



NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

**WIRELESS LOCAL AREA NETWORK (WLAN)
VULNERABILITY ASSESSMENT AND SECURITY**

by

Adam Kessel
Shane Goodwin

September 2005

Co-Advisors:

Carl Oros
Dan Boger

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE September 2005	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE: Title (Mix case letters) Wireless Local Area Network (WLAN) Vulnerability Assessment and Security			5. FUNDING NUMBERS	
6. AUTHOR(S) Captain Shane Goodwin and Captain Adam Kessel				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE	
13. ABSTRACT (maximum 200 words) The proliferation of wireless computer equipment and Local Area Networks (LANs) create an increasingly common and growing threat to Marine Corps Network infrastructure and communication security (COMSEC). This threat requires a capable deterrent in order to mitigate risks associated with both official and un-official wireless LANs. The potential efficiencies gained by employing wireless technology within the Marine Corps and DoD is quite significant. The Marine Corps must leverage this relatively inexpensive technology to conduct operations cheaper, faster and more effectively. However, these same wireless LAN capabilities have introduced new ways in which critical information infrastructure can be viewed, altered or even denied. This thesis proposes the assessment of multiple installations within DoD in order to identify vulnerabilities and ensure secure employment of wireless technologies. These assessments will enable the development of adequate measures to secure existing wireless transmissions and protect future transmissions from observation, modification or denial of service. This thesis will assess threats posed to network infrastructure by wireless networks and evaluate WLANs that exist within the DoD to determine adequate measures to secure transmissions made by those networks. Vulnerability assessments of multiple services at different DoD installations will be conducted in order to gather a wide range of input. These assessments will provide an indication of how DoD installations are leveraging wireless capabilities to improve support to the operating forces. These vulnerability assessments will also provide insight into the current security posture within the DoD with regard to wireless communications. The practices employed by these services will be evaluated to determine the best means of standardizing wireless security procedures within the Marine Corps. In addition, a diverse assortment of wireless software and hardware tools will be tested in order to ascertain the best methods for monitoring and securing wireless networks within DoD. The evaluation of these software and hardware tools will facilitate the creation of an inexpensive and easily distributed WLAN tool kit which can be employed at installations across DoD. The final result desired is for this research is to improve the WLAN vulnerability assessment capability within the Marine Corps.				
14. SUBJECT TERMS Wireless Local Area Network (WLAN), WiFi (802.11a/b/g), WLAN Security, Vulnerability Assessment			15. NUMBER OF PAGES 177	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL	

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**WIRELESS LOCAL AREA NETWORK (WLAN) VULNERABILITY
ASSESSMENT AND SECURITY**

Adam K. Kessel
Captain, United States Marine Corps
B.S., Pennsylvania State University, 1999

Michael S. Goodwin
Captain, United States Marine Corps
B.S., Miami University, 1995

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT

from the

**NAVAL POSTGRADUATE SCHOOL
September 2005**

Authors: Adam Kessel

Shane Goodwin

Approved by: Major Carl Oros
Co-Advisor

Dr. Dan Boger
Co-Advisor

Dr. Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The proliferation of wireless computer equipment and Local Area Networks (LANs) create an increasingly common and growing threat to Marine Corps Network infrastructure and communication security (COMSEC). This threat requires a capable deterrent in order to mitigate risks associated with both official and un-official wireless LANs. The potential efficiencies gained by employing wireless technology within the Marine Corps and DoD is quite significant. The Marine Corps must leverage this relatively inexpensive technology to conduct operations cheaper, faster and more effectively. However, these same wireless LAN capabilities have introduced new ways in which critical information infrastructure can be viewed, altered or even denied. Our thesis proposes the assessment of multiple installations within DoD in order to identify vulnerabilities and ensure secure employment of wireless technologies. These assessments will enable the development of adequate measures to secure existing wireless transmissions and protect future transmissions from observation, modification or denial of service.

This thesis will assess threats posed to network infrastructure by wireless networks and evaluate WLANs that exist within the DoD to determine adequate measures to secure transmissions made by those networks. Vulnerability assessments of multiple services at different DoD installations will be conducted in order to gather a wide range of input. The assessments will provide an indication of how DoD installations are leveraging wireless capabilities to improve support to the operating forces. These vulnerability assessments will also provide insight into the current security posture within the DoD with regard to wireless communications. The practices employed by these services will be evaluated to determine the best means of standardizing wireless security procedures within the Marine Corps. In addition, a diverse assortment of wireless software and hardware tools will be tested in order to ascertain the best methods for monitoring and securing wireless networks within DoD. The evaluation of these software and hardware tools will facilitate the creation of inexpensive and easily distributed WLAN tool kits which can be employed at installations across DoD. Finally

this thesis will make recommendations on how to improve the WLAN vulnerability assessment capability within the Marine Corps.

Specifically, this research will start with the identification of current wireless network requirements and known vulnerabilities as well as threats and attacks posed to wireless networks within DoD. Current solutions available for securing wireless networks will be identified as an attempt to bridge the gap between what is currently available and what is required to ensure wireless network security. Data will be collected and analyzed from wireless vulnerability assessments throughout the DoD which will provide a statistically diverse framework to conduct the research. Selected wireless vulnerability assessments will be completed working in conjunction with the National Security Agency (NSA), Fleet Information Warfare Center (FIWC), Marine Corps Network Operations Security Command (MCNOSC) and Headquarters Marine Corps (HQMC) C4. This analysis will provide insight into assessing and securing wireless networks in garrison environments and provide answers to our research questions. Current wireless tools will be evaluated in order to provide an assessment of their usefulness and relevance within DoD. In addition, a standard set of software and hardware tools will be identified which can be purchased locally by installation level network administrator or deployed centrally from HQMC. The goal of this toolkit would be to provide the network administrators with a powerful but relatively inexpensive arsenal for detecting, assessing and securing wireless networks within their organizations. Once relevant software and hardware tools are identified, standard procedures will be created for detecting, assessing and securing wireless networks on Marine Corps installations or within Major Subordinate Commands (MSCs). The goal of the procedures will be to provide network administrators with specific instructions for successfully managing wireless networks within his or her area of responsibility. The final step of this research will be to determine recommendations to Marine Corps Network Operations Security Command (MCNOSC) and HQMC C4 regarding improving the WLAN vulnerability assessment capability within the Marine Corps. Ultimately, the research will result in a proposed solution which presents the appropriate response to mitigate the risks associated with WLAN technology.

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	BACKGROUND	1
B.	PURPOSE.....	1
C.	TARGET AUDIENCE	2
D.	DOD GUIDANCE.....	2
E.	RESEARCH QUESTIONS.....	3
F.	THE ROAD AHEAD	4
II.	WIRELESS LOCAL AREA NETWORK (WLAN) THREATS AND VULNERABILITIES	7
A.	INTRODUCTION.....	7
B.	THREATS	7
	1. Insider Threats.....	7
	2. Outsider Threats	8
C.	VULNERABILITIES	8
D.	ATTACKS	9
	1. War Driving.....	10
	a. Countermeasures to War Driving.....	10
	2. WEP Attack.....	10
	a. Countermeasures to WEP Attacks	12
	3. Rogue Access Points and Man-in-the-Middle Attacks	13
	a. Countermeasures to Rogue APs and Man-in-the-Middle Attacks	13
	4. Denial of Service Attacks (DoS).....	14
	a. Countermeasures to DoS Attacks.....	14
	5. Bluetooth Attacks.....	15
	a. Countermeasures to Bluetooth Attacks.....	15
E.	SUMMARY	16
III.	WLAN NETWORK SECURITY PRINCIPLES.....	17
A.	INTRODUCTION TO INFORMATION SECURITY	17
	1. The Need for Security in Networking	17
B.	INFORMATION ASSURANCE	17
C.	FUNDAMENTAL PRINCIPLES OF INFORMATION ASSURANCE ..	18
	1. Confidentiality.....	18
	2. Integrity	18
	3. Availability.....	19
	4. Authenticity	19
D.	DEFENSE IN DEPTH.....	20
E.	ENCRYPTION AND FILTERING	20
	1. Encryption	21
	2. Filtering.....	21

F.	WIRELESS NETWORK DEFENSE	22
1.	Encryption	22
2.	Access to the WLAN	23
a.	MAC Filtering	23
b.	Manage SSID	23
c.	Disable DHCP	24
d.	Manage Signal Strength	24
e.	Change Configuration Passwords and Default Accounts.....	24
f.	Update Firmware and Drivers	25
3.	Firewalls	25
4.	Intrusion Detection Systems (IDS)	26
G.	SUMMARY	26
IV.	MARINE CORPS WIRELESS IMPLEMENTATIONS	27
A.	INTRODUCTION.....	27
B.	SECNET-11	27
C.	STRATIS	30
1.	History and Purpose	30
2.	Requirements and Capabilities.....	31
3.	Controls and Threat Description.....	32
a.	Access	32
b.	Threats.....	32
4.	Hardware Architecture	33
5.	Deployable Configuration	33
D.	SUMMARY	34
V.	WIRELESS VULNERABILITY ASSESSMENTS	37
A.	INTRODUCTION.....	37
1.	Assessment Tools.....	37
B.	ORGANIZATION ONE.....	38
1.	Background	38
2.	Wireless Discovery	38
3.	WLAN Assessment Checklist.....	39
a.	NetStumbler - WLAN Basics	41
b.	Yellowjacket - Locating and Signal Accessibility	41
4.	Results	42
a.	AirMagnet – Advanced WLAN Assessment.....	42
b.	WLAN Exploitation and Expanding Privileges.....	44
5.	Recommendations	51
a.	Turn Encryption On.....	51
b.	Change the Default Password on Each Access Point.	51
c.	Turn the Broadcast Power Down.	51
d.	Restrict Access to the Access Points by MAC Address.	51
e.	Do Not Broadcast the SSID.....	51
f.	Separate STRATIS From the NIPRNET and Base Networks.....	51
C.	ORGANIZATION TWO	51

1.	Background	51
2.	Wireless Discovery	52
3.	WLAN Assessment Checklist.....	53
4.	Results	55
D.	ORGANIZATION THREE	61
1.	Background	61
2.	Wireless Discovery	61
3.	WLAN Assessment Checklist.....	63
4.	Results	65
a.	Denial of Service	65
VI.	EVALUATION OF SOFTWARE AND HARDWARE SOLUTIONS.....	71
A.	INTRODUCTION.....	71
1.	Functionality.....	71
2.	Utility.....	71
3.	Complexity.....	72
4.	Cost.....	72
B.	SOFTWARE/HARDWARE APPLICATIONS	72
1.	Open Source Freeware or Shareware Applications	72
a.	NetStumbler.....	72
b.	Kismet.....	74
c.	Ethereal	77
e.	Bootable CDs – (Auditor, Knoppix STD, PHLAK)	78
2.	Proprietary Commercial Software Applications	84
a.	AirMagnet.....	84
b.	AirDefense.....	86
c.	AiroPeek Nx	88
d.	Cognio ISMS.....	89
e.	YellowJacket.....	92
C.	EVALUATION CHART	93
D.	SUMMARY	94
VII.	STANDARD PROCEDURES FOR DETECTING, ASSESSING AND SECURING WLANS.....	97
A.	INTRODUCTION.....	97
B.	COORDINATING A WIRELESS VULNERABILITY ASSESSMENT	97
1.	Internal Assessment.....	97
2.	External Assessment	98
C.	CONDUCTING A WIRELESS VULNERABILITY ASSESSMENT.....	98
1.	Formal Notification of Command	99
2.	In-brief	99
3.	Assessment.....	100
a.	Wardriving.....	100
b.	Locating Wireless Local Area Networks.....	106
c.	Access Point/Wireless Card Exploitation.....	107
d)	Bluetooth and Infrared (IR)	111

