configuration Protocol (DHCP) ranges; encryption algorithm used; SSID; manufacturer, model number, and serial number; and equipment location and assigned user.
2.2.050	Secure all functions of multi-functional wired and wireless devices	Most computing devices, particular handheld wireless devices are multi-functional. For example, a PDA can also be used as a network client or telephone. To secure these devices, the organization's security policy must be applied in all functional areas.
2.2.060	Require user security awareness training	Create or add wired and wireless networking security awareness to existing end user security education program to

SECURITY BEST PRACTICES		
Policy Number	Requirement	Discussion
		ensure end users are aware of the corporate information assurance (IA) policies. See wireless tools document for further information.
2.2.070	If possible, restrict use of wireless technology to less sensitive uses	Consider setting a policy to disallow use of WLAN devices **to access highly sensitive information.** Unless the environment or mission requires use of wireless products, the level of effort to secure such products and the many vulnerabilities associated with such products may mean taking on unneeded risks to highly sensitive data. Organizations must be aware of the risks associated with this technology and take exceptional measures to design security protections into the wireless solution chosen.
2.2.080	If possible, disallow use of WLAN devices in proximity to highly sensitive data.	Consider setting a policy to disallow use of WLAN devices in areas where highly sensitive information is stored or processed. The radios in wireless telephones, head phones, keyboards, etc. may emanate greater distances than expected. Conversations or data entry tones may be picked up via other wired or wireless devices in the area, which were not intended for sensitive data processing.
2.2.090	If possible, disallow use of embedded wireless NICs	If wireless devices will not be authorized for processing highly sensitive data, then consider setting a policy to disallow use of embedded/unremovable wireless NICs in client devices used: in areas where highly sensitive data is processed, for storing or processing highly sensitive information; connecting to wired or wireless networks processing or storing highly sensitive information.
2.2.100	Users must disable unauthorized wireless products before entering sensitive data processing areas	Except for authorized wireless devices, isable RF and IR on WPAN devices (e.g. Bluetooth) if allowed into areas where highly sensitive information is stored or processed. This will mitigate the risk inadvertent retransmission or capture of

SECURITY BEST PRACTICES		
Policy Number	Requirement	Discussion
		sensitive information; this is particularly needed if the area entered is using WLAN technology with which the WPAN device may attempt to autosync or autoconnect.
2.2.110	Disallow use of Bluetooth protocol	Do not use Bluetooth devices to store or process highly sensitive. These devices cannot be secured for use in processing highly sensitive data though use of such features as appropriate encryption algorithms for storing and transmitting data.
2.2.120	Use secure encryption algorithms such as AES	Configure WLAN devices to use secure encryption algorithms such as AES for transmitting highly sensitive information.
2.2.130	If possible, select wireless products which support PKI certificates	Use high or medium assurance PKI certificates for sensitive for transmission using wireless devices WLANs, if approved by approving authority. Use of PKI is a network infrastructure level service and is complex to implement. However, organizations processing highly sensitive or valued data should implement a PKI solution on the enterprise network.
2.2.140	WLANs must comply with host nation frequency management rules	Wireless products and WLANs slated for use in foreign countries must comply with host nation frequency management rules. Some protocol frequency ranges differ from those approved for use in the US.
2.2.150	Perform periodic assessment/screening of the WLAN	Perform assessments for unauthorized or rogue access points, stations, and bridges using an enterprise level wireless IDS, a wireless sniffer, or discover tool. Specific product selection will depend on the size and configuration of the WLAN and the available budget. Enterprises that do not have WLANs should also perform periodic wireless screening. Users or privileged administrators at the subnetwork or branch office level can easily introduce rogue APs and ad hoc networks. Both rogue APs and ad hoc networks can allow attackers access to the wired LAN from remote locations.
2.2.160	Separate the wireless network from the wired enterprise network using a	Install WLAN network level devices (AP, bridges) in DMZ or VLAN.

SECURITY BEST PRACTICES		
Policy Number	Requirement	Discussion
	VLAN or DMZ.	
2.2.170	If possible, disallow use of wireless remote access	Consider setting a policy to disallow use of wireless remote access (using wireless networks from home or public wireless network connections) to access highly sensitive information
2.2.180	If possible, disallow use of hotspots	Consider setting a policy to disallow use of hotspots by stations containing or having access to highly sensitive information
2.2.190	Client OS must comply with all exiting security policies	Operating system installed on client devices, including laptops, PCs, and personal electronic devices (PEDs), should comply with appropriate operating system benchmark and existing organizational configuration policies.

