Global Information Assurance Certification Paper

Topics in Auditing- High Level Review of WLAN (Version 2)

Philip J. Coran

SANS GSNA Practical (v2)

July 17, 2002

Table of Contents

1. GSNA Assignment I - Research in Audit, Measurement Practice and Control

1.1 Introduction- What is Wireless Networking (WLAN)? Why Use It?

While wireless technologies include infrared, microwave, and radio frequency, the focus of this audit will be on the common 802.11b radio frequency protocol (approx. 2.4GHz band). The industry standards group IEEE ratified the 802.11b standard in 1999[1]. Wireless networking is simply a new method of transporting data without wires. In theory, the 802.11b can provide wireless network transfer speeds of up to 11 Mbps. Furthermore, many specialized variations of wireless network technologies are starting to merge together to provide seamless resource connectivity and sharing, which reduces implementation and operational costs.[2] The typical coverage of 802.11b wireless device is several hundred feet, though this can increase to several miles based on the transmission power and the local geography. Wireless networking cards can be found for less than $100 and wireless access points –WAP's (transmitters) under $200. Companies are rapidly adopting Wireless Networking technologies; nearly 20% of companies surveyed by Sage Research currently have wireless networks installed.[3]

WLAN may be used to support network connectivity without physical connections to clients. This technology is often considered a convenience for users and a lower cost option compared to its wired counterpart.

1.2 Focus of Assessment/Audit

The purpose of this audit is to assess the use and security of WLAN used by my organization (ABC) at a specific site. WLAN is used to provide a wireless bridge to the local area network. Specifically, this review will accomplish the following:

- Analyze the WLAN related preventative controls utilized by the site since frail preventative controls can lead to poor service, weak security, uncontrolled/unmonitored growth of WLAN, rogues, and misuse of the technology. Weak WLAN security can have serious implications on overall network security and decrease information privacy and information integrity.
- Determine the basic (encryption, network naming and broadcasting) security settings for the WLAN found at selected major site(s) in the context of a routine comprehensive Financial and IT Audit. These settings have serious ramifications on network security if misconfigured.
- To determine if rogue (unofficial) AP's have been created at the site(s) and the extent of the site's efforts to detect and control rogues. Rogues constitute a serious threat to network security, and can be exploited to gain access to sensitive information, deny service, etc.
- Report findings of the assessment to management to help strengthen controls.

1.3 Risks and Vulnerabilities of Wireless Networking and 802.11B

While there are many advantages to wireless networking, there are as many, if not more, risks to consider. The technology has inherent risks to message integrity, confidentiality, and authenticity.

The most commonly noted vulnerabilities include:

- Rogue Wireless Networks - a wireless network emanating from within the organization and operating without approval
  - *"Wireless LANs are a stealth technology. Most IT departments in large organizations are significantly underestimating how much wireless has already been installed by enterprising departments, as well as individuals." (Jonathan Gossels, President of SystemExperts Corporation)*[4]

- Improperly Configured Wireless Networks
  - Standard encryption security on the 802.11b devices (known as *Wired Equivalent Privacy* or "WEP") settings are set to off when shipped. The site may not enable WEP on its AP's and clients.
    - *"The combination of low cost and ease of deployment is leading to rapid adoption… In many organizations, the deployments are so rapid that the situation is out of control; individual departments are setting up wireless environments that ... are not configured to provide security at the same level as the organization's security policies require for [wired] networks carrying data of comparable value (SystemExperts' Vice President Brad Johnson.)*[5]

    - *A RSA Security chartered a study in London that showed 67 percent of the WLANs ... had no security. Other surveys of New York, Boston and San Francisco indicated that over 50 percent of WLANs deployed were not secure.*[6]

- Risks Inherent to Wireless and 802.11b Protocol & WEP. WEP is the common, non-proprietary security system available on 802.11b WLAN networks. The following vulnerabilities all increase the risk to information integrity, confidentiality, authentication, and availability (through Denial of Service). The following is taken from a recent ISACA Magazine Article:

  The goal of WEP was to provide a level of security commensurate with that found on wired LANs (aka Wired Equivalent Privacy). Since wired networks are not generally very secure unless protected by measures beyond those provided by the network protocols. Many have experienced connecting a computer to a wired LAN and being able suddenly to access resources to which they had no right. This is a common problem, usually controlled by limiting which computers may physically connect to the LAN. However, in the wireless domain, it is more difficult to limit who can connect to the LAN. Coupled with weak key management and a restricted key space, WEP is demonstrably insecure. Researchers also have shown it is possible to listen to packets, inject packets

(leading to a potential denial of service) & alter packets on wireless LANs using WEP[7]

- Static Encryption Keys: WEP relies on the use of identical static keys deployed on client stations and access points. Thus, key management becomes quite difficult as the number of clients increases and the confidentiality of the key decreases with time.

- RC4 Initialization Vector: WEP produces RC4 keys that were too similar and easy to attack. WEP in its current form is flawed because it produces weak RC4 keys. It uses a straightforward and predictable way of incrementing the vector from one packet to the next[8].

    - *While the WEP standard had specified using different keys for different data packets, the key derivation function (how to derive a key from a common starting point) was flawed. Simply put, the keys for different data packets were too similar. Hackers could exploit this similarity to extract information about the shared secret after analyzing a modest number of packets. Once the shared secret was discovered, a malicious hacker could decrypt data packets being passed along the exposed network.* [9]

- Clear Text Service Set Identifier (SSID): a SSID is a unique identifier in the header of packets sent over a WLAN that acts as a password when a mobile client attempts to connect to a specific WLAN network. The SSID is a common network name that clients must have to connect to a specific WLAN. Because an SSID is in plain text and can be sniffed from a packet it does not supply any security to the network.[10] Furthermore, many access points are defaulted to broadcast the SSID for anyone with a Wireless Card and sniffer to see. This only serves to help potential intruders. Additionally, Machine Addresses (MAC) are sent in the clear even with WEP enabled. Both SSIDs and MACs can be exploited by intruders.[11]

- Eavesdropping- Non-private nature of radio frequencies; i.e. anyone can access given the right equipment and range though the information may be of little use due to encryption.

    - Signal extending beyond estimates (Basic Service Set – BSS is an access point) into other non-company areas. Does the network overlap with others? See Exhibit II

The *CANAUDIT*[12] (Exhibit 1) depiction below shows how an unauthorized user may bypass other controls to gain access to a network. The second (original) depiction indicates how WLAN signals may go beyond organizational boundaries and be accessible to other parties.

Exhibit 1

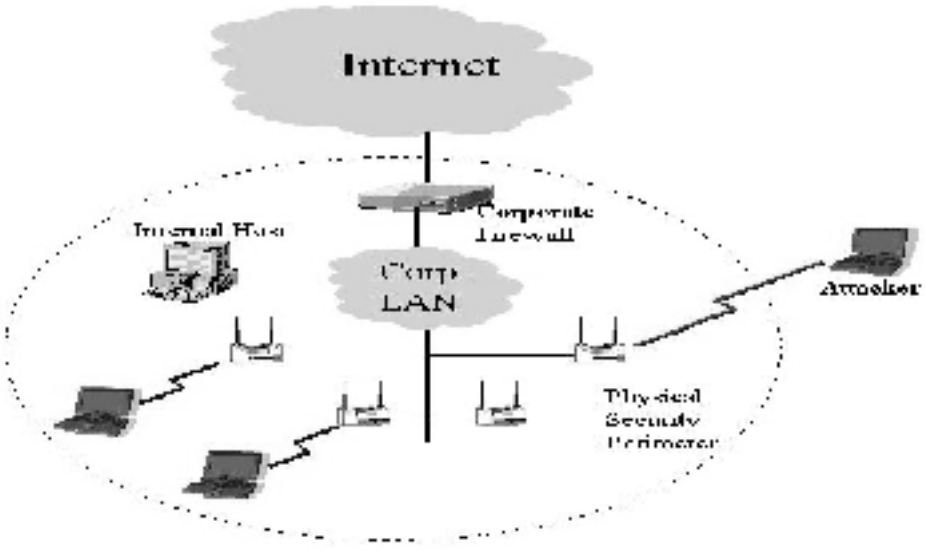
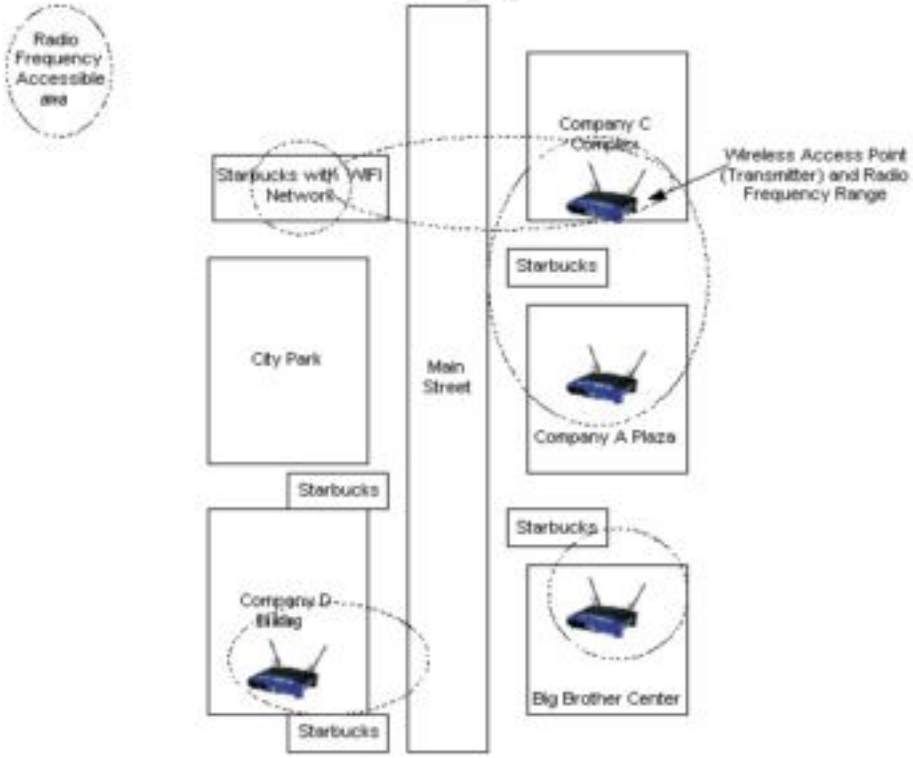


Exhibit II



1.4 Likelihood of Exposure Due to Wireless LAN

Based on my research, I believe there is a high likelihood of exposure due to improperly set up or rogue WAP's. *As quoted by SystemExperts' Vice President Brad Johnson in Computer Security Magazine*, "Businesses don't have the discipline, controls, or policies

in place to handle the dynamic nature of wireless components. Most security guidelines are geared towards the more slowly changing wired environment that, in many cases, forces the end-user to get help or permission to change their computing environment. The result of this truth is that the prevalence of insecure WLANs is not that organizations are failing to take associated security issues seriously, he concludes, but that they simply do not have the tools or knowledge in-house to oversee this quickly evolving technology."[14]

A rogue or poorly configured WLAN Access point could serve as a backdoor to the company network and provide unauthorized users a portal into the company network. From this opening, unauthorized users would be relatively free to *attempt* to access, attack, disrupt, lock, utilize, modify, steal, and take control of network resources and company information. Such an incident could be detrimental to network security, data integrity, information privacy, and even an organizations reputation. Furthermore, it would drain company resources available to act on other issues and normal operations.