4.	Out-brief	111
5.	Formal Report to Document Findings	111
6.	Conduct Follow-up Assessment on Deficiencies	112
D.	RECOMMENDED TOOLKIT.....	113
1.	WLAN Vulnerability Assessment Toolkit (WiVAT).....	113
a.	Hardware/Software	113
VIII.	EXEMPLAR WLAN IMPLEMENTATION GUIDE AND HARDWARE/SOFTWARE USAGE:	117
A.	HIGH LEVEL HARDENED WLAN.....	117
1.	Introduction to Wireless Implementation Research.....	117
2.	Defense in Depth	117
a.	First Level.....	118
b.	Second Level of Defense	119
c.	Third Level of Defense.....	122
d.	Fourth Level of Defense	123
e.	Fifth Level of Defense.....	126
3.	Voice over IP (VOIP).....	130
4.	Power Over Ethernet.....	131
5.	Remote Access	132
6.	Wired vs. Wireless	133
B.	SUMMARY	134
IX.	CONCLUSION AND RECOMMENDATIONS.....	135
A.	THE ROAD LESS TRAVELED	135
B.	CONCLUSION	136
C.	RECOMMENDATIONS.....	137
1.	Information Assurance (IA) Toolkits.....	137
2.	WLAN Training.....	139
3.	Special Education Program (SEP) Payback Utilization.....	141
4.	Increased Investment in WLAN Security and Assessment.....	142
	LIST OF REFERENCES	145
	INITIAL DISTRIBUTION LIST	151

LIST OF FIGURES

Figure 1.	Wireless Directives (From Ref.).....	3
Figure 2.	WEP attack using Aircrack 64 bit key (From Ref.).....	11
Figure 3.	WEP attack using Aircrack 128 bit key (From Ref.).....	12
Figure 4.	SECNET-11 PC Cards to Create Ad Hoc Network (From Ref).....	28
Figure 5.	SECNET-11 PC Cards to Create Infrastructure Network (From Ref.)	29
Figure 6.	Use of SECNET-11 PC Wireless Bridges (From Ref.)	29
Figure 7.	STRATIS Architectural Description (From Ref.)	33
Figure 8.	Deployable STRATIS Configuration (From Ref.)	34
Figure 9.	NetStumbler Discovery at Organization One (From Ref.)	41
Figure 10.	AirMagnet Alarm Notification at Organization One (From Ref.)	44
Figure 11.	IPAQ Screenshot showing connection to SSID 22 (From Ref.).....	45
Figure 12.	Symbol AP Configuration Webpage (From Ref.)	46
Figure 13.	Symbol Website Containing AP Configuration Guidelines (From Ref.)	47
Figure 14.	Symbol Reference Manual Reflecting Default AP Configuration (From Ref.)	48
Figure 15.	Symbol AP Configuration Webpage (From Ref.)	49
Figure 16.	Symbol AP Configuration Webpage (From Ref.)	49
Figure 17.	Telnet AP Interface (From Ref.).....	50
Figure 18.	Symbol AP configuration Telnet Login enabled (From Ref.)	56
Figure 19.	Symbol AP Access Control List (From Ref.)	57
Figure 20.	Kismet screen capture linksys WEP disabled (From Ref.).....	58
Figure 21.	Kismet screen capture ESSID network details (From Ref.)	59
Figure 22.	Airopeek screen capture linksys WEP disabled (From Ref.)	60
Figure 23.	Airopeek screen capture Vocera devices on network (From Ref.).....	62
Figure 24.	Airopeek screen capture AP MAC addresses visible (From Ref.)	66
Figure 25.	WEP attack using Aircrack 64 bit key (From Ref.).....	67
Figure 26.	Airopeek screen capture CMC Emulator DoS (From Ref.).....	68
Figure 27.	NetStumbler (From Ref.).....	73
Figure 28.	Kismet main screenshot (From Ref.).....	76
Figure 29.	Ethereal (From Ref.)	77
Figure 30.	Auditor (From Ref.)	81
Figure 31.	Knoppix (From Ref.)	82
Figure 32.	PHLAK (From Ref.)	83
Figure 33.	AirMagnet (From Ref.).....	85
Figure 34.	AirDefense (From Ref.)	87
Figure 35.	AiroPeek (From Ref.)	88
Figure 36.	Cognio (From Ref.).....	90
Figure 37.	Cognio (From Ref.).....	91
Figure 38.	Yellowjacket (From Ref.)	92
Figure 39.	Kismet main menu screenshot (From Ref.)	103
Figure 40.	gpsmap sample screenshot (From Ref.).....	106

Figure 41.	NIST WLAN Security Checklist (From Ref.)	110
Figure 42.	WiVAT hardware components (From Ref.)	115
Figure 43.	WiVAT packed (From Ref.)	115
Figure 44.	Network Segmentation (From Ref.)	119
Figure 45.	Air Fortress generic configuration (From Ref.)	120
Figure 46.	Air Fortress generic configuration (From Ref.)	121
Figure 47.	Bluesocket Active Connection screen (From Ref.)	122
Figure 48.	Bluesocket's suggested topology (From Ref.)	123
Figure 49.	Air Defense example topology (From Ref.)	125
Figure 50.	Air Defense Rogue AP and Termination techniques (From Ref.)	125
Figure 51.	AMP's AP monitoring (From Ref.)	127
Figure 52.	AMP's visualRF (From Ref.)	128
Figure 53.	Organization 3 overall topology (From Ref.)	129
Figure 54.	Organization 3 device usage (From Ref.)	129
Figure 55.	Vocera sample topology (From Ref.)	130
Figure 56.	Vocera communicator (From Ref.)	131
Figure 57.	iPass remote access topology (From Ref.)	132
Figure 58.	Senforce Security Client (From Ref.)	133
Figure 59.	VX30 Streaming Video Session (From Ref.)	134
Figure 60.	IA Toolkit Software Suite (From Ref.)	138
Figure 61.	IA Chief Training Requirements (From Ref.)	140

LIST OF TABLES

Table 1.	Evaluation of Software / Hardware Applications	94
----------	--	----

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS

ACL- Access Control List

AES- Advanced Encryption Standard

AP- Access Point

COTS- Commercial Off-the-Shelf

DAA- Designated Approving Authority

DHCP- Dynamic Host Configuration Protocol

DISA- Defense Information Systems Agency

DoD- Department of Defense

DoDD- Department of Defense Directive

EMI- Electromagnetic Interference

FIPS- Federal Information Processing Standards

GHz- Gigahertz

GIG- Global Information Grid

HTTP- Hyper Text Transfer Protocol

HTTPS- Hyper Text Transfer Protocol, Secure

IA- Information Assurance

IASO- Information Assurance Security Officer

IDS- Intrusion Detection System

IEEE- Institute of Electronic and Electrical Engineers

IP- Internet Protocol

IPSec- Internet Protocol Security

IR- Infrared

ISSO- Information Systems Security Officer

IT- Information Technology

LAN- Local Area Network

MAC- Media Access Control or Message Authentication Code

MCCDC- Marine Corps Combat Development Command

MCEN- Marine Corps Enterprise Network

MOS- Military Occupational Specialty

MSC- Major Subordinate Commands

MTT- Mobile Training Team

NIC- Network Interface Card

NIPRNet- Non-Classified Internet Protocol Router Network

NIST- National Institute of Standards and Technology

NOC- Network Operations Center

NSA- National Security Agency

OSI- Open Systems Interconnection

PC- Personal Computer

PDA- Personal Digital Assistant

POE- Power Over Ethernet

RADIUS- Remote Access Dial-in User Service

RF- Radio Frequency

RSN- Robust Secure Network

SEP- Special Education Program

SNMP- Simple Network Management Protocol

SSH- Secure Shell

SSL- Secure Sockets Layer

SSID- Service Set Identifier

STIG- Security Technical Implementation Guide

TCP- Transmission Control Protocol

VLAN- Virtual Local Area Network

VOIP- Voice Over Internet Protocol

VPN- Virtual Private Network

VTC- Video Teleconference

WEP- Wired Equivalent Protocol

WIDS- Wireless Intrusion Detection System

WIPS- Wireless Intrusion Protection System

WiVAT- Wireless Vulnerability Assessment Toolkit

WLAN- Wireless Local Area Network

WPA- WiFi Protected Access

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

We would like to thank our families; Florence, Adam, Jackson, Buster, and Brutus for their faithful support during the past two years. We would also like to thank Brian Steckler for planting the seeds of this research during our first year of graduate work. Finally, we would like to thank Major Carl Oros for his insight and guidance throughout the process of developing and completing our thesis.

THIS PAGE INTENTIONALLY LEFT BLANK

DISCLAIMER

The software and hardware evaluation conducted within this research represents a limited assessment based on specific criteria established by the authors. The opinions expressed within this document solely represent the opinions of the authors and should not be considered as an official position of the U.S. Government, Department of Defense or the Naval Postgraduate School.

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The convenience created by wireless devices coupled with their relatively low cost was largely responsible for the exponential growth of WLANs over the past decade. However, the conveniences of wireless technology came at a significant cost. WLANs have introduced vulnerabilities which must be countered in order to continue to reap the fruits of wireless labor. Policy designers realized the shortfalls inherent in the 802.11 standard and have subsequently released more security conscious standards. In addition, DoD has established guidance which levies even more stringent requirements upon wireless network implementations within DoD. Despite the presence of rigorous standards, which must be met in order to implement wireless networks, WLANs can be found on installations across the Marine Corps. The small strides made by additional security conscious standards and more stringent DoD and Marine Corps wireless policies have not slowed the growth of WLANs or eliminated the threats introduced by wireless technologies to Marine Corps information infrastructure.

This thesis will assess threats posed to network infrastructure by wireless networks and evaluate WLANs that exist within the DoD to determine adequate measures to monitor transmissions made by those networks. Vulnerability assessments will be conducted of multiple services at different DoD installations to provide a relevant sample for the study. The assessments will provide an indication of how DoD installations are leveraging wireless capabilities to improve support to the operating forces. These vulnerability assessments will also provide insight into the current security posture within the DoD with regard to wireless communications. The practices employed by these services will be evaluated to determine the best means of standardizing wireless vulnerability procedures within the Marine Corps. In addition, a diverse assortment of wireless software and hardware tools will be tested in order to ascertain the best methods for conducting vulnerability assessments within DoD. The evaluation of these software and hardware tools will facilitate the creation of a WLAN vulnerability assessment tool kits which can be employed at installations across DoD. Finally, this thesis will make

recommendations as to the best ways to improve the WLAN vulnerability assessment capability within the Marine Corps.

The plethora of WLANs in existence today was confirmed during the conduct of numerous WLAN vulnerability assessments aboard DoD and Marine Corps installations during the past year. A critical investment of personnel and resources is required to create such a capability. Leaders, by and large, are not aware of the presence of WLANs or the threats introduced by them. In addition, personnel responsible for managing installation network resources are aware of wireless technology, but do not have the specific training or tools required to assess WLANs within their organizations. The widespread presence of WLANs aboard DoD installations requires the development of a mature WLAN vulnerability assessment capability within the Marine Corps.

The combination of each of these factors creates substantial risks to information infrastructure aboard Marine Corps installations. The lack of awareness and training requires a dynamic and proactive training plan which leverages the WLAN expertise of external agencies. In addition, specific WLAN tools are needed to properly outfit organization IA personnel with the requisite tools to locate and assess WLANs. However, the most effective method to mitigate the risks associated with cheap, plentiful, unsecured wireless devices is to conduct WLAN vulnerability assessments. Effective training programs and capable tools combined with a proficient WLAN vulnerability assessment team will serve as an invaluable resource in mitigating the risks associated with wireless technologies.