2.3 Wireless Hardware Configuration

2.3.1 Network Level Devices

This section applies to network level devices such as access points, routers, bridges, VPN appliances, and management gateways. Only checklist items detailing the recommendation for a specific setting are included in this section.

Table 2-3. Network Level Devices

POLICIES FOR WIRELESS NETWORK LEVEL DEVICES		
Policy Number	Requirement	Discussion
2.3.1.010	Use layer 2 or 3 encryption with AES	Layer 3 encryption with a FIPS 140-2 secure VPN solution is used to secure WLAN traffic to the internal network per the recommended architecture (Figure 2-1). This approach has the advantage of treating wireless access the same as remote access from the Internet – for organizations already equipped with VPN capability. Client devices connecting remotely must meet the requirements for wireless stations in the next section. The alternative architecture (Figure 2-1), which lacks defense-in-depth, relies upon Layer 2 encryption, which occurs between the AP and the client as part of the wireless network. Layer 2 encryption is optional for the recommended architecture, however a robust security management solution is required for protection against layer 2 attacks.
2.3.1.020	Choose products that support a network level security management solution.	IDS/IPS/WDS products monitor traffic as it traverses the WLAN. If this is not possible, then at least make sure that Remote Management is set to “Disabled”.
2.3.1.030	Disable management ports on network devices when not in use	In addition to physical access controls, secure strongly authenticated network access is desired in order to manage the AP in any highly sensitive environment. Secondary protection if this capability is not available is to password protect the port with strong two factor authentication.
2.3.1.040	Use OOB (out-of-band) management across a specially configured VLAN for network	For highest security, manage the APs out-of-band on a separate VLAN from user traffic. Do not manage APs from wireless

POLICIES FOR WIRELESS NETWORK LEVEL DEVICES		
Policy Number	Requirement	Discussion
	administration/management	interfaces. Instead, manage the devices from a separate, wired VLAN that is used only by network administrators with proper authentication credentials using appropriate tools (e.g., Secure Shell (SSH)).
2.3.1.050	WLAN must have session timeout capability and must be set to 15 min or less	This feature mitigates the risk of an abandoned, authenticated session being hijacked by an unauthorized attacker.
2.3.1.060	Set AP transmit power to lowest possible to attain signal strength required	This is a precaution, which can be easily thwarted by an attacker with a powerful antenna. Set AP transmit power to appropriately balance needs for coverage/interference and security.
2.3.1.070	Password-protect AP and bridges beyond manufacturer's default setting	Change default passwords to strong passwords consistent with the organization's security policy.
2.3.1.080	Change default SSID	Change the default SSID to a locally unique wireless network name that does not identify the host organization.
2.3.1.090	Disable SSID broadcast mode	Disable SSID broadcast mode to require users know the network name before associating. This setting does not prevent an experienced attacker from discovering the network's SSID but should be viewed as a part of a multilayered security posture.
2.3.1.100	Enable MAC address filtering	Enable MAC address filtering from a central server if automatic device network registration is operational within the enterprise. If automatic network registration is not operational, manual registration for an enterprise is probably not justified for wireless devices. This setting does not prevent an experienced attacker from discovering and spoofing an authorized MAC address but should be viewed as a part of a multilayered security posture. Bear in mind that MAC address filtering may adversely impact fast secure roaming.
2.3.1.110	Backup system configuration settings	Ensure enterprise level network products select can save backup configuration files onto another device (backup area on server). This requirement is similar to

POLICIES FOR WIRELESS NETWORK LEVEL DEVICES		
Policy Number	Requirement	Discussion
		saving wired router configurations in compliance with best practices for disaster recovery preparedness.
2.3.1.120	Enable Wireless Client Isolation	Disallow wireless clients from communicating with each other through an access point unless there is a business requirement for such communication.
2.3.1.130	Enable and configure logging	Review logs frequently; recommend the forwarding of alerts to central logging system.

2.3.2 Wireless Client Stations

This section applies to client devices which use the 802.11 protocol. These devices include workstations, laptops and Personal Digital Assistants (PEDs). It is not recommended that software AP implementations be used at this benchmark level. Mobile wireless computing devices are also not recommended, however, recommendations are included for mitigating risks to data stored or accessed by mobile devices. A more appropriate use for wireless at this benchmark level, would be as a wireless bridge or extension of the wireless network or in an area where a wired network or clients is not possible or practical.

With the acceptance of wireless standards, have come increase interoperability, thus most enterprise level WLANs will consist of multiple client NICs which may be different from the network level products used. For example a Cisco AP with 3COM and Cisco NICs. However, selecting products that can be made to comply with security best practices is essential to security wireless data in a sensitive environment. Table 2-4, *Wireless Client Station*s, lists the CIS recommended policies securing for wireless client devices.