1.5 Potential Consequences of Wireless Networking

Due to the inherently open nature of a wireless network and the relative anonymity of wireless connections, wireless networks are becoming a popular exploit and backdoor into networks.[15]

Coupled with threats such as hackers, snoopers, and unethical employees, there are significant risks posed to networks, information privacy, data integrity, and legal liability. If the wireless LAN is intended for access to a corporate network, the information gathered could be subsequently used to impersonate a legitimate user or device to perform a network intrusion. It is very difficult to detect when someone is sniffing the WLAN.[16]

1.6 Current State of Practice

Based on my research, I was unable to find a specific published assessment methodology that would cover the broad ground this project is designed to cover. There were several resources that were published on SANS and computer security forums that detailed methods to "War Drive", detecting rogue access points, and testing configuration of specific WLAN hardware for security vulnerabilities. The following include a list of documents that are related to this project. These documents were found by conducting web searches, reviewing documentation in the SANS reading room, and reviewing previously posted practical assignments for the GIAC certification.

1.6.1 Related Audit Programs

- *Initial Wireless Networking Audit for Higher Educational Institutions* Contributed December 7, 2001 by Jim Dillon http://www.auditnet.org/docs/wireless.doc
    - This document is oriented towards educational institutions that have already developed formal approaches to WLAN implementation. The audit plan is primarily focused on the cost benefit, development controls, analysis and policies regarding the usage and implementation of WLAN.
    - The audit program contains one control objective to test on rogue networks but does not go into detail on how to test this.

- The audit program appears to be focused on post implementation issues.

- *Auditing a Wireless Access Point: The Orinoco Outdoor Router 1000 Configured as a Wireless Access Point* Contributed by Slawomir Marcinkowski February 10, 2002 http://www.giac.org/practical/Slawomir_Marcinkowski_GSNA.doc
  - This document is oriented towards a specific hardware device though it covers a myriad of control concepts applicable to WLAN APs.
  - The audit program appears to be designed to audit from within the organization, testing specific items that only administrators should have access to (ACLs, Settings, etc.).

- *Wireless LANs: The Hacker's Best Friend Contributed by Chad Parks* of Canaudit Inc. November, 2001 http://www.canaudit.com/Articles_Pubs/past_articles/Nov01_perspective.htm
  - This article offers some helpful information on vulnerabilities posed by WLANS. It offers an outline (with more details available for a fee) of a generic WLAN audit program.

1.6.2 Related Articles

While there is no shortage of articles and published reports on WLAN security, the most heavily relied upon pieces have been posted in this report as endnotes. The most heavily used are as follows:

- Klemencic, Joe. "Basic Security Mechanisms for Wireless Networks." July 16, 2001 http://online.securityfocus.com/infocus/1199
  - A higher level overview of WLAN risks and protection measures.
- Stanley, Richard A. "Wireless LAN Risks and Vulnerabilities" Volume 2 2002. Information Systems Control Journal
  - A helpful overview of WLAN vulnerabilities aimed at the Auditor. It also offers rich references to other articles and sources.
- Armstrong, Illena . "Today's Telecommuting World." February 2002. Computer Security Magazine http://www.scmagazine.com/scmagazine/2002_02/main.html
  - A comprehensive and mid level overview of WLAN security issues
- Owen, Daniel. "Wireless Networking Security: As Part of Your Perimeter Defense Strategy" January 23, 2002. http://rr.sans.org/wireless/netsec.php
  - A detailed research article, you must register with SANS to access.
- Benjamin Huey, Penetration Testing 80211.b Networks, page 9, http://rr.sans.org/wireless/test.80211b.php, 2/24/02
  - A detailed research article, you must register with SANS to access.
- Convery, Sean. SAFE: Wireless LAN Security in Depth. by CISCO in 2002. www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm
  - A detailed whitepaper on WLAN security including CISCO's proprietary dynamic encryption and radius authentication enhancements.

1.7 Suggested Improvements to Audit Techniques

Due to the substantial risks inherent in wireless networking, organizations should be prepared to conduct assessments to determine the extent of controls on wireless technologies emanating from their site(s). Though audit programs are already available

that include work programs for specific hardware types (i.e. a specific brand of wireless routers) and implementations; I have been unable to find a broad, higher-level wireless assessment program. The work program I am proposing is designed for the auditor (including the IT auditor and technologically savvy financial auditor) who is interested in conducting a high level audit on a site's use of WLAN. It is designed to provide the auditor with a picture of how pervasive WLAN is at a site (or site sample for larger organizations) and how controlled it may be. Also, the auditor can utilize a less complicated hardware setup in the event that their hardware and operating system use is limited to the Win9X platform. From this vantage point, the auditor can encourage more focused audits to explore added specific controls on the site WLAN.

As the technology is relatively new, the organization may have yet to designed specific policies, standards, and procedures to govern the use of WLAN. Without such policies and standards, a formal, full-scope audit may be premature.

1.8 Subjective Measurements of WLAN Security

The auditor needs to determine how pervasive use of WLAN is at the site to be audited. This will provide the auditor with a subjective view on the risk the site may be exposed to given the variables (location, WLAN security). Such risks can be mitigated by:

- Pervasive Controls[17]; SOP's-policies & procedures, training
- Detective Controls[18]: self audits, internal reviews

1.9 Objective Measurements of WLAN Security

The auditor can use tools and evaluate specific settings on the WLAN. Examples of objective areas include

- Specific Controls: settings on WLAN- i.e. WEP, SSID (the WLAN Network Name or Service Set Identifier) to be determined using a tool such as Network Stumbler- see page 11 for further details
- Detective/Monitoring Controls: Intrusion Detection Systems monitoring network with WAP's attached
- Preventative Controls: Added firewall protection on segments containing WAP
- Corrective Controls- policies or processes to correct exceptions

2. GSNA Assignment II: The Audit Checklist

The assessment checklist is organized in four stages and is outlined in the following tables and commentary. The results "grade" for each step is indicated as follows:

	Control is Satisfactory and appears to be operating effectively.
	Control is partially effective and can be improved. Enhancing control may be available.
	Control is mostly ineffective and should be improved. Also applies to where an additional control can be implemented that would significantly improve the control environment.
	The control is not operating effectively or does not exist. An appropriate control needs to be implemented.

N/A	No grade applies

2.1 Define Assessment Scope and Pre-audit Administrative

The auditor needs to determine the scope and objectives of the assessment. Once determined and documented, the auditor should present the proposal to Audit Management to obtain permission (written) and guidance. This is necessary for the assessment to continue.

Procedure 1- Permission	Permission/Notification	*Type*: **S**ubjective / **O**bjective	S
Reference:	N/A - generally recommended practices		
Risk:	The auditor may have not obtained formal permission from Audit Management to perform the audit. The lack of approval may be detrimental to the auditor and their department.		
Compliance:	A field letter sent to the site will include notification of the WLAN audit and list of information requests. The field letter should be sent within standard timeframes of the audit process. If it is the first site-audit with WLAN within scope, the auditor will make a special effort to contact the site to ensure they understand the audit scope.		
Testing:	Verify that audit management is aware and supports the audit plans. Also confirm that client management is aware of audit group's intentions to audit WLAN.		
Rating		*Date*	*Auditor*	*Reviewer*
Comments:	The assessor should be cautious in making plans to conduct an *unannounced* review. If he or she goes to a site unannounced, the personnel at the site may catch-on and confront the auditor- leading to an awkward, relationship-damaging situation. Your hat color may come into question while you are exploring the site with an antenna-equipped laptop. It is my opinion that an announced assessment is preferable, as it will seem "fairer" to the assessed facility even though it has some potential to bias the results of the assessment.		
Follow up:			

Procedure 2- Determine Scope	Audit Scope and Objective	*Type*: **S**ubjective / **O**bjective	S
Reference:	Generally recommended practices, part of the concept from CISA Methodology[19]		
Risk:	Audit may choose audit samples or locations without prior knowledge pertaining to the site, facilities and capabilities. Audit resources may be used inefficiently and disrupt client site with unneeded questions and exercises.		
Compliance:	Audit has necessary information to select auditable areas, choose proper staffing and hardware/software. Audit sets expectations for itself and client.		