I. INTRODUCTION

A. BACKGROUND

The proliferation of wireless computer equipment and Local Area Networks (LANs) create an increasingly common and growing threat to Marine Corps Network infrastructure and communication security (COMSEC). This threat requires a capable deterrent in order to mitigate risks associated with both official and un-official wireless LANs. The potential efficiencies gained by employing wireless technology within the Marine Corps and DoD is quite significant. The Marine Corps must leverage this relatively inexpensive technology to conduct operations cheaper, faster and more effectively. However, these same wireless LAN capabilities have introduced new ways in which critical information infrastructure can be viewed, altered or even denied. Our thesis proposes the assessment of multiple installations within DoD in order to identify vulnerabilities and ensure secure employment of wireless technologies. These assessments will enable the development of adequate measures to secure existing wireless transmissions and protect future transmissions from observation, modification or denial of service.

B. PURPOSE

The primary goal of our research was to enhance or develop the WLAN vulnerability assessment capability within the Marine Corps. There are obviously many ways in which one can attempt to approach this broad topic. Many students have labored in the complex arena of wireless security in the past. We have seen a great deal of valuable and insightful research completed in various aspects of wireless security. In preparation for our thesis, we studied a great deal of this research and came to the conclusion that the majority of existing work provided technical data on advanced wireless subjects and policies. Consequently, we wanted our research to provide a practical, hands-on approach to the subject. Our research will provide individuals tasked with managing wireless networks with background, context and fundamental principles of wireless security. This vital information will lay the foundation for the practical application of procedures, software and hardware tools and lessons learned from other

wireless network implementations. The final result desired is that individuals tasked with wireless network security are equipped with the often over-looked fundamental principles, real world applications, and the requisite software and hardware tools to accomplish the task.

C. TARGET AUDIENCE

Our target audience would range from installation G-6's to unit level network administrators. Our research seeks to expose this audience to the relatively new and challenging arena of wireless network security. While many of these individuals are familiar with network security as it pertains to wired infrastructure, we learned that the vast majority were unfamiliar with our proposed subject matter.

D. DOD GUIDANCE

Although the purpose of our thesis research was not intended to present the details of DoD wireless policy, it is obviously germane to any discussion of wireless assessment and security. We have chosen to weave the principles of these policies into our discussion throughout various chapters without delving into the minute details of specific protocols or standards. We have purposely avoided an extensive discussion of specific policies for several reasons. First, policies evolve over time and our desire was to speak to overarching principles which govern wireless assessment and security vice describing particular policies, protocols and standards which are more subject to change over time. Second, as previously alluded to, we came to the determination that there was an abundance of technical discussion regarding the definition and application of specific protocols and policies already in existence. Finally, our desired target audience was network administrators and higher level leaders who are fairly new to the arena of wireless security. We believe that these individuals require a more practical approach and exposure to wireless security and assessment, which is not overwhelmed by technical verbiage. While the evaluation of the specific characteristics of DoD policy is outside the scope of our thesis, the policies shown in Figure 1 guided our discussion throughout our research. In addition to the references listed in Figure 1, we used the following Navy and Marine Corps specific guidance: Marine Corps Information Assurance Operational

Standard USMC IA OPSTD 014 Wireless Local Area Networks (WLANs) and Technical Guidance for Implementation of DoN WLANs to frame our review of wireless security and assessment.

Policy	Description
DISA Wireless STIG	The DISA STIG is published as a tool to assist in the improvement of the security of DoD information systems. The guidance provided in the STIG is authoritative according to DoD Directive 8500.
DoD Directive (DoDD) 8100.2 (Draft)	Describes the appropriate use of use of commercial wireless devices, services, and technologies in the DoD Global Information Grid (GIG)
DoD Directive (DoDD) 8500.1	Prescribes the use of information assurance in a defense-in-depth approach
DoD Instruction (DoDI) 8500.2	Implements policy; assigns responsibilities and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks under DoDD 8500.1.
DoD Instruction (DoDI) 5200.40	DoD Information Technology Security Certification and Accreditation Process (DITSCAP), http://iase.disa.mil/ditscap/ditsdocuments.html , is required for any new IT system. It is used to implement policy, assign responsibilities, and prescribe procedures for Certification and Accreditation (C&A) of information technology (IT), including automated information systems, networks, and sites in DoD. The System Security Authorization Agreement (SSAA) is key to the DITSCAP. The SSAA is used to guide and document the results of the C&A and the implementation of IT security requirements. It resolves several issues including the critical schedule for the C&A, the budget, security requirements, functionality of the system, and performance issues.

Figure 1. Wireless Directives (From Ref. 1)

E. RESEARCH QUESTIONS

The following questions serve as the impetus for our research and will be answered throughout the course of our thesis:

- 1.) What threats and vulnerabilities are introduced to the Marine Corps critical information infrastructure by emerging wireless technologies?
- 2.) What fundamental network security principles should be applied to safeguard wireless communications?
- 3.) How is the Marine Corps currently leveraging wireless technologies to support operating forces and supporting establishments?

¹Department of Defense, Defense Information Systems Agency, (2004), Wireless Security Support Program, *Wireless LAN Security Framework*, (sec. 3, p. 1).

4.) How are DoD and Marine Corps activities performing with regard to secure wireless implementations and assessment capabilities?

5.) What economical software and hardware solutions are available to assess and secure WLANs?

6.) What standards or procedures must be enacted in order to ensure Marine Corps wireless networks adhere to Department of Defense and Department of the Navy Wireless Policies?

7.) What recommended changes or additions to existing wireless policy will improve the current security posture within the Marine Corps?

8.) What type of implementation and use of encryption would ensure the necessary protection of wireless networks and are there any DoD approved and secure networks to model after?

F. THE ROAD AHEAD

Our thesis will seek to introduce individuals to wireless security by progressively exposing the need for security through the identification of real world threats and vulnerabilities posed to wireless networks. Once the threats and vulnerabilities to wireless infrastructure are discussed, we will review network security fundamentals and wireless security principles which will help mitigate those threats. Our thesis will then look at 802.11 initiatives and implementations within the Marine Corps in order to expose individuals to the Marine Corps wireless “state of affairs. Once we review examples of wireless implementations within the Marine Corps, we will discuss the results of actual wireless network vulnerability assessments that we conducted. These assessments will show the need for standard procedures for assessing and securing wireless networks. Given standard procedures, we will discuss potential software and hardware solutions that are available to wireless network administrators. Our thesis will also provide recommended software and hardware solutions based on our evaluation during the course of our research. We will then discuss a model or exemplar wireless network implementation within the Department of Defense, which will show current technology adapted to DoD regulations and policies. Our research will conclude by

making recommendations to higher headquarters based on the overall results of our thesis research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WIRELESS LOCAL AREA NETWORK (WLAN) THREATS AND VULNERABILITIES

A. INTRODUCTION

The best way to begin securing a Wireless Local Area Network (WLAN) is learning who and what your potential threats are as well as your operating vulnerabilities. Also, you must know what the value of the data is that you want to protect. You must decide if high value data can be protected on a wireless network. Threats range from people, support infrastructure, to natural disasters. The vulnerabilities that exist within WLANs arise from many sources but the 802.11 protocol itself has serious weaknesses that have been partially addressed in recent iterations of the 802.11 protocol such as 802.11i. Another example of a vulnerability comes from the technical misconfiguration of devices on the network. These threats and vulnerabilities will be discussed and analyzed further in the following sections.

B. THREATS

It is just as important to know what kind of individuals or groups would be interested in attacking your network as it is being aware of their motivations. For example, a government WLAN may be threatened by activists from interest groups, other countries' intelligence and surveillance community or terrorists. In this instance, the government would need high-level security because of the greater skill level achieved by other countries and the obvious sensitive information that they would be after. In contrast, a corporate WLAN may be threatened by disgruntled former employees or competitors. These employees could pose a minimal threat depending on what kind of access they were given and how quickly it was taken away. On the other hand, competitors could hire extremely skilled IT professionals to carry out attacks on a WLAN in order to obtain proprietary information or to gain a competitive edge.

1. Insider Threats

Insider threats comprise the single largest threat to any organization. In a WLAN with lower level security procedures this threat could initiate itself by providing

unauthorized users with the Service Set Identification (SSID) which would be needed to access the network. For a more secure WLAN, the insider threat proliferates by opening up opportunities for theft of laptops that leave the building. In many cases the insider threat comes from accidentally or maliciously deleting files where most security mechanisms cannot prevent these types of problems. Another common act that is represented by the insider threat comes from the abuse of authority. Accessing network shares that an employee does not have rights to or reading other employees emails are both serious insider threats that are very difficult to prevent. Simpler insider threats include the use of unauthorized software, using company resources for illegal acts or personal profit, theft or destruction of computer equipment, unauthorized hardware or peripherals, and disclosure of sensitive data. A good example of an insider threat is an authorized user that installs unauthorized software such as GoToMyPC which is software that is designed to bypasses organization's firewalls and gives remote users, backdoor access to the network.

2. Outsider Threats

As mentioned previously, outsider threats come from various sources that range from serious to very minimal security risks. Outsider threats can include amateur or professional hackers, terrorists, competitors, activists, former employees, contractors, unsponsored or organized criminals, and media representatives.

At least seven foreign countries are training their intelligence officers in how to hack into U.S. computers². Government networks, proprietary commercial information, and scientific research are all vulnerable.

C. VULNERABILITIES

While a Threat is commonly understood to be anything that is a source of danger, an identified vulnerability is something that may expose your network to the identified threats. Vulnerabilities are regularly discovered and announced by vendors and authors of affected devices, software, or protocols. There are also multiple agencies that are

²Dennis Hughes, (1997, February 3), Outsider Threats, *Fortune*, p.27.

devoted to discovering vulnerabilities and disseminating information about them. One such organization is dedicated to government cyber security called The United States Computer Emergency Readiness Team (US-CERT) which is a partnership between the Department of Homeland Security and the public and private sectors. Established in 2003 to protect the nation's Internet infrastructure, US-CERT coordinates defense against and responses to cyber attacks across the nation. The following excerpt from the US-CERT is an example of a known vulnerability and is very difficult to defend against.

IEEE 802.11 wireless network protocols use a Clear Channel Assessment (CCA) algorithm to determine whether or not the radio frequency (RF) channel is clear so that a device on the network can transmit data. The CCA algorithm used in conjunction with Direct Sequence Spread Spectrum (DSSS) transmission is vulnerable to an attack in which a specially crafted RF signal will cause the algorithm to conclude that the channel is busy, so that no device in range of the signal will transmit data. This type of signal is sometimes called "jabber." The attacker must be actively transmitting a signal and within range to affect wireless devices³.

D. ATTACKS

There are many, very well documented attacks on WLANs which can circumvent established security procedures with relative ease. Defense Information Systems Agency defines a high level view of common attacks on wireless networks in the following categories: Traffic Analysis, Passive Eavesdropping, Plaintext attack, Unauthorized Access, Man in the Middle, ARP attacks, Replay attacks, Session Hijacking, Redirection, and Denial of Service⁴. Many of the most devastating attacks are hard to accomplish without extensive knowledge in both network and host penetration techniques as well as radio frequency theory and application. The following section represents an assessment of significant attacks used to compromise wireless networks.

³The United States Computer Emergency Readiness Team (US-CERT), Vulnerability Note VU#106678, <http://www.kb.cert.org/vuls/id/106678>, August 8, 2005.

⁴Department of Defense, Defense Information Systems Agency, (2004), Wireless Security Support Program, *Wireless LAN Security Framework*, (sec. 2, p. 1).