Table 2-4. Wireless Client Stations

POLICIES FOR WIRELESS CLIENT DEVICES		
Policy Number	Requirement	Discussion
2.3.2.010	Disable recording on clients used in areas where highly sensitive information is stored or processed	Verify that client devices such as PDAs and other PEDs have the ability to disable recording or establish a policy that require users turn the devices off and physically disable the RF and IR ports.
2.3.2.020	Install and configure anti-virus software on all wireless devices	Verify that anti-virus software can be installed on all WLAN client devices, such as PDA and other PEDs, prior to purchase.
2.3.2.030	Password protect WLAN devices	Verify that WLAN client devices have password protection features beyond default settings. For PEDs, the device should zerorize after 3 unsuccessful password attempts. Be sure critical data and configurations are backed up frequently. Password protect critical files and folders to prevent access during hijacked authenticated sessions.
2.3.2.040	Install and configure host based firewall	Verify that host based firewall software can be installed on all WLAN client devices, such as PDA and other PEDs, prior to purchase.
2.3.2.050	Power off WLAN receivers and transmitters when not in use	Verify WLAN client device management software utility has this feature prior to purchasing. Users should be trained in this requirement to ensure this is done prior to entering sensitive area. If wireless communication is not needed for large periods of time, disabling wireless when not in use is a good security practice.
2.3.2.060	Enable mutual authentication for peer-to-peer WLANs	Peer-to-peer communications, also known as ad hoc networking, bypasses network based security and allows clients to directly communicate. This method is not a good practice in an enterprise environment. Mutual authentication occurs when each peer provides assurance of its identity. This can be done by using pre-installed PKI certificates or through use of other authentication protocols.
2.3.2.060	Use only wireless NICs that allow the disabling of peer-to-peer networking	Peer-to-peer communications, also known as ad hoc networking, bypasses network

POLICIES FOR WIRELESS CLIENT DEVICES		
Policy Number	Requirement	Discussion
	capabilities	based security and allows clients to directly communicate. Disable this feature to prevent inadvertent peer-to-peer communications.
2.3.2.070	For Windows 2000 and Windows XP systems, ensure most current service pack is used.	To mitigate existing vulnerabilities with the Windows Wireless Zero Configuration service do one of the following: - Disable WZC when using Windows 2000 and verify wireless NICs can operate with this service disabled; or - Ensure Windows XP, SP2 or greater is installed;
2.3.2.080	For mobile clients, set default setting to WLAN NIC radio to "Off"	This setting controls the status of the wireless NIC's radio upon bootup. Users should be aware of when they are communicating wirelessly. This setting, while inconvenient, will mitigate the risk to mobile devices containing sensitive data as this will force the user to actively initiate a wireless session only when needed. Ensure users are trained on the need to disable the radio when wireless communication is not needed.

This page intentionally left blank.

3. EVALUATED PRODUCTS CAPABILITY MATRIX

Tables 3-1 and 3-2 provide a quick reference matrix for reviewing the results of product testing done and research completed thus far by CIS. Detailed configuration guidance can be found in the product specific sections of each wireless benchmark.

The following checks in Table 3-1 are applicable only to network level wireless devices such as access points, bridges, routers, and etc.

Table 3-1. Evaluated Products Matrix for Network Devices

Policy Number	Requirement	Apple Airport	Cisco	Dlink	Linksys
Wireless Network Level Devices					
2.3.1.010	Use layer 2 or 3 encryption with AES.	No	Yes	No	Yes
2.3.1.020	Choose products that support network level Security Management Solution			Not tested	
	Allow separate NIDS device	Yes	Yes		Yes
	Built-in NIDS	Yes	Yes		No
	Remote syslog for NIDS event-correlation	Yes	Yes		No
2.3.1.030	Disable management ports on network devices when not in use	Yes	No	Yes	No
2.3.1.040	Use OOB management across a specially configured VLAN for network administration/management	Yes	Yes	No	No
2.3.1.050	WLAN must have session timeout capability and must be set to 15 minutes or less	No	Yes	No	No
2.3.1.060	Set AP transmit power to lowest possible to attain signal strength required	Yes	Yes	Yes	No
2.3.1.070	Password-protect AP and bridges beyond manufacturer's default setting	Yes	Yes	Yes	Yes
2.3.1.080	Change default SSID	Yes	Yes	Yes	Yes
2.3.1.090	Disable SSID broadcast mode	Not tested	Yes	Yes	Yes
2.3.1.100	Enable MAC address	Yes	Yes	Yes	Yes