Testing:	Audit plan is utilized and complete no later than two weeks prior to audit. The audit plan is modifiable based on fieldwork, but significant scope/timing changes should be reported to audit management and client site management.						
Rating		*Date*		*Auditor*		*Reviewer*	
Comments:	This is an audit QA step.						
Follow up:							

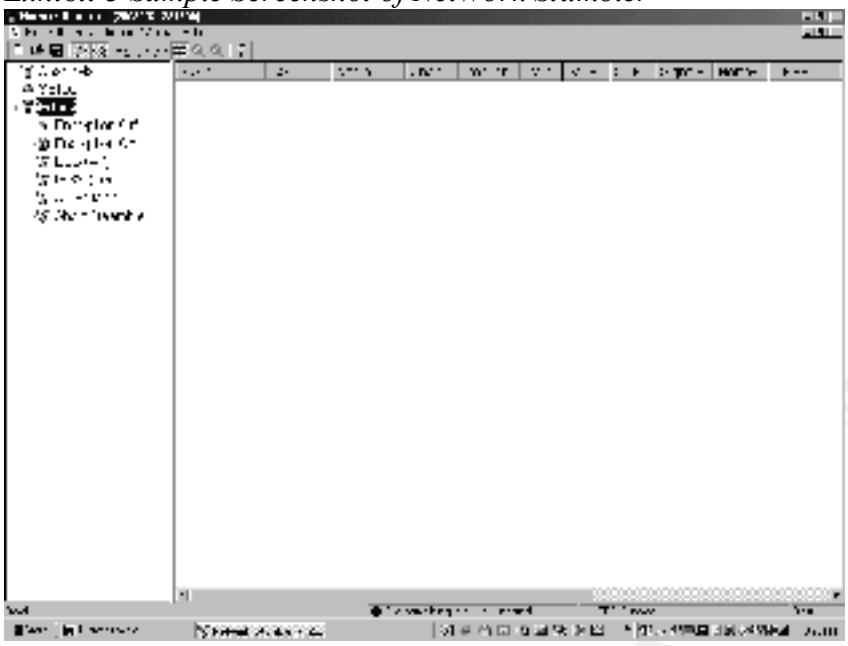
Procedure 3- Validate Testing Equipment	Validating Equipment/Software	*Type*: **S**ubjective / **O**bjective	O
Reference:	Software Utilities, Windows Utilities (control panel, etc.)		
Risk:	The auditor's toolset may not be operating properly, rendering the tools useless or inaccurate.		
Compliance:	Auditor has familiarized himself/herself with testing tools and software. His/her tools have been tested to verify they are working correctly.		
Testing:	1-Test the Wireless Networking Card using control panel and or NIC utilities. 2-Test the scanning/sniffing software (NetStumbler, Airsnort[20], etc.) against a known system. This step will be repeated before WLAN testing is conducted to ensure proper functioning.		

Rating		Date		Auditor		Reviewer	
Comments:	A known system is a known WAP.						

The assessor should have a proven test system available for their use and be familiar with the proper functioning of the test tools. A recommended tool for this type assessment would be *Network Stumbler*[21], a free tool that works on Windows platforms. It is relatively simple to use and can be operated on a modest laptop. It is not a packet sniffer tool, though it is able to indicate which visible (Service Set ID broadcasting) systems may be accessible in at a location. A tool should be on a promiscuous mode and operating with a properly functioning wireless networking card. Another tool that can sniff and can be used to crack WEP is Airsnort. This tool requires a UNIX platform to run. Network Associates has a commercial scanning tool called "Sniffer Wireless[22]" that can view WLAN traffic and can decrypt WEP encoded packets.

The assessor has a myriad of choices available in terms of boosting their capacity to receive AP signals. Choices include multi decibel antennas of differing types[23] including directional, omni directional, patch antennas, yagi, arrays, and even home made antennas. Gains vary; I recommend that you choose an antenna that will allow you to discover access points more easily (omni directional) since you will probably be conducting walkthroughs without actually knowing the locations of all WAPs. A directional antenna can allow you to further hone in on the location of a WAP. The higher the gain, the better the chance that you detect weaker or more distant WAPs. Another useful tool is a GPS device that can be used to precisely tie a location to the reception areas of a WAP. The Network Stumbler tool has functionality built into the software to work with a GPS unit that can be connected to your testing hardware.

Exhibit 3 Sample Screenshot of NetWork Stumbler



2.2 Pre Audit Planning- Obtain Relevant Background Information

The major risk that this step applies to is that Management at the site is not aware of divisional or corporate guidelines and may have set up WLANs that do not conform to policies.

If there are standards and policies available, the assessor may further tailor the assessment towards measuring compliance at a later stage. Conversely, if there are no policies and documentation available, the assessor should note this and continue on the assessment. A lack of such information should be reported to management. The auditor may have to interpret information security policies if they do not specifically address WLAN. Interpretations on general information security policies should be confirmed with Audit Management if auditor feels policies also apply to WLAN. The auditor does not set policies and procedures and should be reluctant to be put in this position. However, the auditor can subjectively measure policies and procedures for appropriateness, timeliness, and completeness.

Procedure 4- Strategy & Implementation	Assess WLAN Strategy and Implementation	*Type*: **S**ubjective / **O**bjective	S
Reference:			
Risk:	The site may have installed WLAN in an unstructured way leading to loss of efficiencies, inconsistent quality and security, and potential service outages.		
Compliance:	For significant WLAN projects, the site should have a detailed plan, timeline, standards, and objectives for WLAN.		

Testing:	-Obtain site level (or a plan that includes the site) WLAN implementation plan, maintenance plan, etc. This plan should detail WLAN strategy, budget, security concerns and remedies. -Review an inventory of WLAN WAP's and NICs for timeliness and detail. While we are not actually confirming the accuracy of the lists, the presence of these documents does lean towards some degree of change control and monitoring. Equipment standards can also be determined from this list, assuming the equipment is standardized. -If new guidelines on WLAN have been released from Corporate sources, is the local site aware? Does the site have a plan of action to address new standards? What is their progress?						
Rating		Date		Auditor		Reviewer	
Comments:							

Procedure 5- Preventative Controls	Determine Preventative Controls - Policies and Procedures at / or applicable to site	*Type*: **S**ubjective / **O**bjective	S
Reference:	Corporate Policies or site-specific policies depending on the stronger of the two.		
Risk:	Site may be operating WLAN outside of company policies, leading to differing standards, eroded security, and loss of efficiencies.		
Compliance:	Site should have policies and practices to cover WLAN usage and security.		
Testing:	Obtain and review local policies and practices, governing policies and procedures if the site adopts from another source. Obtain and review user awareness documentation that covers WLAN. In spite of there being policies, these policies *may* not be explicit or timely enough to be effective and could be enhanced. This is the subjective aspect of the testing.		

Rating		Date		Auditor		Reviewer	
Comments:							

Procedure 6- Detective Controls	Detective Controls	*Type*: **S**ubjective / **O**bjective	O
Reference:			
Risk:	Management may not be aware of improper WLAN activity and network resources may be compromised.		
Compliance:	Management uses a utility to monitor WLAN traffic for unusual occurrences, potential exceptions. If exceptions are found, this will lead to the finding and disabling of rogues as well as misconfigured official WAPs.		

Testing:	Understand nature of extent of monitoring or detective controls, document successful "catches". An IDS or Firewall on the segment containing WLAN is a good indication of a system based detective control and pervasive control.						
Rating		Date		Auditor		Reviewer	
Comments:	These refer to tools and efforts designed to catch or detect exceptions to policies; or unusual occurrences that may signify a control issue. This may be considered a back-end control depending on when the exception occurrence is noted.						

Procedure 7- Information Security Ownership	WLAN Security Owner	*Type*: **S**ubjective / **O**bjective	S
Reference:	If the organization promotes Information Security Ownership (ISO) as a guideline, this added control might be contributing towards better WLAN controls. This depends on your organization.		
Risk:	Without information security ownership, security concerns may be overlooked or passed over when dealing with new technologies, etc.		
Compliance:	The site (unless very small) has an ISO or equivalent who is responsible for Information Security issues. This individual or group should be aware of WLAN initiatives locally and that of Corporate.		
Testing:	Meet with ISO or equivalent, learn about their level of understanding on this area and discuss what any plans, policies, etc. that may be applicable to the site. Lack of understanding may result from either lack of information flow from corporate, inadequate training on ISO, and or a lack of interest.		
Rating		Date	Auditor	Reviewer
Comments:	This is a recommended practice, based on the author's work experience.		

2.3 Audit Steps in the Field

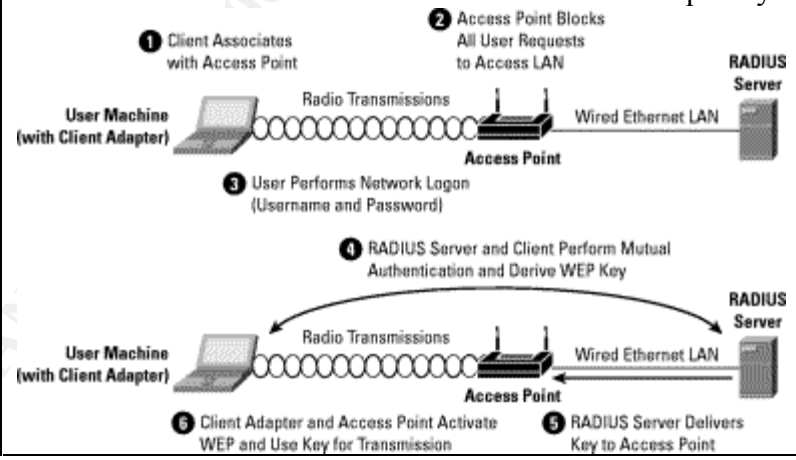
The auditor shall actually conduct most of the interviewing and detail testing during this stage. The assessor needs to determine the extent of controls in place down to which actual locations are to be assessed. He/she will also scope the extent of the testing- indoor, outdoors, organization campus only, etc. He/she may go as far as going to a non-company location adjacent or near a site to assess WLAN (with permission of course if the location is not on public property). Leave some wiggle room once you are at the site in case you determine that an alteration or addition may be helpful. Also keep in mind outside groups, such as vendors who may be attached to corporate network and may have established their own WLAN, attached in someway to your organization's network.

Procedure 8- Firewall Protection	Data Gathering - Firewall Protection	*Type*: **S**ubjective / **O**bjective	O
Reference:	SANS GSNA Course Material- Penetration Testing 802.11B Networks[24]		
Risk:	The LAN may be under attack and compromised due to weaknesses in the WLAN.		
Compliance:	Management is utilizing a firewall in front of the Access Points to protect resources from WLAN originating attacks. Activity should be logged, monitored, and reviewed.		
Testing:	Discuss with management any firewall type efforts (router or software based) that may limit activity from subnets that feature WAPs. Are logs reviewed?		
Rating		Date		Auditor		Reviewer	
Comments:	The firewall settings should be audited in a separate review for appropriateness. For now a high level understanding is within scope of this review: purpose of firewall, allowed services, logging.		

Procedure 9- Encryption Key	Data Gathering- Encryption Level and Key	*Type*: **S**ubjective / **O**bjective	O
Reference:	SANS GSNA Course Material- Penetration Testing 802.11B Networks[25]		
Risk:	Encryption key may be easily guessable or sequential, rendering it largely ineffective. A lower level of encryption (40 bit) makes it much easier for a password to be brute force cracked.		
Compliance:	Encryption key is not easily guessable, high encryption level utilized (128 bit)		
Testing:	Review the WEP key; destroy record of key after review.		
Rating		Date		Auditor		Reviewer	
Comments:	This is a cursory review; does the key seem "random"? Or is it sequential i.e. abcdefghighk…..? This test does not validate the weaknesses of WEP. What is the encryption strength?		