1. War Driving

War driving is the simplest and most frequently used attack on WLANs because of the simplicity and the small amount of knowledge needed. In order to perform this attack, you would need a laptop or PDA and a wireless network card or to increase your range you could attach an antenna. There are open source software tools as well that will display the SSID, signal strength, channel, and whether or not Wired Equivalent Privacy (WEP) is being used of any 802.11 WLAN. The major risk involved with this attack is the fact that any novice user could accomplish it without prior training of any kind. This becomes such a large risk because the impact ranges from simple information leakage or bandwidth reduction to completely compromising an entire network.

a. Countermeasures to War Driving

The quickest and easiest solution to combat war driving is to turn off the broadcast SSID to prevent novice hackers from seeing what SSID is being used. The next step would be to set up an Access Control List (ACL) with only authorized Media Access Control (MAC) addresses allowed to associate to the network which is known as MAC address filtering. What this results in is a gradual escalation of security that prevents your average wireless computer user from accessing your network. The natural next step is to implement WEP which is meant to protect data as it traverses the wireless medium using the RC4 cryptographic cipher. Although WEP has been soundly defeated from different angles, it is yet another attempt to slow down an attacker that may or may not have the knowledge required to crack WEP. So the question remains, is WEP good enough?

2. WEP Attack

WEP has been proven to be extremely weak due to the repeated use of Initialization Vectors (IV) which are combined with a secret key to form a 128 bit WEP key at its strongest implementation. Using this weakness, a relatively simple program can extract a WEP key which allows an attacker onto the network. Figure 2 displays a screenshot from the authors in which a WEP crack was done on a Department of Defense (DoD) wireless network with a 64 bit key. Figure 3 displays a WEP crack that was done

on a Department of Defense (DoD) wireless network with a 128 bit key. In this instance of the attack, it took approximately 2 hours but with only a few users connected to the access point, there was a small amount of data useable in order to crack the WEP. Conversely, if an AP has 20 to 30 users connected to it accessing higher volumes of data, the attack could be done in roughly half the time or approximately one hour. This attack has become more refined recently and there is even an open source Graphical User Interface (GUI) called AirSnort by The Shmoo Group which does most of the work for you. Of course most of this must be done on a Unix or Linux operating system but some of these tools, including AirSnort, have been ported to Windows and are very difficult to install. This prevents your average Windows user from obtaining these tools and using them.

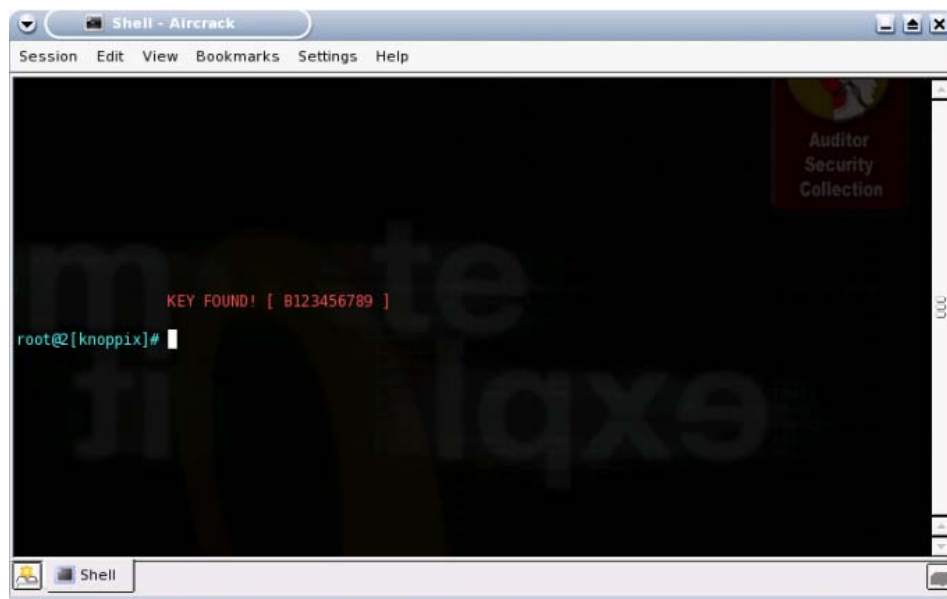


Figure 2. WEP attack using Aircrack 64 bit key (From Ref. 5)

⁵Adam K. Kessel, Captain USMC, Naval Postgraduate School, Aircrack Screen Shot, August 2, 2005.

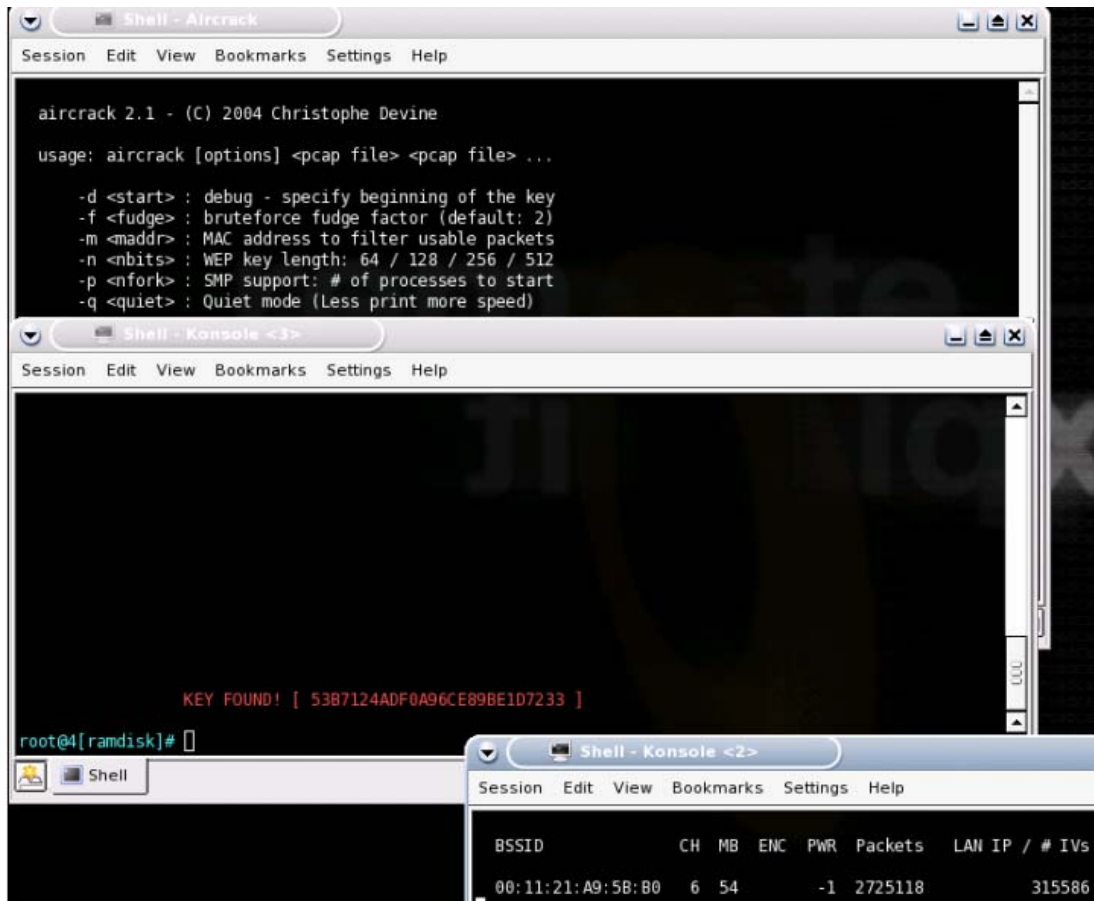


Figure 3. WEP attack using Aircrack 128 bit key (From Ref. 6)

a. Countermeasures to WEP Attacks

The best solution is to employ IEEE 802.1x/EAP port-based authentication and encryption mechanisms such as WiFi Protected Access (WPA2) or Advanced Encryption Standard (AES). In addition, Virtual Private Networks (VPN) are extremely effective in preventing unauthorized access if implemented correctly. The 802.11i standard will attempt to eliminate all security weaknesses associated with WEP and provide an alternative to VPN usage.

⁶Adam K. Kessel, Captain USMC, Naval Postgraduate School, Aircrack Screen Shot, August 2, 2005.

3. Rogue Access Points and Man-in-the-Middle Attacks

Rogue access points are the most often occurring security threat generally stemming from the insider of an organization. This is often done to allow mobile internet access to a particular workspace. While creating a comfortable environment for this particular user, what they generally do not realize is that they are subverting all security procedures by providing easy access to an otherwise secure network. The other possibility is an outsider that is able to gain access into an organization and set up an AP which can provide a back door into the wired network. This is particularly devastating because without any wireless intrusion detection devices, an outsider could have access to the network for an extended amount of time while going undetected from the outside.

The most commonly understood attack is one that involves clients associating with an AP that is different from the one they thought they were connected to. A common scenario is the wireless internet café where a laptop user trusts that he or she is connecting to the café's wireless internet service. With a laptop or even a PDA, an attacker can use one network card to knock the user off the AP with a simple Denial of Service (DoS) attack and one to act as the legitimate AP using a program that duplicates an AP running in Master mode. In this attack, an unsuspecting user could be connecting to an attacker's computer while transmitting sensitive information such as login credentials, WEP information, or worse, sensitive financial account data.

a. Countermeasures to Rogue APs and Man-in-the-Middle Attacks

An organization must continue to employ a combination of existing wireless security mechanisms in order to prevent more advanced attacks. Wireless Intrusion Detection Systems help to alert system administrators when unusual, suspect, or unauthorized traffic patterns exist. New features of the IDS allow automatic termination of an unauthorized AP or client on the network which allows administrators to focus on locating and eliminating the intruder rather than attempting to contain the attacker's access. In addition, most IDSs keep logs of all activity on the network which can be useful for reviewing and preventing future attacks. Some attacks are virtually unstoppable at this point in time because there is no way to guard the airwaves. This type of attack, known as Denial of Service (DoS), will be examined further in the next section.

4. Denial of Service Attacks (DoS)

The most dangerous attacks against mission critical wireless networks come from Denial of Service attacks. As mentioned previously, due to the nature of the radio frequency (RF) medium and the design of the 802.11 protocols, wireless networks cannot be protected against Layer 1 and certain Layer 2 DoS attacks⁷. There are a surprising number of different ways to implement a DoS attack which makes it even more difficult to defend against. The most basic DoS attack is a physical layer attack which is also known as RF jamming. There are two kinds of physical layer DoS attacks. The first is known as RF jamming and is implemented by generating a high power radio frequency signal that overpowers any other RF signals on the wireless medium preventing other signals from access. A DoS attacker must be actively transmitting a signal and within range to affect wireless devices. In this case, the only hardware needed is some type of custom-built transmitter that floods selected channels with high power RF signal in order to fill that specific area of the spectrum. This prevents any other logical use of the wireless medium because it is basically used up. The other physical layer attack involves the crafting of legitimate packets that attack the 802.11 physical carrier sense algorithm.

Another attack involves spoofing the Disassociation and Deauthentication frames which are used in the 802.11 protocol when setting up and tearing down a connection. This type of attack is probably the most well-known and used DoS attack on WLANs⁸. This attack floods the wireless medium with frames that knock clients off the network. In addition, a spoofed and modified authentication frame will cause a client to become disassociated and generally causes erratic behavior. Most of the DoS attacks are implemented by either modifying or flooding the wireless medium with legitimate frames used in the 802.11 protocol.

a. Countermeasures to DoS Attacks

One defense against layer 3 DoS attacks is in the 802.11i implementation which is protected with Temporal Key Integrity Protocol (TKIP). Of course a DoS attack

⁷A.A. Vladimirov, K.V. Gavrilenko, A.A. Mikhailovsky, (2004), *WI-FOO: The Secrets of Wireless Hacking*, (chap. 8, pp. 192-197), Addison-Wesley.