Policy Number	Requirement	Apple Airport	Cisco	Dlink	Linksys
Wireless Network Level Devices					
	filtering				
2.3.1.110	Backup system configuration settings	Not tested	Yes	Not tested	Yes
2.3.1.120	Enable Wireless Client Isolation	Not tested	Yes		Yes
2.3.1.130	Enable and configure logging	Yes	Yes	Not tested	Yes. WAN interface only

APPENDIX A. PUBLICATIONS

Books

Peikari, Cyrus and Fogie, Seth. Maximum Wireless Security. Sams Publishing, Indianapolis, IN, 2003.

Wireless Communication Standards - A Study of IEEE 802.11, 802.15, and 802.16, Todor Cooklev, IEEE Press, 2004.

Real 802.11 Security - Wi-Fi Protected Access and 802.11i, Edney and Arbaugh, Addison Wesley, 2004.

Wi Foo: The Secrets of Wireless Hacking", Andrew Vladimirov, et al, Pearson / Addison Wesley, June 2004.

Standards

IEEE Computer Society LAN/MAN Committee, IEEE Std. 802.1X-2001, IEEE Standard for Local and metropolitan area networks— Port-Based Network Access Control, Institute of Electrical and Electronics Engineers, Inc., New York, NY, June 2001.

IEEE Computer Society LAN/MAN Committee, ANSI/IEEE Std 802.11, 1999 Edition, Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements—Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Institute of Electrical and Electronics Engineers, Inc., New York, NY, 1999.

Web Articles

Gast, Matthew. "A Technical Comparison of TTLS and PEAP". October 17, 2002. http://www.oreillynet.com/pub/a/wireless/2002/10/17/peap.html (from the author of 802.11 Wireless Networks: The Definitive Guide)

Microsoft Corporation. "Enterprise Deployment of Secure 802.11 Networks Using Microsoft Windows". December 30, 2004 http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/ed80211.mspx

Web Sites

http://www.wi-fi.org/OpenSection/index.asp?TID=1

http://www.wi-fi.org/OpenSection/certified_products.asp?TID=2

http://www.wlana.org/

http://standards.ieee.org/wireless/

APPENDIX B. ACRONYMS

AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard
AP	Access Point
CIS	Center for Internet Security
DAC	Discretionary Access Control
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DISA	Defense Information Systems Agency
DoD	Department of Defense
DOS	Denial of Service
DSL	Digital Subscriber Line
DSSS	Direct Sequence Spread Spectrum
EAP	Extensible Authentication Protocol
EDGE	Enhanced Data Rate for Global Evolution
E-mail	Electronic Mail
FCC	Federal Communications Commission
FHSS	Frequency Hopping Spread Spectrum
FIPS	Federal Information Processing Standard
GHz	Gigahertz
GSM	Global System for Mobile communications
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transport Protocol
HTTPS	Hyper Text Transport Protocol - Secure
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
IPS	Intrusion Protection System
IPSec	IP Security
LAN	Local Area Network
LEAP	Lightweight EAP
LDAP	Lightweight Directory Access Protocol
MAC	Media Access Control
NIC	Network Interface Card

OS	Operating System
OOB	Out of Band Management
PAN	Personal Area Network
PCI	Peripheral Component Interconnect
PCMCIA	Personal Computer Memory Card International Association
PCS	Personal Communications Service
PCT	Private Communication Technology
PDA	Personal Digital Assistant
PEAP	Protected Extensible Authentication Protocol
PED	Personal Electronic Device
PIM	Personal Interface Module
PKI	Public Key Infrastructure
PPP	Point-to-Point-Protocol
PPTP	Point-to-Point Tunnel Protocol
RADIUS	Remote Access Dial-in User Service
RAS	Remote Access Server
RSN	Robust Security Network
RF	Radio Frequency
SID	System Identifier
SMS	Short Message Service
SSH	Secure Shell
SSID	Service Set Identifier
SSL	Secure Sockets Layer
SOHO	Small Office/Home Office
STIG	Security Technical Implementation Guide
TCP	Transmission Control Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TTLS	Tunneling TLS
USB	Universal Serial Bus
VPN	Virtual Private Network
VoIP	Voice-over-IP
WAP	Wireless Application Protocol
WDS	Wireless Detection System
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity

WISP	Wireless Internet Service Provider
WLAN	Wireless LAN
WLANA	Wireless LAN Association
WMAN	Wireless Metropolitan Area network
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network
WZC	Wireless Zero Configuration