Procedure 10- Encryption System	Encryption System	*Type*: **S**ubjective / **O**bjective	O
Reference:	GSNA SANS Course Material[26]		
Risk:	The integrity of the 802.11b WEP key erodes with time due to its static nature. Static keys are more vulnerable to being compromised with time and increasing user base.		
Compliance:	The site uses a different method of encryption than WEP. This security should be superior to that of WEP. WEP is considered as a minimum-security level and may be insufficient if improved encryption schemes are approved of by IT, etc. One such proprietary encryption scheme is CISCO LEAP[27] which uses asymmetric keys and authenticates to the RADIUS server.		

Testing:	Review the WEP key. Determine if a different encryption from WEP is used or shall be implemented in the near future. Does current encryption scheme comply with corporate guidelines if applicable?						
Rating		Date		Auditor		Reviewer	
Comments:							

Procedure 11- Improved Authentication	Added Authentication	*Type*: **S**ubjective / **O**bjective	O
Reference:	SANS GSNA Course Material- Penetration Testing 802.11B Networks[28]		
Risk:	Users do not need to authenticate to the company network to access the WLAN, thereby reducing network security. This is an enhancing control that forces the user to be authenticated by a RADIUS server when connecting and authenticating to WLAN. RADIUS can add a much stronger level of authentication when connecting to WLAN and subsequently the network.		
Compliance:	The site uses RADIUS authentication for WLAN access to strengthen authentication controls. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point.[29]		
Testing:	Determine if the site is adding a RADIUS authentication process for clients attempting to connect through WLAN.		
Rating		Date		Auditor		Reviewer	
Comments:	The following is a graphical depiction[30] of a client authenticating via the RADIUS server to access the WLAN and subsequently the LAN. 		

Procedure 12- Conducting the WLAN Assessment	Assess chosen locations WLAN using tool such as NetStumbler.	*Type*: **S**ubjective / **O**bjective	O
Reference:	www.networkstumbler.com		

Risk:	Site may have poorly configured WLAN; WLAN may be lacking basic security such as WEP encryption, and may be broadcasting SSID, there may be unofficial/rogue WAPs as well.
Compliance:	Company WAPs are configured to meet a minimum standard of security; namely WEP enabled and SSID broadcasting disabled. Rogue WAPs are controlled.
Testing:	-Assess the location(s) for WAPs, both officially sanctioned and unofficial rogue WAPs emanating from within the site. -Document settings indicated in Network Stumbler (SSID, Encryption Security Enabled/Disabled) in following table template. -Review MAC addresses for inventoried WLAN devices with those of WAPs detected. Undocumented WAP's may be rogues, third party WAP's, or improperly introduced equipment. -Perimeter test outside of facilities if possible to assess if range of WAPs is extending beyond company areas.
Rating	Date | Auditor | Reviewer
Comments:	This will require some exercise and time depending on the geographic area to be covered. The assessor should note where (GPS will be helpful in this process), when, and tie to the appropriate log (NetStumbler or other WAP detector) during this process. If an AP is discovered, the assessor should be cognoscente of where it may be originating. It is possible that the WAP could be emanating from another organization or it could be a *rogue*. A rogue is an AP that originates from your site but was not set up through official procedures. Rogues could constitute a serious vulnerability; their security is unlikely to match those of corporate standards. Network Stumbler will not indicate if non-broadcasting SSID WAPs are operating thus limiting the effectiveness of tool and audit. However, the tool will detect the lower-hanging fruit that is more likely to be utilized by a threat group.

Sample Logging Template for Detected WAPs

Access Point Location[1]	Date/Time/ Auditor	MAC Address Matches Inventory?	Stumbler Log	SSID	Security				Rogue		
					WEP	LEAP	Other	None	Y	N	?

[1] Note if the AP is received outside company site perimeter during testing

2.4 The end of the Audit Fieldwork

The auditor should ensure that his/her findings are properly reviewed by management and passed on to the client in a controlled manner.

Procedure 13-Review and Presentation to Management	Writing and Presenting Audit Report; Communication with Management	*Type*: **S**ubjective / **O**bjective	S
Reference:	ABC Internal Audit Practice		
Risk:	Management may be unaware of findings or may not act on them in an appropriate fashion.		
Compliance:	Audit findings should be accurately reported to management. Management should understand and be able to respond to findings in writing. Response should detail Management's plan of action.		
Testing:	Provide audit report to management, solicit feedback and obtain responses in writing. Do so in your organization's standard timeframe.		
Rating	N/A | Date | | Auditor | | Reviewer |		
Comments:			

3. WLAN Workprogram in Practice

3.1 Background Information Related to ABC

ABC is an R&D focused multinational company. ABC operates in a competitive market and is subject to significant regulatory issues. Subsequently, information protection is a major priority to ABC.

The ABC Internal Audit group is centrally based in ABC's home country and performs ABC full-scope audits on Financial/IT areas on a rotational basis depending on the site. In 2001, the Internal Audit group will cover over 120 auditable entities. Depending on the market size, a specific site can be audited every 1-3 years, or sooner as circumstances dictate. Business units within ABC tend to be somewhat autonomous though corporate guidelines and policies are expected to be followed. Due to this autonomous culture, Internal Audit sometimes needs to "interpret" guidelines and apply them to our audits in the lack of specific policies at a local site. In some cases, business units have diverging policies due to the unique nature of their activities, regulatory environment, and locations.

3.2 Official ABC Guidelines on WLAN

ABC has not provided its user and IT communities with universal policies or standards on the use of wireless networking technologies.

Based on discussions with ABC Corporate Security, Internal Audit has determined that only several sites are said to be officially utilizing wireless networking technologies. These sites are said to be using CISCO WLAN equipment, some are enhancing security using CISCO LEAP proprietary encryption security. Specific guidelines on WLAN are currently in development by the Corporate Security group. Corporate Security currently provides "Information Protection Guidelines" which are specific control expectations on network security, application level security, and operating system security. In some cases, such as WLAN, the guidelines do not address specific technologies. In such cases, Internal Audit "interprets" the guidelines and applies them to situations in the field.

3.3 Conducting the Audit

Internal Audit- Obtaining Agreement to Perform Assessment

Internal Audit has not performed wireless audits in the past; this audit is, in a sense, a pilot project. With the blessings of Audit Management, the first audit including wireless components will be performed at a major sales and R&D location overseas during a full scope Financial / IT Audit. Specific audit steps are defined in the following sections.

3.4 Define Assessment Scope and Pre-audit Administrative

Procedure 1- Permission	Permission/Notification	*Type*: **S**ubjective / **O**bjective	S
Reference:	N/A - generally recommended practices		
Risk:	The auditor may have not obtained formal permission from Audit Management to perform the audit. The lack of approval may be detrimental to the auditor and their department.		
Compliance:	A field letter sent to the site will include notification of the WLAN audit and list of information requests. The field letter should be sent within standard timeframes of the audit process. If it is the first site-audit with WLAN within scope, the auditor will make a special effort to contact the site to ensure they understand the audit scope.		
Testing:	Verify that audit management is aware and supports the audit plans. Also confirm that client management is aware of audit group's intentions to audit WLAN.		

Results:	Request was made to Audit Management approximately one and one-half months prior to audit kick-off and provided Management approval to proceed. The Internal Audit Manager was aware of the WLAN audit plans based on numerous planning meetings we both participated in prior to leaving for the client facilities. As this is the first comprehensive site audit with a WLAN audit component, the site management was informed of our plans approximately a month before start date. Intentions to audit WLAN have been added to field letter template so future clients will be notified on all routine site audits.						
Rating	N/A	*Date*	5/X/02	*Auditor*	PJC	*Reviewer*	N/A
Comments:	This is an audit quality control procedure						
Follow up:							

Procedure 2- Determine Scope	Audit Scope and Objective	*Type*: **S**ubjective / **O**bjective	S
Reference:	Generally recommended practices, part of the concept from CISA Methodology[31]		
Risk:	Audit may choose audit samples or locations without prior knowledge pertaining to the site, facilities and capabilities. Audit resources may be used inefficiently and disrupt client site with unneeded questions and exercises.		
Compliance:	Audit has necessary information to select auditable areas, choose proper staffing and hardware/software. Audit sets expectations for itself and client.		
Testing:	Audit plan is utilized and complete no later than two weeks prior to audit. The audit plan is modifiable based on fieldwork, but significant scope/timing changes should be reported to audit management and client site management.		
Results:	While not optimal, the site topography and use of WLAN was largely unknown to the auditor until actually in the field. Due to language differences, informational documents would have required translation to decipher and a translator was not available until actually in the field at the overseas facility. Basic site information such as market size, prior audit findings, surveys were reviewed prior to leaving for the field.		

Rating	N/A	*Date*	5/7/02	*Auditor*	PJC	*Reviewer*	
Comments:	This is an audit quality control procedure and does not receive a pass / fail notation.						
Follow up:							

Procedure 3- Validate Testing Equipment	Validating Equipment/Software	*Type*: **S**ubjective / **O**bjective	O
Reference:	Software Utilities, Windows Utilities (control panel, etc.)		
Risk:	The auditor's toolset may not be operating properly, rendering the tools useless or inaccurate.		
Compliance:	Auditor has familiarized himself/herself with testing tools and software. His/her tools have been tested to verify they are working correctly.		
Testing:	1-Test tools using control panel and or NIC utilities. 2-Test against a known system. This step will be repeated before WLAN testing is conducted to ensure proper functioning.		
Results	1-Auditor relied on Lucent Technologies WaveLAN Gold WLAN NIC Utilities and of control panel hardware profiles to verify NIC operated properly- see exhibit 4. 2-Auditor tested Network Stumbler while piloting against known system in the office, a general screen shot available in Exhibit 3, actual log results Exhibit 5. Scan results were as expected.		

Rating	N/A	Date	5/X/02	Auditor	PJC	Reviewer	
Comments:	Due to our audit group's standard WIN9X image, we limited our software tool for WLAN scanning to *Network Stumbler* that can operate on our standard platform.						