⁸Ibid., para. 2.

used against this type of network corrupts the TKIP Michael message integrity checksum which causes the receiver to shut the connection down for a minute while it generates a new session key. This is not very easy to do and is not very well documented either.

5. Bluetooth Attacks

Bluetooth is a wireless specification that uses short-range radio and was designed to be used within approximately 30 feet. Bluetooth is an industry specification for short-range RF-based connectivity for portable personal devices. The IEEE Project 802.15.1 has derived a Wireless Personal Area Network standard based on the Bluetooth v1.1 Foundation Specifications⁹. One major security issue is the fact that the Bluetooth standard allows a single device to communicate simultaneously with multiple other devices. Many Bluetooth radios are embedded in devices and users often do not realize whether they are on or even that they have a Bluetooth device to begin with. Bluetooth attacks can permit network sniffing, device detection, data and services theft.

Two well known attacks on Bluetooth devices are called Bluesnarfing and Bluejacking. Bluesnarfing attackers are exploiting a problem with some implementations of the object exchange (OBEX) protocol, which is commonly used to exchange information between wireless devices. An attacker can synchronize with the victim's device (this is known as *pairing*) and gain access to any information or service available to the legitimate user. Bluejacking is the practice of sending messages between mobile users using a Bluetooth wireless connection. People using Bluetooth-enabled mobile phones and PDAs can send messages, including pictures, to any other user within a 10-meter or so range¹⁰.

a. Countermeasures to Bluetooth Attacks

Bluetooth should always be disabled unless it is being used and when it is being used, most versions allow you to turn discovery of your device off. In addition,

⁹IEEE, *IEEE 802.15 WPAN Task Group 1*, <http://www.ieee802.org/15/pub/TG1.html>, Retrieved August 19, 2005.

¹⁰searchMobileComputing.com, *Definitions*, http://searchmobilecomputing.techtarget.com/sDefinition/0,290660,sid40_gci961342,00.html, Retrieved August 8, 2005.

your firmware should be the most current according to the manufacturer. The best solution is to use high level authentication and ensure Bluetooth communication is only over encrypted links to prevent sniffing and theft.

E. SUMMARY

Although there are many useful mechanisms available to secure wireless networks, there is no out of the box solution which is why many wireless experts agree that within the wireless arena, it is still considered “The Wild West.” The identified threats are always increasing, vulnerabilities are discovered every day, and the attacks are becoming simpler and more automated. The key to combat this uphill battle is staying one step ahead of your adversaries and staying up to date on current vulnerabilities and attacks.

III. WLAN NETWORK SECURITY PRINCIPLES

A. INTRODUCTION TO INFORMATION SECURITY

1. The Need for Security in Networking

Given the threats and vulnerabilities discussed in the previous chapter, it is important to understand the basic principles of network security that help us mitigate those threats. Security is a general concept that most rational individuals would agree is a good idea. The problem is that security usually comes at a price and that price can be measured squarely in terms of convenience. For example, if you want your home to be a safe place for those who live there, you must incorporate the necessary security measures. Those security measures might include rudimentary physical deterrents like fences and doors or more complex security measures like alarm systems and close circuit television technologies. Those security measures will likely improve the security posture of your home. However, those same security measures will levy inconveniences upon your family who now must unlock doors and disable alarms when moving throughout your home.

The world of computer networking is similar, in that, the amount and complexity of security measures that you employ have a direct impact on the convenience of network users. So the more secure of a network environment that you desire, the more convenience is reduced for those that operate within that environment. While most people desire security they insist upon convenience. Therein lies the fundamental conflict between security and convenience which forms the foundation for WLAN security. Convenience is after all one of the primary reasons we use and rely so heavily upon wireless technologies today.

B. INFORMATION ASSURANCE

Information Assurance can be defined as measures used to protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction

capabilities. Information Assurance is the security discipline that encompasses Communication Security (COMSEC), Information Security (INFOSEC), and the control of compromising emanations (TEMPEST) ¹¹.

C. FUNDAMENTAL PRINCIPLES OF INFORMATION ASSURANCE

There are three generally agreed upon principles that apply to all discussions related to the secure transmission of information. These principles are Confidentiality, Integrity, and Availability and are frequently referred to using the acronym of CIA. Some proponents of network security have added the additional tenet of authenticity, thereby extending the acronym to CIAA. It can be argued that the concerns of this additional principle are derived from integrity, but each will be covered in brief below.

1. Confidentiality

Confidentiality is a property with which information is not made available or disclosed to unauthorized individuals, entities, or processes¹². Confidentiality basically means keeping sensitive information in confidence or limited to certain individuals or organizations. In network defense, it is critical to prevent unauthorized users from observing information that they either do not need or should not see. In a wired network, confidentiality is often compromised by tapping into a network cable or other network resources. The task of confidentiality is even more challenging in a wireless environment because access to the medium is not physically restricted. In addition, it is often difficult to control the range of the transmitted wireless signals.

2. Integrity

The concept of integrity means that information is accurate and protected from unauthorized changes¹³. Integrity translates into ensuring that information cannot be maliciously or accidentally altered without its owner's or user's knowledge. In network

¹¹Department of Defense (DOD) Directive 8100.2, (2004), *Use of Wireless Devices, Services, and Technologies in the DOD Global Information Grid (GIG)*.

¹²National Institute of Standards and Technology (NIST), (2002), *Wireless Network Security; 802.11 Bluetooth and Handheld Devices*, (Special Publication 800-48).

¹³United States Marine Corps (USMC) Information Assurance Operational Standard, (2005), *014 Wireless Local Area Networks V 1.0*, (USMC IA OPSTD 014).

defense it is imperative to prevent data traveling across a network to be corrupted or modified. This task is made more difficult due to inherent weaknesses in the 802.11 standard which does not include strong message integrity features¹⁴. These vulnerabilities are more apparent in a wireless network when adequate data encryption is not present.

3. Availability

The concept of availability means that information resources are readily available when they are required¹⁵. Ensuring information is accessible in a reasonable amount of time is no small challenge to network administrators. Both malicious and non-malicious users can reduce or deny the availability of network resources. Availability, like the other information assurance concepts, is absolutely essential to wireless networks. Once the transmission medium is limited or denied, the underlying and fundamental premises of wireless networks are usurped as communications become inefficient and ineffective. Availability can be jeopardized by innocent individuals monopolizing the medium or by unauthorized users orchestrating any number of denial of service attacks.

4. Authenticity

The concept of authenticity means to verify the identity of the user, device, or other entity in a computer system, often as a prerequisite to allowing access to resources in a system, and 2) to verify the integrity of data that has been stored, transmitted, or otherwise exposed to possible unauthorized modification¹⁶. Another way to think about authenticity is that it is ensuring the stated originator of the information is in fact the true originator. Authenticity is tied closely to the concept of integrity because data integrity guarantees that information is accurate. Since part of the verified data is the actual data source, it can be argued that authenticity is implied with integrity.

¹⁴National Institute of Standards and Technology (NIST), (2002), *Wireless Network Security; 802.11 Bluetooth and Handheld Devices*, (Special Publication 800-48).

¹⁵United States Marine Corps (USMC) Information Assurance Operational Standard, (2005), *014 Wireless Local Area Networks V 1.0*, (USMC IA OPSTD 014).

¹⁶National Institute of Standards and Technology (NIST), (2002), *Wireless Network Security; 802.11 Bluetooth and Handheld Devices*, (Special Publication 800-48).

D. DEFENSE IN DEPTH

DoD Directive 8500.1 directs the use of a Defense in Depth approach as a means of protecting network infrastructure through a series of defense mechanisms which provide a multi-layered approach to network security. Defense in Depth assumes that even the best technology will have inherent flaws or limitations which could be exploited given enough time, interest or resources from prospective hackers. Having multiple layers of defense ensure gaps in one security technology are adequately covered by the strengths in another technology. For example, using an Intrusion Detection System (IDS) is one way to monitor activity on a network. However, wired and wireless IDSs come in many different forms which include both signature and behavior based tools. A good defensive posture would include behavior and signature based applications so that both new and old attacks can be recognized and prevented. In addition, Defense in Depth means using other defensive mechanisms like firewalls, encryption schemes, and strong authentication protocols coupled with those different types of IDS's. Since there are a multitude of methods and levels of attackers, no single strategy or mechanism can completely protect a network. Each method and every type of attacker presents unique challenges to the secure network. This multi-layered approach to network defense will not guarantee the safety of your network, but it will harden your network and provide enough deterrence to prevent most attackers and significantly slow down more advanced adversaries. While the concept of slowing down potential hackers may not provide much comfort to network administrators, a properly implemented defense in depth philosophy may provide just enough time to recognize, foil and protect critical information infrastructure from an attack.

E. ENCRYPTION AND FILTERING

There are generally two mechanisms which can be used to secure local area networks: encryption and filtration. Most security professionals are strong advocates for one methodology or the other. Good security professionals will practice the concepts of defense in depth and incorporate both mechanisms into the security plan. Each approach is designed for a particular scenario as described below:

1. Encryption

Encryption can be defined as the process for obscuring information in order to make it unreadable without “special knowledge”. The concept of cryptography or using codes to conceal and protect important information has been practiced by individuals for hundreds of years. However, its use was not widespread until government agencies began implementing it during the 1970’s. Encryption is the primary means for securing traffic on a network. Valid traffic needs encryption to protect the confidentiality, integrity and authenticity of each packet. Encryption uses algorithms or ciphers to transform information known as plain text into an encrypted form known as cipher text. The ciphers or algorithms commonly use a metric known as a key to encrypt and decrypt data that flows through an encrypted network¹⁷.

2. Filtering

The concept of filtering is used by intrusion detection systems, firewalls and device access control lists to identify packets that could be harmful to your network. These “bad bits” never reach critical communication infrastructure because they are appropriately identified and turned away from your network through the use of packet filtering. Packet filtering breaks down data packets into individual bits of data for the purposes of determining what to do with the payload portion of the packet. Packet filtering seeks to recognize protocols, port numbers, purpose of traffic, source of traffic, destination of traffic, not to mention specific data that is contained within the traffic. It involves the process of applying security policies to all traffic that attempts to enter or leave the network. When “bad bits” fail authentication or match a specific deny rule or fail to match a specific permit rule they are dropped from the network¹⁸. In general, there are two different types of packet filtering; stateless and stateful. Stateless filtering is less expensive and least complex of the two. It provides high volume coarse granularity filtering with no maintenance of state information. For this reason it is also referred to as static filtering because packets are dealt with individually with no regard for relationship

¹⁷WikiPedia, *The Free Encyclopedia*, <http://en.wikipedia.org/wiki/Encryption>, Retrieved July 27, 2004.

¹⁸J.D. Fulp, (2004), Center for Information Systems Security Studies and Research, *Course Notes for CS3690 Network Security*, Naval Postgraduate School.

or correlation to previous or future packets. Stateless or static packet filtering only evaluates information found in layer 3 or layer 4 headers. In contrast, stateful filtering maintains information about each packet in a table and references that table in order to make decisions on how to handle future traffic. Because of this more detailed analysis of each packet, stateful filtering impacts the efficiency of traffic flow across your network. However, the value of stateful packet filtering should not only be measured in terms of how long it takes traffic to flow across your network. The tradeoffs between convenience and security demand that latency concerns are balanced with security concerns. Ultimately, packet filtering will be measured by how well it protects your network from the myriad threats and attacks mentioned in Chapter 2.

F. WIRELESS NETWORK DEFENSE

The mobility, flexibility and costs associated with WLANs are making wireless network implementations more and more popular. However, WLANs have some unique differences and challenges from the wired network that must be overcome in order to secure network traffic. Local Area Networks are bound physically by wired cables and can be secured by managing access to the physical medium. Wireless networks are not bound by wires or even by walls. When network transmissions travel through the air they are susceptible to being viewed, altered or even denied by any individual with access to the radio frequency spectrum. The radio frequency spectrum is a shared medium which can be accessed by anyone with basic tools, many of which are open source and easily obtained.

1. Encryption

One of the first security principles that must be addressed in a WLAN is the issue of encryption. With traffic flowing freely through the air, network administrators must choose an encryption scheme to protect critical information from being viewed. One of the first and most common encryption schemes available is Wired Equivalent Privacy (WEP). WEP was designed to provide wireless networks with the same level of protection that was available to wired networks. WEP is a protocol that uses a series of secret user keys and system generated values to provide 64 or 128 bit encryption for

wireless networks. While WEP is the most common data encryption scheme used to protect WLANs today, it proved to be very susceptible to password cracking and replay attacks. These and other weaknesses in the WEP protocol have led to updated encryption schemes like WiFi Protected Access (WPA). WPA was created to be backwards compatible with WEP features to enable it to be use with both newer and older versions of hardware. WPA leverages a substantially larger initialization vector (IV) to accompany its 128 bit keys. In addition, WPA employs options for the use of either Temporal Key Integrity Protocol (TKIP) or Advanced Encryption Scheme (AES) which dramatically increases the number of keys in use in addition to a strong Message Authentication Code (MAC) to prevent replay attacks¹⁹.

2. Access to the WLAN

There are a few relatively simple steps that can be implemented to limit access to a wireless network. These steps are listed below:

a. MAC Filtering

All network devices have Media Access Control (MAC) addresses that uniquely identify them on a network. Configuring your router or access point to only allow traffic from specific MAC addresses to travel on the WLAN is easy way to enforce access control. This will allow only these specific users to associate and connect to the wireless network. While these addresses can be spoofed, the application of MAC filtering is a good starting point for keeping unauthorized users off the WLAN.

b. Manage SSID

Wireless devices must use Service Set Identifiers (SSIDs) in order to uniquely identify and differentiate themselves within a wireless architecture. The SSID is initially set to a default value by the manufacturer of a wireless router or access point. These default values are common knowledge among network administrators as well as

¹⁹Planet3 Wireless Inc., (2005), *Certified Wireless Network Administrator (CWNA) Study Guide*, New York; McGraw-Hill Osborne.

potential hackers. The default SSID should be changed from the default value to another generic term that does not provide more information about the network. In addition, wireless routers or APs automatically broadcast the SSID to the rest of the world. However, these devices have the option that enables individuals to turn off the “Broadcast SSID” option.

c. Disable DHCP

Dynamic Host Configuration Protocol (DHCP) assigns IP addresses to all devices that connect to the network. Once users have IP addresses they are able to gain other information about the network like IP ranges and DNS servers. By disabling DHCP, network administrators are forced to assign static IP addresses to all users which can be tedious in large networks but it is another line of defense against network intruders.

d. Manage Signal Strength

Managing signal availability in a WLAN is another fundamental step that network administrators should take to secure wireless networks. Signal strength should be monitored to limit the availability of the signal to only necessary workspaces. Using maximum signal strength in a small office environment may enable access to your WLAN from unsecure parking lots and streets which could be nearby. In addition, APs should be turned off when not in use to further limit the availability of your WLAN’s signal from unauthorized users. Administrators routinely limit access to wired network resources to within working hours, which is why wireless infrastructure should be regulated in similar fashion.

e. Change Configuration Passwords and Default Accounts

Wireless network devices, such as routers and access points have administrator accounts which are established to enable the WLAN administrator to configure the device. These accounts also have default passwords which can be obtained easily on the Internet. These administrator accounts should be renamed and the default

passwords should be changed to prevent potential hackers from accessing and re-configuring devices on the WLAN.

f. Update Firmware and Drivers

Manufacturers of Wireless Network Interface Cards (NICs) and access points routinely publish updates to firmware and drivers. The updates often contain improvements to the functionality of the devices but can also correct vulnerabilities that have been identified in their devices. These vulnerabilities represent security holes that can be exploited by attackers if the appropriate patches are not applied.

3. Firewalls

Encrypting data and managing access to the wireless medium are not enough to keep the WLAN secure from all the emerging threats discussed in the first chapter. Firewalls or gateways are yet another way to limit “bad guys” or “bad data” from entering your network. Firewalls are software and hardware solutions that filter the data that enters and exits the network. There are many different categories of firewalls, some of the most common types are packet-filtering gateways, circuit-level gateways and application-level gateways. Each of these different types of firewalls are designed to examine data at different layers in the OSI model. For example, packet filtering firewalls generally review traffic at the network or transport levels. This level of examination allows the firewall to filter traffic based on critical information found within the TCP and IP packet headers. TCP and IP packet headers will indicate source and destination addresses, source and destination port numbers, along with the protocol type²⁰. Regardless of the type or types of firewall(s) that are implemented to protect your network, they all serve the purpose of controlling access to or from a protected network. Depending on the security requirements and policies for a particular network, several types of firewalls can be employed. For example, it is not uncommon for a network infrastructure to employ packet filtering firewalls, proxy servers serving as circuit level gateways, and application level firewalls to limit access to the network. The use of

²⁰John Mairs, (2002), *VPNs: A Beginner's Guide*, New York; McGraw-Hill Osborne.

multiple categories of firewalls adds yet another level of defense in depth and serves to significantly harden your network infrastructure.

4. Intrusion Detection Systems (IDS)

The use of wireless IDSs and other network monitors are yet another way to improve the security of your WLAN. These software tools help to enforce organizational wireless policies and ultimately protect sensitive data on your network. A wireless IDS will provide warnings through the use of alarms which are triggered when your wireless security policies and/or rules are broken. These alerts allow for real time monitoring and response to unusual activity on the WLAN. In addition to signaling unusual, suspect, or unauthorized traffic patterns, most IDSs keep logs of all activity on the network which can be useful for reviewing and preventing future attacks, and troubleshooting connectivity problems not to mention measuring the performance of the wireless network.

G. SUMMARY

Leveraging the benefits of wireless technology means incurring significant risks to critical information infrastructure. The purpose of this chapter was to introduce network security principles and fundamental WLAN defense mechanisms. These basic principles and tools will provide the foundation for mitigating the risks outlined in the first chapter. Individuals using a network to communicate must be assured of the data's confidentiality, integrity, availability, and authenticity. This information assurance is achieved through a security policy which is based upon a rigorous philosophy of defense in depth. In addition, the network defense plan will include the use of encryption to protect legitimate data along with a variety of traffic filtering technologies to prevent suspicious or illegitimate data within critical networks. These principles are the critical building blocks for the wireless network solutions outlined in subsequent chapters of this document.

IV. MARINE CORPS WIRELESS IMPLEMENTATIONS

A. INTRODUCTION

The Marine Corps is currently using and/or exploring the use of WLAN technologies in several different applications. The majority of these wireless applications leverage technologies other than 802.11b. In the tactical communication arena there are numerous initiatives leveraging other wireless protocols aimed at improving command and control on the battlefield. For example, Marine Corps Systems Command and Marine Corps Tactical Systems Support Activity (MCTSSA) are collaborating on the use of 802.16 networks as a data distribution system in Iraq. The Marine Corps is also exploring prototype over-the-horizon communications systems and a mobile command post system. There are also initiatives which couple the use of 802.11b and SECNET-11 encryption technology to provide secure unclassified and classified wireless networks in support of Marine Expeditionary Force (MEF) Command Operational Center (COC) missions. One of the initial wireless implementations in the Marine Corps was introduced to improve logistical support for the operating forces. This adaptation of a Warehouse Management System (WMS) has proven to dramatically improve the efficiency and reliability within the supply chain, in addition to significant decreases in the required administration by of supply warehouse personnel. Regardless of the protocol, each of these wireless initiatives are designed to help the Marine Corps leverage technology to become more mobile and more connected.

B. SECNET-11

The Marine Corps is currently exploring Harris Corporation's SECNET-11 Personal Computer (PC) Card technology to provide secure wireless data, video, and Voice over IP (VoIP) capabilities. SECNET-11 is the only NSA certified 802.11b application due to its ability to provide Type 1 cryptography to secure data and network header information for all network layers. In other words, the entire packet is encrypted which prevents potential adversaries from gaining information from intercepted traffic analysis. The use of SECNET -11 PC Cards to provide secure communication up to the

Secret level significantly reduces the set-up time, cost and bulk of externally wired encryption equipment.

SECNET-11 cards can be used to connect wireless users together using the same SSID, channel and traffic encryption key. This configuration allows individual laptops to communicate with each other without an accompanying network infrastructure. Figure 4 below shows the use of SECNET-11 cards in Ad Hoc Mode creating a typical Ad Hoc Network.

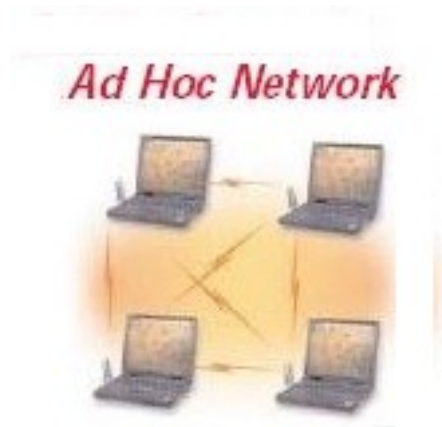


Figure 4. SECNET-11 PC Cards to Create Ad Hoc Network (From Ref²¹)

When SECNET-11 Wireless Bridges are added to the Ad Hoc configuration you are able to create an Infrastructure Network. The SECNET-11 bridges can be configured in access point or bridge mode. The access point configuration uses the bridge much like a hub and links all stations together. The bridge mode supports point to point communications between individual wireless users. An example of this infrastructure configuration is displayed below in Figure 5.

²¹Harris Secure Communications, *Secure Wireless Local Area Network*, http://download.harris.com/app/public_download.asp?fid=843, Retrieved August 6, 2005.