Exhibit 4

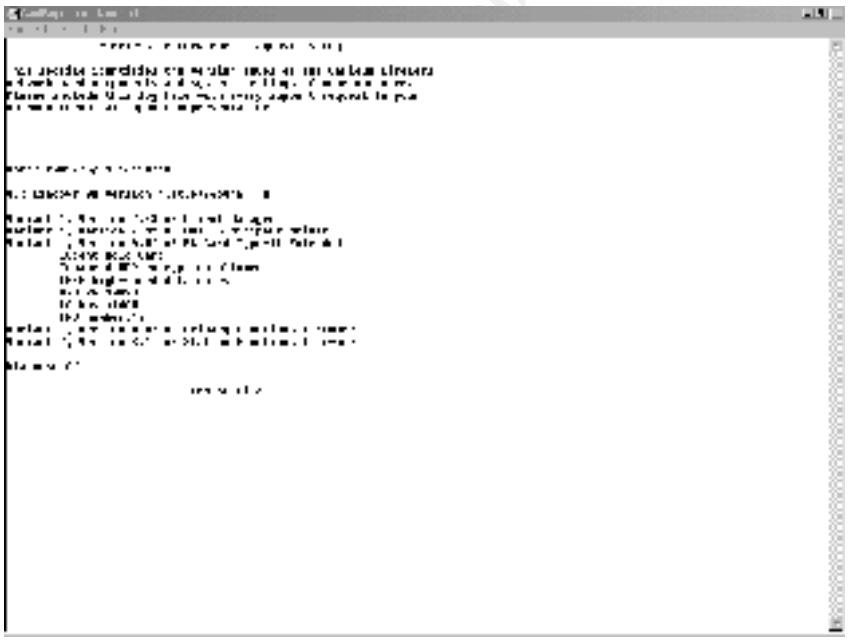
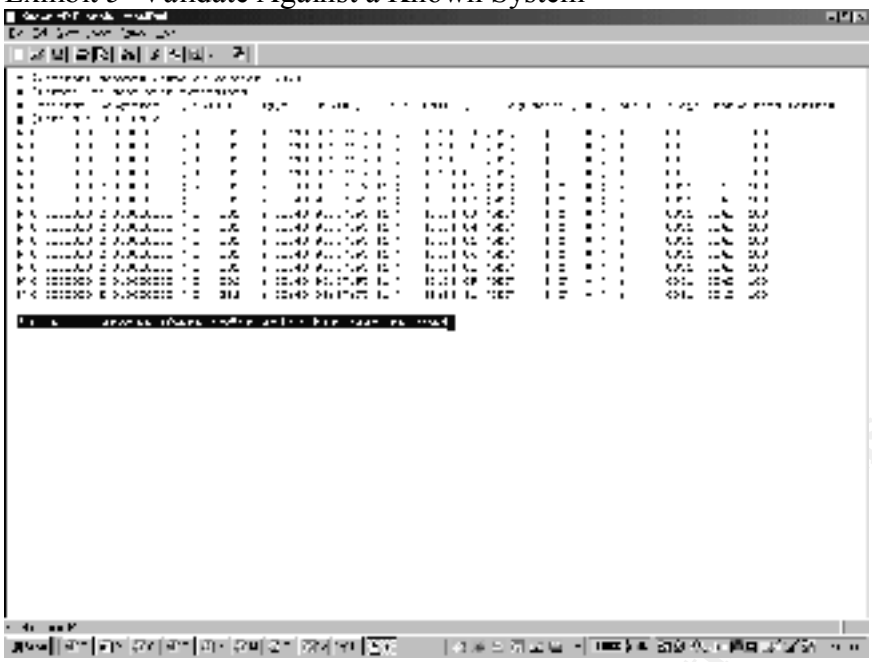


Exhibit 5- Validate Against a Known System



3.5 Obtain Relevant Background Information

The risk that this step applies to is that site Management is not aware of Corporate guidelines and may have set up WLANs that do not conform to policies. Due to the multinational and autonomous culture of ABC, there is not an overarching WLAN policy that is applicable to the specific sites being audited at this time. In spite of this, there are "Information Protection Guidelines " (IPGs) that appear to apply to WLAN in the opinion of the audit group since the IPGs cover network security. The auditor's interpretations on general information security policies should be confirmed with Audit Management if auditor feels policies also apply to WLAN. The auditor, by nature, does not actually set policies and procedures and should be reluctant to be put in this position.

If standards and policies available, the assessor has specific items to audit against. He or she may further tailor the audit towards measuring compliance at a later stage if they so desire.

Procedure 4- Strategy & Implementation	Assess WLAN Strategy and Implementation	*Type*: **S**ubjective / **O**bjective	S
Reference:			
Risk:	The site may have installed WLAN in an unstructured way leading to loss of efficiencies, inconsistent quality and security, potential service outages.		
Compliance:	For significant projects, the site should have a detailed plan, timeline, standards, and objectives for WLAN.		

Testing:	-Obtain site level (or a plan that includes the site) WLAN implementation plan, maintenance plan, etc. This plan should detail WLAN strategy, budget, security concerns and remedies. -Review an inventory of WLAN WAP's and NICs for timeliness and detail. While we are not actually confirming the accuracy of the lists, the presence of these documents does lean towards some degree of change control and monitoring. Equipment standards can also be determined from this list, assuming the equipment is standardized. -Is the local site aware of any new guidelines on WLAN from Corporate sources? Does the site have a plan of action to address new standards? What is their progress?
Results	1-Discussed the WLAN efforts at the site with the Network Infrastructure Manager and their assistant on 5/x/02. They both indicated that the site does not have a formal WLAN implementation plan. Rather, the infrastructure group has responded to business units at requests on a case-by-case basis. The requesting site incurs the costs. 2-While there is not a formal WLAN plan, some undocumented standards have been utilized, including using CISCO Aironet 350 Series WAPs, CISCO Aironet 350 Adapters (cards), a single SSID naming standard, consistent security settings, and centralized management of WLAN by IT Infrastructure. An extensive spread sheet (can not be reproduced due to sensitive information) containing all official 159 AP's by MAC address, location, name, and IP address was provided to audit. The list included activation date, and appeared to be kept up to date. 3-As there are not specific corporate standards at the time of this project, the area cannot be tested. The site's Infrastructure Manager correctly identified the same resource the audit group identifies as the most likely to advising of a formal corporate policy on WLAN. The auditor feels that the Information Protection Guidelines principals on security are covered in later steps in the audit program (specific security settings).

Rating 		Date	5/X/02	Auditor	PJC	Reviewer	

Comments:	Though a formal plan is not available, there are mitigating controls and understandings as to how WLAN should be setup. The audit corroborated these informal standards in practice. Audit will recommend developing a formal plan and document of standards. See Audit Report Section of this document.

Procedure 5- Preventative Controls	Determine Preventative Controls – WLAN Policies and Procedures Applicable to Site	*Type*: **S**ubjective / **O**bjective	S
Reference:	Determine Preventative Controls -Policies and Procedures at / or applicable to site.		
Risk:	Site may be operating WLAN outside of company policies, leading to differing standards, eroded security, and loss of efficiencies.		
Compliance:	Site should have local policies and practices to cover WLAN usage and security.		
Testing:	Obtain and review local policies and practices, governing policies and procedures if the site adopts from another source. Obtain and review user awareness documentation that covers WLAN. In spite of there being policies, these policies *may* not be explicit or timely enough to be effective and could be enhanced. This is the subjective aspect of the testing.		
Results	Based on discussions on 5/X/02 with the IT Infrastructure Manager and the IT Information Security Officer, Internal Audit determined that there are not formal policies or procedures at the site though there are informal processes and understandings on WLAN setup and access requests. These understandings were corroborated with the assistant Infrastructure Manager on the same date. Testing in step 4 appears to support this assertion.		
Rating		Date 5/x/02	Auditor PJC	Reviewer
Comments:	As mentioned in step 4, informal understandings are prevalent at this location. As such, corroborative inquiry appeared to be the reasonable way to verify this other than cataloging and comparing understandings to actions. Due to these informal standards, this control is considered to be mostly ineffective and a recommendation will be made to management to formalize this.		

Procedure 6- Detective Controls	Detective Controls	*Type*: **S**ubjective / **O**bjective	O
Reference:			
Risk:	Management may not be aware of improper WLAN activity and network resources may be compromised.		
Compliance:	Management uses a utility to monitor WLAN traffic for unusual occurrences, potential exceptions. If exceptions are found, this will lead to the finding and disabling of rogues as well as misconfigured official WAPs.		
Testing:	Understand nature of extent of monitoring or detective controls, document successful "catches". An IDS or Firewall on the segment containing WLAN is a good indication of a system based detective control and pervasive control.		

Results	Discussed with Infrastructure Manager on 5/X/02 responsible for WLAN at site. Currently management does not have any monitoring controls or detective controls to address unauthorized activity on the WLAN. As such, no further audit steps were made on this front. This control should be implemented and will be addressed in recommendations to management.						
Rating		Date	5/x/02	Auditor	PJC	Reviewer	
Comments:							

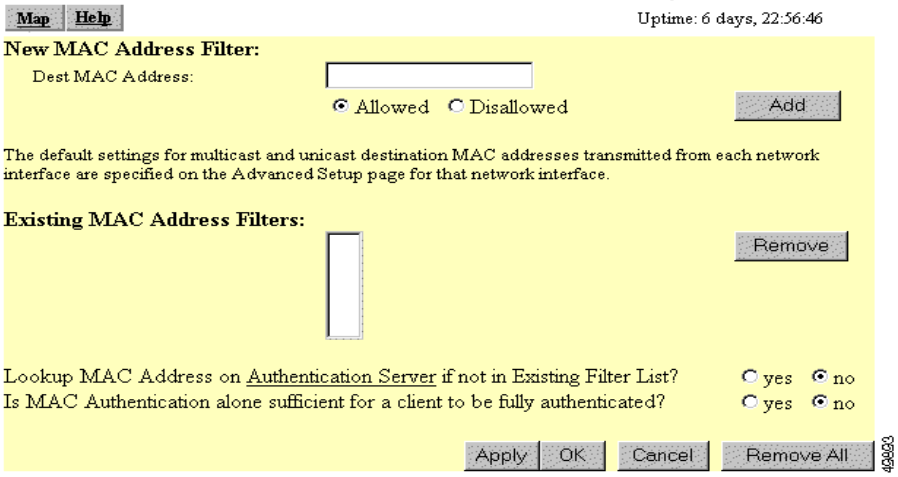
Procedure 7-Information Security Ownership	WLAN Security Owner	*Type*: **S**ubjective / **O**bjective	S
Reference:	If the organization promotes Information Security Ownership (ISO) as a guideline, this added control might be contributing towards better WLAN controls. This depends on your organization.		
Risk:	Without information security ownership, security concerns may be overlooked or passed over when dealing with new technologies, etc.		
Compliance:	The site (unless very small) has an ISO or equivalent who is responsible for Information Security issues. This individual or group should be aware of WLAN initiatives locally and that of Corporate.		
Testing:	Meet with ISO or equivalent, learn about their level of understanding on this area and discuss what any plans, policies, etc. that may be applicable to the site. Lack of understanding may result from either lack of information flow from corporate, inadequate training on ISO, and or a lack of interest.		
Results:	The are multiple ISO's at the sites being audited. The IT ISO is aware of WLAN security issues but has not been active in this area.		

Rating		Date	5/x/02	Auditor	PJC	Reviewer	
Comments:	This is a recommended practice, based on the author's work experience. An informal verbal suggestion was made to ISO and supervisor to more actively influence Infrastructure on WLAN security areas. Since the ISO process has been formalized and no directions have come from corporate, the auditor views this as a partial explanation on the reluctance of the ISO to become more involved. If the WLAN policies had been set forth from corporate and the ISO failed to act, this would result in a written recommendation to management. Some leeway should be given since the ISO program is relatively new.						

3.6 Audit Steps in the Field

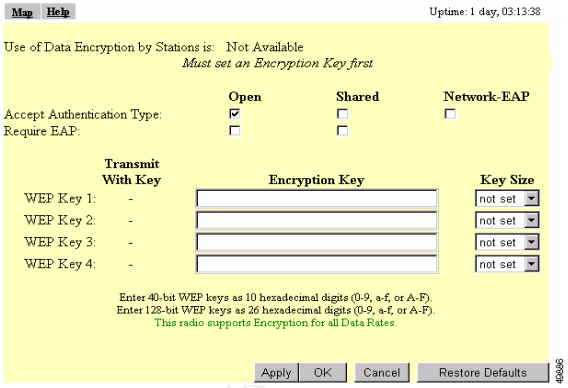
The assessor needs to determine which actual locations are to be assessed. He/she will also scope the extent of the testing- indoor, outdoors, organization campus only, etc. He/she may go as far as going to a non-company location adjacent or near a site to be assessed (with permission of course if the location is not on public property). It would be helpful to map out your routes you intend to take though you should leave some wiggle room once you are at the site in case you determine that an alteration or addition may be helpful. Also keep in mind outside groups, such as vendors who may be attached to corporate network and may have established their own WLAN.

Procedure 8- Firewall Protection	Data Gathering - Firewall Protection	*Type*: **S**ubjective / **O**bjective	O
Reference:	SANS GSNA Course Material[32]		
Risk:	The LAN may be under attack and compromised due to weaknesses in the WLAN.		
Compliance:	Management is utilizing a firewall in front of the Access Points to protect resources from WLAN originating attacks. Activity should be logged, monitored, and reviewed.		
Testing:	Discuss with management any firewall type efforts (router or software based) that may limit activity from subnets that feature WAPs. Are logs reviewed? *Remainder of Page Deliberately Left Blank*		

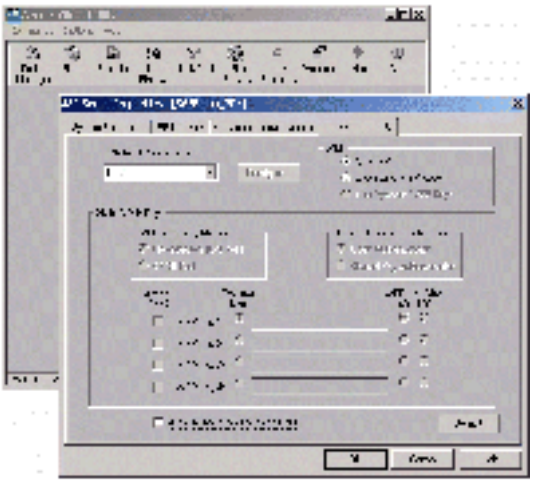
Results	Discussed the control with the Network Infrastructure Manager and their subordinate on 5/X/02. Informed that there is not currently such a configuration in place. Noted that the Manager appeared to be very interested in exploring this control further. The CISCO Aironet 350 system does not offer a firewall as part of its offering. However, a control that would appear to be helpful is filtering clients based on their MAC Addresses. The Cisco Aironet does offer this capability. The following image is a generic example of the configuration settings on the Aironet AP. The administrator can enter MAC addresses of approved devices. This boosts security but also can be burdensome to mobile users and administrators alike. 
Rating ●	● Date: 5/X/02 Auditor: PJC Reviewer:
Comments:	These controls have been recommended to management as enhancing controls. Management appeared interested in evaluating these added controls.

Procedure 9- Encryption Key	Data Gathering- Encryption Level and Key	*Type*: **S**ubjective / **O**bjective	O
Reference:	SANS GSNA Course Material[33]		
Risk:	Encryption key may be easily guessable or sequential, rendering it largely ineffective. A lower level of encryption (40 bit) makes it much easier for a password to be brute force cracked.		
Compliance:	Encryption key is not easily guessable, higher encryption level utilized (128)		
Testing:	Review the WEP key; destroy record after review.		

Results	On 5/X/02 Network Infrastructure Management informed us that WEP 128bit encryption is used as a standard. We were provided a hand written copy of the WEP Key and it appeared to be "random" based on its appearance to the auditor. The 26 character key length appeared to indicate 128bit encryption being used. We also verified the settings on an AP console. The following screen shot[34] *is a generic example* the WEP settings on an Aironet Access Point. In this case WEP has been disabled since there is no key entered. To ensure that the WEP settings are at 128 bits, there should be 26 hexadecimal characters in the key field and key size set to 128.



Desktop support inputs the WEP key in the CISCO NIC utility to configure the client to connect according to the local standards. The setup is then locked by password; users are unaware of the configuration password for the NIC utilities. The lockout was verified for two client laptops, a password protected the settings on the NIC card and I was unable to view or edit security settings.

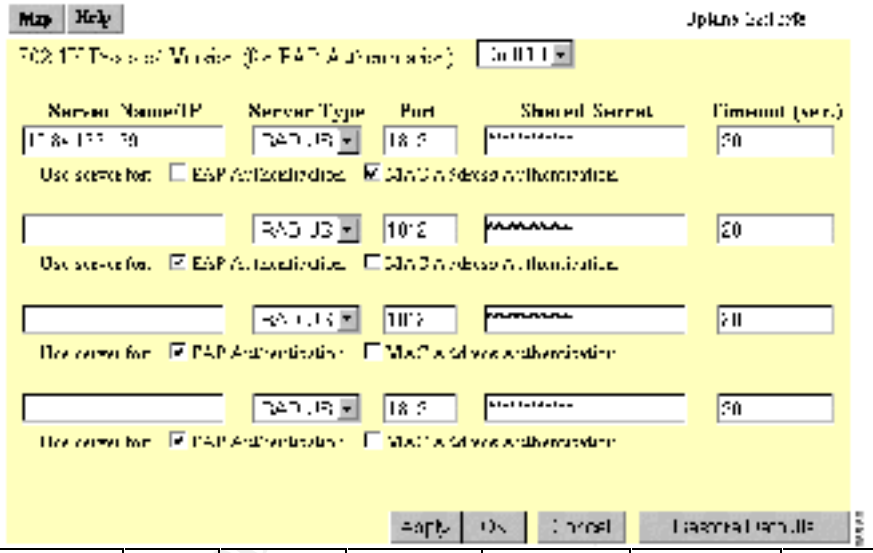


The WLAN NIC Options including key management can be found in the NICs utilities assuming that the administrator has the password to access the settings. A sample screen[35] shot of the client utilities including key management indicates that WEP is not enabled. If it were, keys would be entered and WEP setting would be a choice other than "No Wep".

Rating		Date	5/X/02	Auditor	PJC	Reviewer	

Procedure 10- Encryption System	Encryption Key	*Type*: **S**ubjective / **O**bjective	O
Reference:	SANS Security Essentials Course Material[36]		
Risk:	The integrity of the 802.11b WEP key erodes with time due to its static nature. Static keys are more vulnerable to being compromised with time and increasing user base.		
Compliance:	The site uses a different method of encryption than WEP. This security should be superior to that of WEP. WEP is considered as a minimum-security level and may be insufficient if improved encryption schemes are approved of by IT, etc. One such proprietary encryption scheme is CISCO LEAP[37] which uses asymmetric keys.		
Testing:	Determine if a different encryption from WEP is used or shall be implemented in the near future. Does current encryption scheme comply with corporate guidelines if applicable?		
Results:	Discussed with Infrastructure Manager on 5/x/02 the current encryption method for WLAN. As discussed previously, the local sites are using a WEP 128bit key. There are no plans to move beyond WEP to a more robust and dynamic encryption method. The manager responded with interest to this question and wanted to study it further.		
Rating 		Date	Auditor / Reviewer
Comments:	This is considered an enhancing control at this time since there is not any formal guideline to move beyond WEP at the time this project is being performed. It is not necessarily fair in the opinion of this auditor to indicate the control is ineffective.		

Procedure 11- Added Authentication	Stronger Authentication	*Type*: **S**ubjective / **O**bjective	O
Reference:	SANS GSNA Course Material- Penetration Testing 802.11B[38]		
Risk:	Users do not need to authenticate to the company network to access the WLAN, thereby reducing network security. This is an enhancing control that forces the user to be authenticated by a RADIUS server when connecting and authenticating to WLAN. RADIUS can add a much stronger level of authentication when connecting to WLAN and subsequently the network.		
Compliance:	The site uses RADIUS authentication for WLAN access to strengthen authentication controls. RADIUS allows a company to maintain user profiles in a central database that all remote servers can share. It provides better security, allowing a company to set up a policy that can be applied at a single administered network point.[39]		
Testing:	Determine if the site is using or adding a RADIUS authentication process for clients attempting to connect through WLAN.		