Infrastructure Network

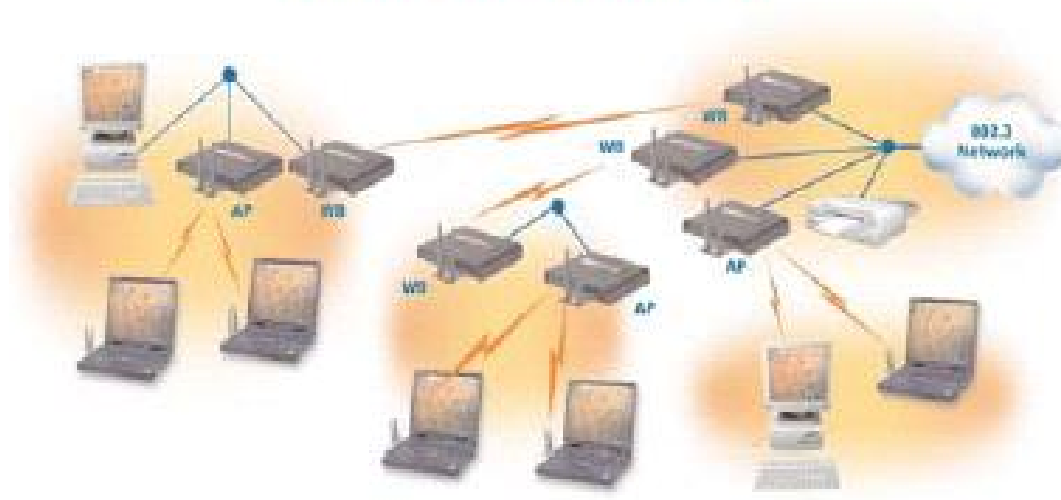
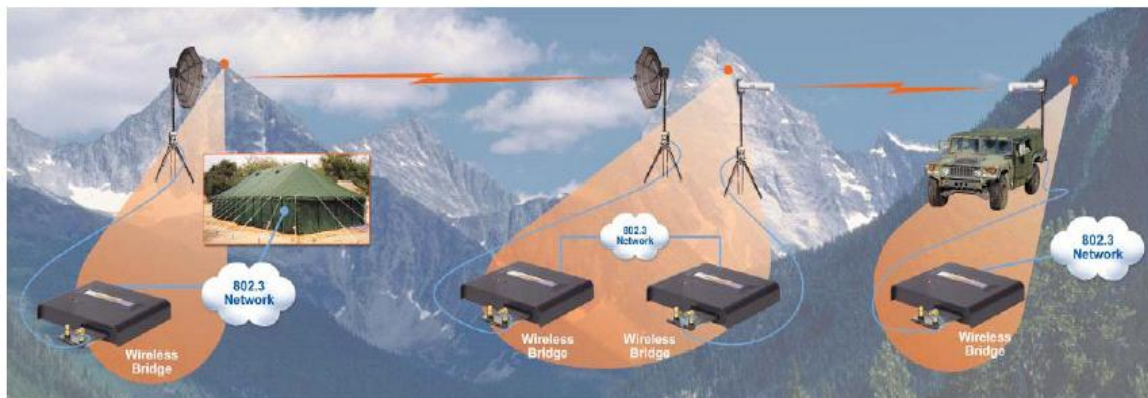


Figure 5. SECNET-11 PC Cards to Create Infrastructure Network (From Ref. ²²)

As seen in Figure 6, SecNet-11 Wireless Bridges can be used to transmit secure data up to ranges of 10 miles with the use of external antennas and/or amplifiers. This capability significantly increases the usefulness and application in tactical environments when data can be secured over extended ranges as seen in the below representation.



SecNet 11 Wireless Bridges can securely transmit and receive multimedia information (data, voice, and video) over an extended range.

Figure 6. Use of SECNET-11 PC Wireless Bridges (From Ref. ²³)

²²Harris Secure Communications, *Secure Wireless Local Area Network*, http://download.harris.com/app/public_download.asp?fid=843, Retrieved August 6, 2005.

²³Ibid.

The Marine Corps has several current and future initiatives tied to the use of SECNET-11 technology. SECNET-11 has been used by U.S. Conventional and Special Forces in Afghanistan and Iraq. The Marine Corps recently used a large scale implementation during tsunami relief efforts in Thailand in early 2005 to enhance the secure communications with the Command and Control Headquarters. Regardless of configuration, SECNET-11 provides Type 1 encryption to secure transmission of data at rates up to 11 Mbps using the 802.11b protocol.

C. STRATIS

STRATIS is an acronym for STorage, Retrieval, Automated Tracking, Integrated System (STRATIS). It integrates radio frequency (RF) equipment for “real time” communication with a supply database while on the warehouse floor. STRATIS is application software known as a WMS which performs real time operations, directs and manages labor, maximizes equipment utilization and tracks and controls inventory. This system will operate in conjunction with a host system such as Supported Activity Supply System (SASSY) or Asset Tracking for Logistics and Supply Systems (ATLASS) Version II+. The host system provides data such as using unit demands to the WMS and the WMS provides data such as inventory balances and the status of using unit demands back to the host. The WMS also controls and tracks the actions occurring on the warehouse floor.

STRATIS operator workstations are either fixed computer workstations on a carousel lift station, in the receiving section, on a supervisor’s desk or a radio frequency communication (RF) hand-held terminal.

1. History and Purpose

STRATIS is a computer based transaction oriented process control system, which provides constant tracking and control of material at all stages in the physical distribution process²⁴. STRATIS is used to perform receiving, request and issue processing, warehouse inventory, shelf-life management, material tracking, re-warehousing,

²⁴SG Automation, (2000), *STRATIS Functional Description*.

reconciliation, end of day processing, and a whole host of management control functions. The STRATIS project is sponsored by Marine Corps Systems Command for use by Marine Corps Activities. STRATIS was originally implemented at Camp Lejeune, North Carolina in January of 1998 as a “prototype” warehouse control system. The system was upgraded and re-hosted from a Tandem mid-range platform to a PC based platform. STRATIS was implemented at MCB Camp Pendleton, CA in March 2001, at 3rd Material Readiness Battalion (MRB) Camp Kinser, Okinawa, Japan in February 2003, and at MCBH, Hawaii in March 2003²⁵. Based on its success, the re-hosted STRATIS was implemented at other Marine Corps Activities.

2. Requirements and Capabilities

STRATIS was designed to provide the following major measurable objectives²⁶:

- Control 100,000 stock numbers and 70,000 mechanized storage locations.
- Process and stow 700 receipts per eight hour day.
- Process and pick 1,400 issues per eight hour day.
- Pack 1,400 issues per eight hour day at the consolidation and single item packing stations.
- Delivery 1,400 issues per eight hour day using the Consolidation Manifesting and Transportation System (CMATS).
- Provide on-line interface capability with the Marine Corps SASSY system.
- Provide software for total tracking and control of all transactions.
- Maintain real-time update of all material balances by location.
- Assign stow locations within the mechanized warehouse in real-time and to improve cube utilization.
- Provide management and supervisory information to allow control through corrective adjustments to the system.
- Provide process controlled automation for all warehouse distribution functions including receiving, stowing, picking, packing, and consolidation.
- Print issue documents, packing lists, and packing and stow labels.

²⁵Marine Corps Systems Command, (2001), *STRATIS Secure System Authorization Agreement Outline*.

²⁶*Ibid*.

3. Controls and Threat Description

a. Access

STRATIS has several different types of controls to limit access to the system. Employees access the system with individually assigned employee identification numbers and passwords. Supervisors assign employee identification numbers along with access privileges which determine the type of functions that each employee can perform in the system. Employees can be assigned any one of twenty different security levels that create access to different sets or groups of functions. Authorization to access STRATIS is verified each time an employee signs in.

b. Threats

STRATIS, like the majority of other government systems is vulnerable to a wide assortment of threats. There are threats to the confidentiality and integrity of the data processed, stored, and transmitted by the system. Additional threats exist to the availability of the assets of the system to assist in executing the STRATIS mission. Threats are from those who would target STRATIS for espionage, criminal activity, unlawful use, denial of service, or malicious harm. External or internal threats include espionage, terrorist, hackers, and vandals. The most likely incident involves an authorized user who accidentally or inadvertently commits or omits some action that damages or compromises the system, one of its components, or information processed, stored, or transmitted by the system. The next most likely incident involves an authorized user who takes deliberate action to damage the system, one of its components, or its data for personal gain or vengeful reasons. Such a person could also engage in espionage, other criminal activity, or exploitation or expropriation of the assets of the system for personal gain²⁷.

²⁷Marine Corps Systems Command, (2001), *STRATIS Secure System Authorization Agreement Outline*.

4. Hardware Architecture

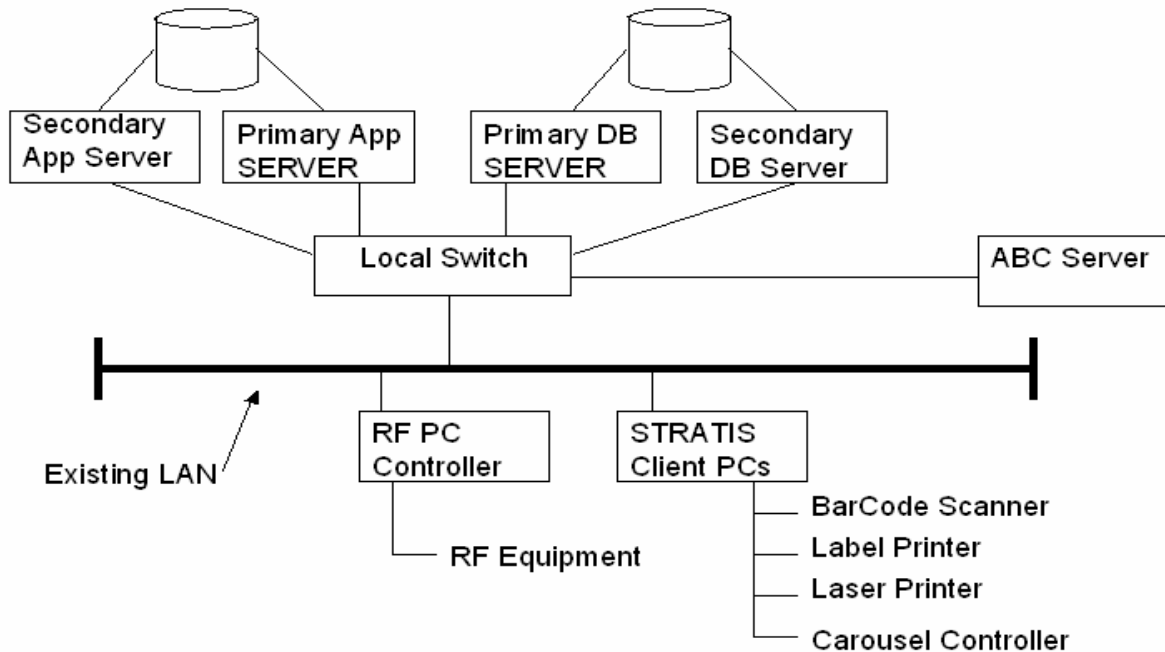


Figure 7. STRATIS Architectural Description (From Ref. ²⁸)

5. Deployable Configuration

The success of STRATIS in garrison has led the Marine Corps to further explore its application in deployed tactical environments. A more portable and “ruggedized” version of STRATIS has already been deployed to Iraq in an attempt to decrease errors and increase efficiency within supply operations. This automated inventory control system is scaled down but still possesses enough capabilities to manage inventory at a dock, vehicle park, warehouse or aboard ship. Figure 8 reflects the scaled down version consisting of a single wireless access point, two “ruggedized” handheld portable RF devices, printer, docking stations, along with the requisite cables and manuals, which can all be secured in a padded metal suitcase.

²⁸Marine Corps Systems Command, (2001), *STRATIS Secure System Authorization Agreement Outline*.

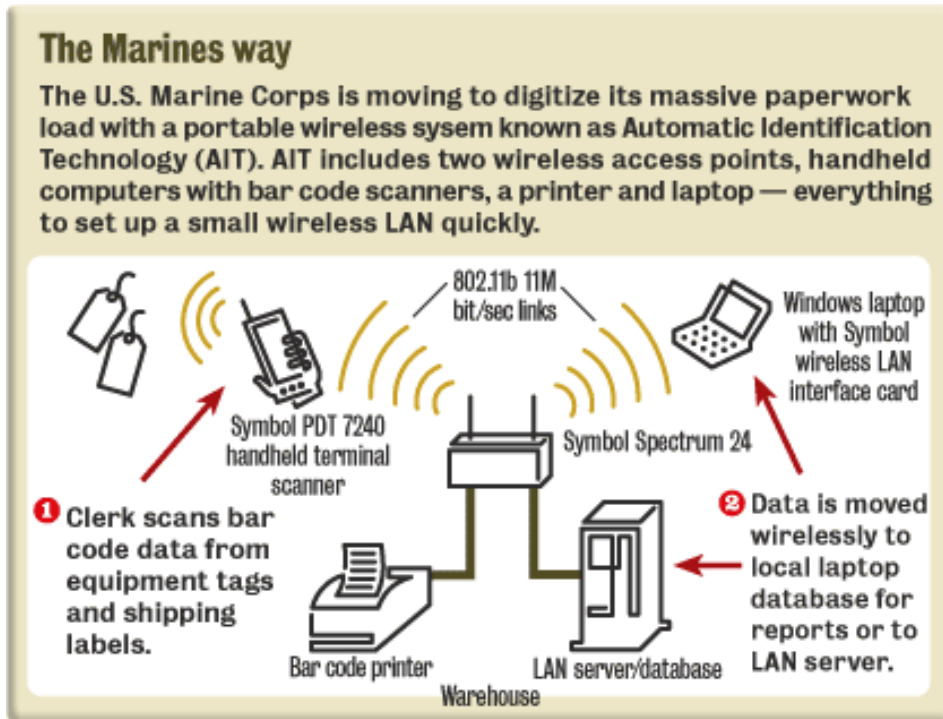


Figure 8. Deployable STRATIS Configuration (From Ref. 29)

These deployable implementations are not intended for the front lines of combat operations. Inventory control is typically conducted in the rear where vital combat service support channels can be protected. However, with the success and obvious improvements to supply chain accuracy and efficiency, STRATIS will be used closer and closer to the battlefield.