Results	Discussed the control on 5/x/02 with the Infrastructure Manager who indicated that an authentication server is not currently used in this fashion though he appeared interested in utilizing the current RADIUS server for this purpose. A way to test the tying of RADIUS to the WLAN would be to review the Access Point settings. In this case, a *generic* CISCO Aironet 350 configuration screen is included below as a resource. The auditor would be able to access this screen by accessing the *Authenticator Configuration Page* of the Aironet utilities. The example below indicates that one RADIUS server is being authenticated too by clients accessing the applicable access point. 						
Rating		Date	5/x/02	Auditor	PJC	Reviewer	
Comments:	This is considered an enhancing control						

Procedure 12- Conducting the WLAN Assessment	Assess Selected Locations use of WLAN through tool such as Network Stumbler.	*Type*: **S**ubjective / **O**bjective	S/O
Reference:	www.networkstumbler.com		
Risk:	Site may have poorly configured WLAN; WLAN may be lacking basic security such as WEP encryption, and may be broadcasting SSID, there may be unofficial/rogue WAPs as well.		
Compliance:	Company WAPs are configured to meet a minimum standard of security; namely WEP enabled and SSID broadcasting disabled. Rogue WAPs are controlled.		

Testing:	-Assess the location(s) for WAPs, both officially sanctioned and rogue WAPs emanating from within the site. (re-test equipment prior to this step) -Document settings indicated in Network Stumbler (SSID- Service Set ID, Encryption Security Enabled/Disabled) in following table template. -Review MAC addresses for inventoried WLAN devices with those of WAPs detected. -Perimeter test outside of facilities if possible to assess if range of WAPs is extending beyond company areas. *Remainder of page deliberately left blank*

Results:

Table I consists of excerpts from the Network Stumbler Scans with sensitive information removed. Three scans were performed in three distinct locations. The first two scans took place on all of my company's floors in multi-tenant office buildings. The third scan took place in a dedicated company campus and was in an isolated area.

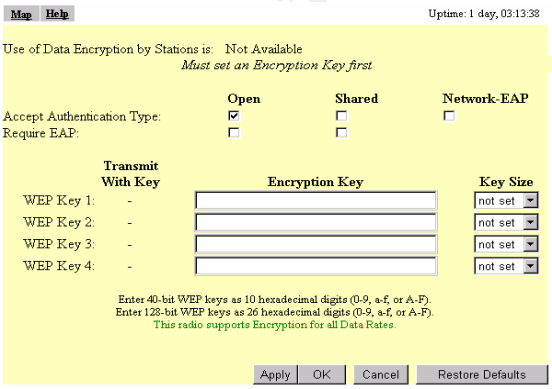
With the exception of entries 2 and 3 there were no obvious indicators of ABC WAP's emanating from my site. Any properly configured official ABC AP's would not be seen by Network Stumbler due to their lack of SSID broadcasting as was learned previously in the audit process. Since scans 1-2 occurred in multi-tenant office building in a busy downtown district, it was not possible to rule out the other 27 WAP's as rogues. Eight of the 27 remaining WAP's indicated in the log had distinct company names and were assumed to be emanating from them and were ruled out as ABC rogues.

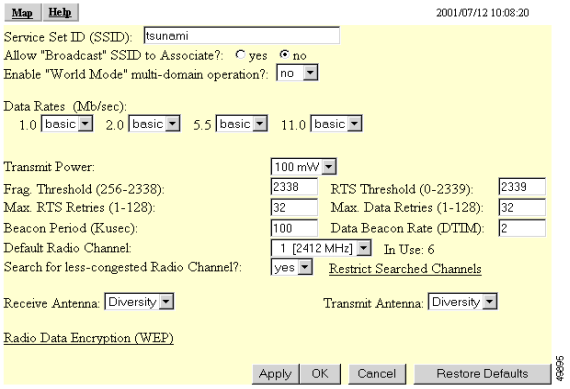
Management was provided a list of the 19 remaining unidentified AP's and MAC addresses none corresponded to those on file according to Infrastructure Management. Infrastructure Management informed us that they would investigate these AP's to determine if they were rogues. This reinforces having a monitoring control in place by the client site.

Access Points 2-3 were official ABC Access Points that were misconfigured to be broadcasting the SSID and were not using WEP. Management was immediately informed and corrected these exceptions immediately. We ran a brief scan in the same general area and did not detect either WAP. Recommendations detailed in section 3.8.

The image below is a generic example of what the security may have looked like on the console level for the two Wireless Access points (2-3) with WEP disabled. The sample configuration screen shot below indicates that WEP is off since no keys have been set. The Admin. would need to enter a valid key and set the size to 128 bit WEP. Once a key is entered, a new pull down menu called *Use of Data Encryption by Stations* would appear. The administrator would have three choices; No Encryption (default), Optional, and Full Encryption. *Full Encryption* should be enabled to ensure WEP is used.
Taken from CISCO's Aironet online help: www.cisco.com/univercd/cc/td/doc/product/wireless/air o1200/accsspts/ap120scg/bkscgch4.htm#43927

This image is a generic example of what the console may have looked like for AP's 2-3; broadcasting their SSID. The second option should be set to *no*- this would disallow devices that do not specify an SSID to associate with the access point. With *no* selected, the SSID used by the client device must match exactly the access point's SSID. This adds some degree of security but there are still issues related to SSIDs as mentioned in section 1.2.
www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350 /accsspts/ap350scg/ap350ch3.htm#13891





Rating		Date	5/X/02	Auditor	PJC	Reviewer	

Comment: Management informed us that the 2 access points were unconnected to the network at the time of the review. They explained that the APs were used only for DRP testing and had been left on inadvertently. We had no way of verifying their assertions.

TABLE I – Network Stumbler Scan Results

SCAN SITE 1 Excerpts			# $Date: 2002-05-16				
	Location	(SSID)	Type	(BSSID)	Time	WEP Y/N	Rogue Y?
1	Unable to Disclose	(default)	BBS	(00:07:40:0b:3f:07)	06:42:40	N	
2	Unable to Disclose	***My Organization***	*BBS*	*(00:X:X:X:X:X)*	*06:51:36*	*N*	N
3	Unable to Disclose	***My Organization***	*BBS*	*(00:X:X:X:X:X)*	*06:53:23*	*N*	N
4	Unable to Disclose	name removed	BBS	(00:02:2d:41:74:0f)	07:03:02	Y	
5	Unable to Disclose	(aironet)	BBS	(00:40:96:54:24:0c)	07:03:27	Y	
6	Unable to Disclose	name removed	BBS	(00:90:fe:70:b8:7a)	07:04:10	N	
7	Unable to Disclose	(HKRDS55)	BBS	(00:60:dc:10:10:af)	07:07:29	Y	
8	Unable to Disclose	(FM WaveLAN)	BBS	(00:02:2d:0a:f5:01)	07:07:50	N	
9	Unable to Disclose	(FM WaveLAN)	BBS	(00:02:2d:0a:f5:04)	07:08:00	N	
10	Unable to Disclose	(HKRDS53)	BBS	(00:60:dc:10:10:45)	07:08:13	Y	
11	Unable to Disclose	name removed	BBS	(00:60:1d:f2:3c:24)	07:08:23	N	
12	Unable to Disclose	(cisco)	BBS	(00:40:96:44:80:66)	07:08:30	Y	
13	Unable to Disclose	name removed	BBS	(00:08:21:94:c2:71)	07:13:59	Y	
14	Unable to Disclose	(000000SJ001)	BBS	(00:02:2d:38:b7:ce)	07:14:12	Y	
15	Unable to Disclose	name removed	BBS	(00:50:8b:99:54:f8)	07:14:17	Y	
16	Unable to Disclose	(HKRDS57)	BBS	(00:60:dc:10:10:3d)	07:14:22	Y	
17	Unable to Disclose	name removed	BBS	(00:90:cc:1b:e1:f1)	07:14:30	N	
18	Unable to Disclose	(7B0645GROUP)	BBS	(00:60:1d:22:ca:6b)	07:14:58	N	
19	Unable to Disclose	(WaveLAN Network	BBS	(00:02:2d:21:16:b4)	07:15:16	N	
20	Unable to Disclose	-101	BBS	(00:a0:f8:9e:a2:5c)	07:15:23	N	
21	Unable to Disclose	(SHOWROOM)	BBS	(00:02:2d:03:84:32)	07:15:39	Y	
22	Unable to Disclose	(DA8D6CGROUP)	BBS	(00:02:2d:3a:a3:37)	07:16:08	Y	
SCAN SITE II	**ABC Company**	# $Date: 2002-05-28					
23	Unable to Disclose	Name Removed	BBS	(00:90:99:81:e2:45)	01:08:06	N	
24	Unable to Disclose	Name Removed	BBS	(00:a0:b0:23:e7:f9)	01:11:15	N	
25	Unable to Disclose	(000000GROUP)	BBS	(00:02:2d:0f:51:3e)	02:04:06	Y	
26	Unable to Disclose	(000000GROUP)	BBS	(00:60:1d:f2:d9:ba)	02:09:50	Y	
27	Unable to Disclose	(000000GROUP)	BBS	(00:02:2d:00:b1:70)	02:09:54	Y	
28	Unable to Disclose	(000000GROUP)	BBS	(00:02:2d:0a:2e:da)	02:10:15	Y	
29	Unable to Disclose	(AirMac Network)	BBS	(00:60:1d:1e:c0:22)	01:35:52	N	
SCAN SITE III ABC Company			# $Creator: Network Stumbler Version 0.3.23				
n/a	No AP's Picked Up						

3.7 The end of the Audit Fieldwork

The auditor should ensure that his/her findings are properly reviewed by management and passed on to the client in a controlled manner.

Procedure 13-Review and Presentation to Management	Writing and Presenting Audit Report; Communication with Management	*Type*: **S**ubjective / **O**bjective	S
Reference:	ABC Format		
Risk:	Management may be unaware of findings or may not act on them in an appropriate fashion.		
Compliance:	Audit findings should be accurately reported to management. Management should understand and be able to respond to findings in writing. Response should detail Management's plan of action.		
Testing:	Provide audit report to management, solicit feedback and obtain responses in writing. Do so in your organization's standard timeframe. ABC timeframe is at the end of the audit.		
Results:	The audit recommendations were made on 5/X/02 and will be responded to in writing within 60 days as is standard audit practice at ABC. The client has agreed verbally to evaluate and implement our recommendations with the exception of needing further time to evaluate 3-5 in the following section 3.81. Audit will follow-up on client's status by 7/X/02.		

Rating	N/A	Date	6/1/02	Auditor	PJC	Reviewer	
Comments:							

3.8 Evaluating the Audit

This audit was ABC's first in the Wireless Networking arena. It was conducted in the context of a comprehensive Financial and Information Technology audit at several important overseas sites for ABC Company.

3.81 Auditability and Securability of WLAN

Auditing WLAN is possible depending on your goals. This audit was designed to be part assessment, and part audit; WLAN is a new technology that diverges on many fronts but converges into the LAN. The technology has some significant security shortcomings. The goal of this audit was to provide comfort that the client's site was implementing WLAN in a controlled manner and that security was in place up to a certain point (i.e. WEP). It is clear that security can be significantly increased by strengthening authentication, the encryption system, and improving pervasive controls.

Audit's findings resulted in:

- 2 misconfigured WAP's being corrected

- Assisting in establishing monitoring controls for rogue and misconfigured AP's
- Using a less obvious SSID and disabling SSID broadcasting
- Further study in increasing security of WLAN and network through RADIUS authentication and firewalls.

These measures will enhance WLAN security and reduce potential exposures to threat groups. The audit can be improved in several ways:

- Use more sophisticated technology to:
    - Detect misconfigured closed systems (non broadcasting SSIDs)
    - Sniff or probe networks exposed by open WLANs
    - Verify the origin of rogues or WLAN signals
    - Test against specific standards when applicable
    - Determine what is visible if an inappropriate user accesses a WLAN.

In closing, the auditor feels that this pilot audit was helpful in bettering WLAN controls at this ABC site and future audit sites. Auditing is an evolving process and requires us to start somewhere. More sophisticated auditing methods, tools, and practices will emerge with auditor experience and technology maturation.

4. Findings of WLAN Audit

4.1 Executive Summary

Internal Audit performed a high-level Wireless Networking (WLAN) Audit during the time period of 5/x/02-5/x+x/02 at ABC X Site. While some controls appeared to be operating effectively, we recommended enhancements in the following areas to local management:

- Developing policies and procedures on WLAN development and use
- Utilizing more robust data encryption and WLAN authentication processes
- Monitoring WLAN for unauthorized activity and weak security settings

Security was found to be generally satisfactory though significant enhancements can be added to further protect ABC. Management agreed with our recommendations and is in the process of evaluating solutions for identified ABC WLAN weaknesses.

4.2 Audit Report Detail

Internal Audit performed a high-level Wireless Networking (WLAN) Audit during the time period of 5/x/02-5/x+x/02 at ABC X Site(s) and determined that WLAN controls can be improved in the following areas:

1. Policies and Procedures (Pervasive, Preventative Controls, see test procedures 4-5)
2. WLAN Monitoring (Detective and Monitoring Controls, see test procedure 6)
3. Encryption (see test procedure 9)
4. Authentication Security (test procedure 11)
5. Network Security (test procedure 8)

6. Weak Settings On Two WLAN Access Points (test procedure 12)

Risks:

1. Lack of formalized policies can lead to inconsistent security and controls.
2. Undetected rogues and misconfigurations are likely to create security gaps in the ABC network that can be exploited by unauthorized users.
3. The standard type of encryption used (Wired Equivalent Privacy-WEP) on the WLAN weakens over time since it is a "static/symmetric" key. WEP is known to have other weaknesses that can also be exploited by unauthorized users to attack or access the ABC network.
4. Current authentication between the access point and client does not require network level authentication. The lack of this control makes it easier for intruders to gain access to ABC information resources.
5. Without a firewall protecting ABC from WLAN originating attacks, an intruder who breaches the WLAN may be relatively uninhibited in further exploiting ABC Network Resources.
6. Misconfigured access points erode information security by providing unauthorized users a lower hurdle of security to penetrate.

Recommendations:

1. Create standards and policies on WLAN security, setup, request processes, end-user security, non-ABC use, and change management (page 22-24, procedures 4-5). Coordinate with the local Information Security Officer to ensure that policies & procedures are in compliance with corporate standards.
2. Periodically review sites for "rogue" Wireless Access Points using a Wireless Sniffer tool and other monitoring tools. Also review official WLAN Access Points on a periodic basis to ensure that they are operating appropriately (page 24 and 26, procedures 6 and 8).
3. Consider upgrading encryption to a proprietary encryption scheme such as CISCO LEAP. Since CISCO hardware and software is already the standard (and offers LEAP) at the site, the cost should be incremental other than the time for reconfiguration of access points and clients (page 29, procedure 9).
4. Utilize a RADIUS level of authentication to further protect the network from unauthorized users. The current RADIUS server for Remote Access Services may be expandable for this purpose. The CISCO Aironet access points and clients already offer RADIUS level authentication within the software (page 29, procedure 11).
5. Implement a firewall type service on the area of the network housing WLAN access points to contain any breaches from going beyond the WLAN (page 26, procedure 8).
6. Access Points should be consistent to policies and security standards. The two access points that were found to be broadcasting without encryption enabled should be rectified (pages 30-33, procedure 12). We also recommend changing SSID to a name less traceable to ABC. This will require time to reconfigure Access Points and Clients. In the future, we recommend semiannual reviews of ABC WAPs to ensure appropriate security. These reviews will also identify potential "rogue" or unauthorized access points connected to ABC's network.

Discussed With:

1. Mr. Peiper Okeechobee- IT Infrastructure Manager
2. Ms. Sasha Hosenfefer - IT Infrastructure Assistant Manager
3. Mr. Italk– Local Audit Manager

---

[1] Pratap, Oak. "Deploying Wireless Technology—A Case for IT Governance" Volume 2 2002, page 53, Information Systems Control Journal, www.isaca.org
[2] Klemencic, Joe. "Basic Security Mechanisms for Wireless Networks." July 16, 2001 http://online.securityfocus.com/infocus/1199
[3] Stanley, Richard A. "Wireless LAN Risks and Vulnerabilities" Volume 2 2002. Information Systems Control Journal
[4] Armstrong, Illena . "Today's Telecommuting World." February 2002. Computer Security Magazine http://www.scmagazine.com/scmagazine/2002_02/main.html
[5] Armstrong, Illena . "Today's Telecommuting World." February 2002. Computer Security Magazine http://www.scmagazine.com/scmagazine/2002_02/main.html
[6] Armstrong, Illena . "Today's Telecommuting World." February 2002. Computer Security Magazine http://www.scmagazine.com/scmagazine/2002_02/main.html
[7] Stanley, Richard A. "Wireless LAN Risks and Vulnerabilities" Volume 2 2002, page 57, Information Systems Control Journal, www.isaca.org
[8] Stanley, Richard A. "Wireless LAN Risks and Vulnerabilities" Volume 2 2002, page 57, Information Systems Control Journal, www.isaca.org
[9] WEP Fix using RC4 Fast Packet Keying, www.rsasecurity.com/rsalabs/technotes/wep-fix.html
[10] Definition taken from Webodedia, www.webopedia.com/TERM/S/SSID.html
[11] Wireless Networking Security, SANS Institute Security Essentials Course Material, page 6-34
[12] http://www.canaudit.com/Articles_Pubs/past_articles/Nov01_perspective.htm images no longer posted
[14] Brad Johnson Quoted by Armstrong, Illena . "Today's Telecommuting World." February 2002. Computer Security Magazine http://www.scmagazine.com/scmagazine/2002_02/main.html
[15] Owen, Daniel. "Wireless Networking Security: As Part of Your Perimeter Defense Strategy" January 23, 2002. http://rr.sans.org/wireless/netsec.php
[16] Owen, Daniel. "Wireless Networking Security: As Part of Your Perimeter Defense Strategy" January 23, 2002. http://rr.sans.org/wireless/netsec.php
[17] Control concepts terminology taken from 2001 CISA Review Technical Information Manual, page 31, Information Systems Audit and Control Association, www.isaca.org
[18] Control concepts terminology taken from 2001 CISA Review Technical Information Manual, page 31, Information Systems Audit and Control Association, www.isaca.org
[19] 2001 CISA Review Technical Information Manual, page 31, Information Systems Audit and Control Association, www.isaca.org
[20] http://airsnort.shmoo.com/
[21] http://www.netstumbler.com/ Current *Network Stumbler* is Version 0.3.23
[22] http://www.sniffer.com/products/sniffer-wireless/default.asp?A=3
[23] For more information see http://www.hdcom.com/2.4ghzantennas.html
[24] Huey, Benjamin "Penetration Testing 80211.b Networks." Page 9 httphttp://rr.sans.org/wireless/test_80211b.php, 2/24/02
[25]Huey, Benjamin "Penetration Testing 80211.b Networks." Page 9 http://rr.sans.org/wireless/test_80211b.php, 2/24/02
[26] Wireless Networking Security, SANS Institute Security Essentials Course Material, page 6-34
[27] CISCO LEAP information: http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350cards/mac/incfg/m350ch4.htm
[28]Benjamin Huey, Penetration Testing 80211.b Networks, page 9, http://rr.sans.org/wireless/test_80211b.php, 2/24/02
[29] Search.com Definition http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214249,00.html
[30] Convery, Sean. SAFE: Wireless LAN Security in Depth. Whitepaper publication by CISCO. www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm, January 15, 2002

[31] 2001 CISA Review Technical Information Manual, page 31, Information Systems Audit and Control Association, www.isaca.org
[32] Huey, Benjamin "Penetration Testing 80211.b Networks." Page 9 http://rr.sans.org/wireless/test_80211b.php, 2/24/02
[33] Huey, Benjamin "Penetration Testing 80211.b Networks." Page 9 http://rr.sans.org/wireless/test_80211b.php, 2/24/02
[34] Taken from CISCO's Aironet online help: www.cisco.com/univercd/cc/td/doc/product/wireless/airo1200/accsspts/ap120scg/bkscgch4.htm#43927
[35] Convery, Sean. SAFE: Wireless LAN Security In Depth. Whitepaper publication by CISCO. www.cisco.com/warp/public/cc/so/cuso/epso/sqfr/safwl_wp.htm, January 15, 2002
[36] Wireless Networking Security, SANS Institute Security Essentials Course Material, page 6-34
[37] CISCO LEAP information: http://www.cisco.com/univercd/cc/td/doc/product/wireless/airo_350/350cards/mac/incfg/m350ch4.htm
[38]Huey, Benjamin "Penetration Testing 80211.b Networks." Page 9 http://rr.sans.org/wireless/test_80211b.php, 2/24/02
[39] Search.com Definition http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci214249,00.html

Last Updated: July 22nd, 2017

Upcoming Training

SANS Network Security 2017	**Las Vegas, NV**	**Sep 10, 2017 - Sep 17, 2017**	**Live Event**
SANS AUD507 (GSNA) @ Canberra 2017	**Canberra, Australia**	**Oct 09, 2017 - Oct 14, 2017**	**Live Event**
SANS OnDemand	**Online**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s Only**	**Anytime**	**Self Paced**