D. SUMMARY

The Marine Corps has leveraged 802.11 WLAN technologies for use in several critical applications. These applications possess different vulnerabilities due to the various configurations and encryption methodologies. The STRATIS system has been in operation longer than SECNET-11 but is still a relatively immature wireless implementation. It was developed with a priority on logistical support vice security. The SECNET-11 PC Card and Wireless Bridge technology was developed from the perspective of security from its inception. While both implementations use the same

²⁹John Cox, (2002), Marine Tackle Paperwork with Wireless LAN, *Network World*, Retrieved August 2, 2005, http://www.networkworld.com/news/2002/132978_06-03-2002.

802.11b protocol, they are distinct in their approach to security. One leverages relatively weak encryption schemes while the other employs Type 1 Encryption which is required by the DoD WLAN policy to ensure confidentiality, integrity and availability of wireless transmissions. The vulnerabilities inherent in the STRATIS application make it an ideal candidate for assessment. As a result, it will be reviewed in detail in subsequent chapters.

THIS PAGE INTENTIONALLY LEFT BLANK

V. WIRELESS VULNERABILITY ASSESSMENTS

A. INTRODUCTION

The purpose of this chapter is to discuss the results of several DoD vulnerability assessments that were conducted during the course of our research. These assessments each present distinct characteristics that are worthy of consideration when determining standard procedures for assessing and securing WLANs. In addition, each of these assessments demonstrate the strengths and weaknesses of specific software and hardware tools for the purposes of conducting WLAN vulnerability assessment and monitoring enterprise WLAN assets. A total of three organizations were assessed with emphasis placed on Marine Corps installations. A Joint Command was also assessed in order to compare with the Marine Corps installations.

1. Assessment Tools

There is a wide assortment of tools that are available to conduct vulnerability assessments. During the course of our research we used several open source or shareware tools to gain useful information about WLANs. NetStumbler, a Windows based program used to provide basic WLAN discovery data, along with more advanced LINUX based tools like Kismet and Ethereal are the most popular open sourced tools that were used to conduct our research. There are obviously multiple WLAN tools which can be purchased for WLAN assessment and monitoring. We frequently used various versions of Airopoek, AirMagnet, and Air Defense for our WLAN traffic analysis. In addition, our research required the use of Yellowjacket, a WLAN analyzer with a directional finding capability by Berkeley Varitronics Systems. Each of these tools played an integral role in our assessments. These and other tools will be described and discussed in greater detail in subsequent chapters.

B. ORGANIZATION ONE

1. Background

Organization One is a tenant command on a medium sized installation which was relatively isolated by natural security features of mountain and water boundaries. Civilian and military populations were employed at the installation. The primary threats posed to the organization and installation as a whole was insiders or external threats equipped with high gain antennas. Unclassified, Classified and higher level networks were resident at the installation. Organization One was selected due to the recent implementation of a wireless inventory management system, known as STRATIS. The host installation was not aware of any wireless activity on the installation at the time of the assessment.

2. Wireless Discovery

The assessment was completed in May of 2004. There were no approved wireless implementations at the time; however the organization had a limited compliance waiver which authorized operation of STRATIS at the time of the assessment. STRATIS was the only wireless activity that was found at the installation during the assessment. The following checklist represents a short list of wireless attributes observed during the wireless discovery phase.

3. WLAN Assessment Checklist

Network Type

DSSS	FHSS	Bluetooth	Broadband
802.11a	802.11	802.15	802.16
802.11b			
802.11g			

Network Structure

Independent / Adhoc

Infrastructure / Managed

Network Topology

Point to Point

Point to Multipoint

Channel Usage

1	2	3	4	5	6	7	8	9	10	11
---	---	---	---	---	---	---	---	---	----	----

Access Points

Number 6

Vendor(s) 1) Symbol

MAC Filtering

Yes

No

Physical Access

Yes

No

Configuration Access

Wired

Wireless

Excessive Signal Strength

Yes No

Antenna(s)

Type(s)

Omni-directional

Wireless Hosts/Clients

Number 18

Type(s) 1) Symbol handhelds
2) Laptops
3)

SSID

Names of ESSIDs 1) 22 4)
2) 5)
3) 6)

Broadcasting in Clear ☒ Yes ☐ No

Encryption

Type None

WEP Yes ☒ No Frequency of Key Changes

WPA Yes ☒ No Frequency of Key Changes

IDS

Type None

a. NetStumbler - WLAN Basics

We used an open source tool known as NetStumbler to get some basic information about the network. Figure 9 is a screen shot taken during the assessment used to confirm the MAC Addresses of the access points, the SSID, the channels being used, as well as, the vendor who produced the access point.

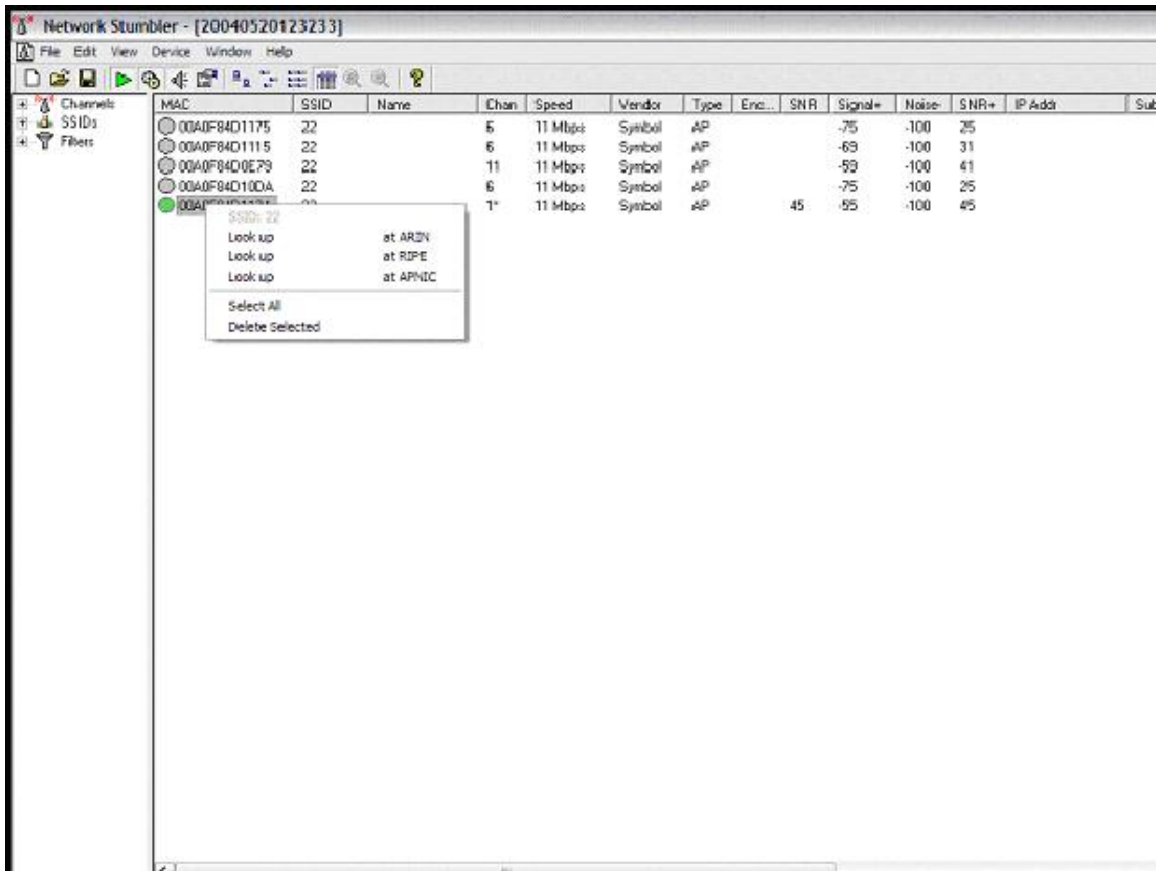


Figure 9. NetStumbler Discovery at Organization One (From Ref. 30)

b. Yellowjacket - Locating and Signal Accessibility

Given basic information about the wireless network, we used YellowJacket directional finding 802.11b Network Analyzer to locate the APs and determine signal accessibility. Yellow Jacket was very effective at physically locating

³⁰Shane Goodwin, Captain USMC, Naval Postgraduate School, NetStumbler Screen Shot, May 20, 2004.

each AP. Three of the six APs were found in locations different from their original planned location. This may have been done to increase signal area, however with the small size of this facility and the strength of each AP, this should not have been a problem. It seems most likely that the installer felt it necessary to separate the AP's by a greater distance than originally planned to create a more symmetrical layout. One of the APs, AP 1 (00:AO:F8:4D:10:DA), was found to have an exceptionally low signal strength. Three of the units had two omni direction antenna attached directly to the unit in the standard fashion. Three other APs were equipped with nonstandard antennas. The APs with non standard antennas had one omni directional attached directly to the unit and another longer outdoor omni directional antenna attached a few feet away. The antennas are likely used to account for coverage area lost due to steel and concrete beams near the installation point. These antennas indicated greater signal strength in all cases except one. The outside antenna associated with AP 4 (00:AO:F8:4D:11:15) was separated by approximately four feet, concrete and steel beams, and windows from the standard omni directional antenna attached directly to the unit. AP 4's nonstandard omni directional antenna showed an extremely weak signal that was likely from the other antenna. This antenna is probably nonfunctional.

4. Results

a. AirMagnet – Advanced WLAN Assessment

Given basic information about the wireless network, to include physical mapping of the network and signal accessibility, the next step was to try to gain access to the network. NetStumbler reflected that the STRATIS implementation was not using WEP. This along with other useful information was confirmed using AirMagnet. One of the helpful tools offered by AirMagnet is a series of warnings or alarms to assist WLAN administrators or hackers in identifying vulnerabilities. AirMagnet identified the following vulnerabilities in Organization One's WLAN:

AP broadcasting SSID (22) in clear text. For security reasons, it is generally recommended that the SSID broadcast be turned off in the AP configuration. Even though turning off SSID broadcast does not secure your WLAN by any definition,

it does prevent your AP from being discovered by war-driving tools such as NetStumbler. Turning off SSID broadcast also blocks out casual WLAN hackers who do not have sophisticated tools and knowledge.

AP with WEP encryption disabled. If a higher-level encryption mechanism such as VPN is not used, data exchange between this AP and its client stations is subject to eavesdropping by intruders. In addition, unauthorized clients without encryption keys can associate with this AP and consume its resources.

Client station with WEP encryption disabled. If higher-level encryption mechanism is not used, WLAN data exchange with this client station is subject to eavesdropping by intruders. In addition, this client station may accidentally associate with any AP outside your organization thus exposing sensitive information stored on the client. Figure 10 below displays these warnings or alarms that were identified by AirMagnet.

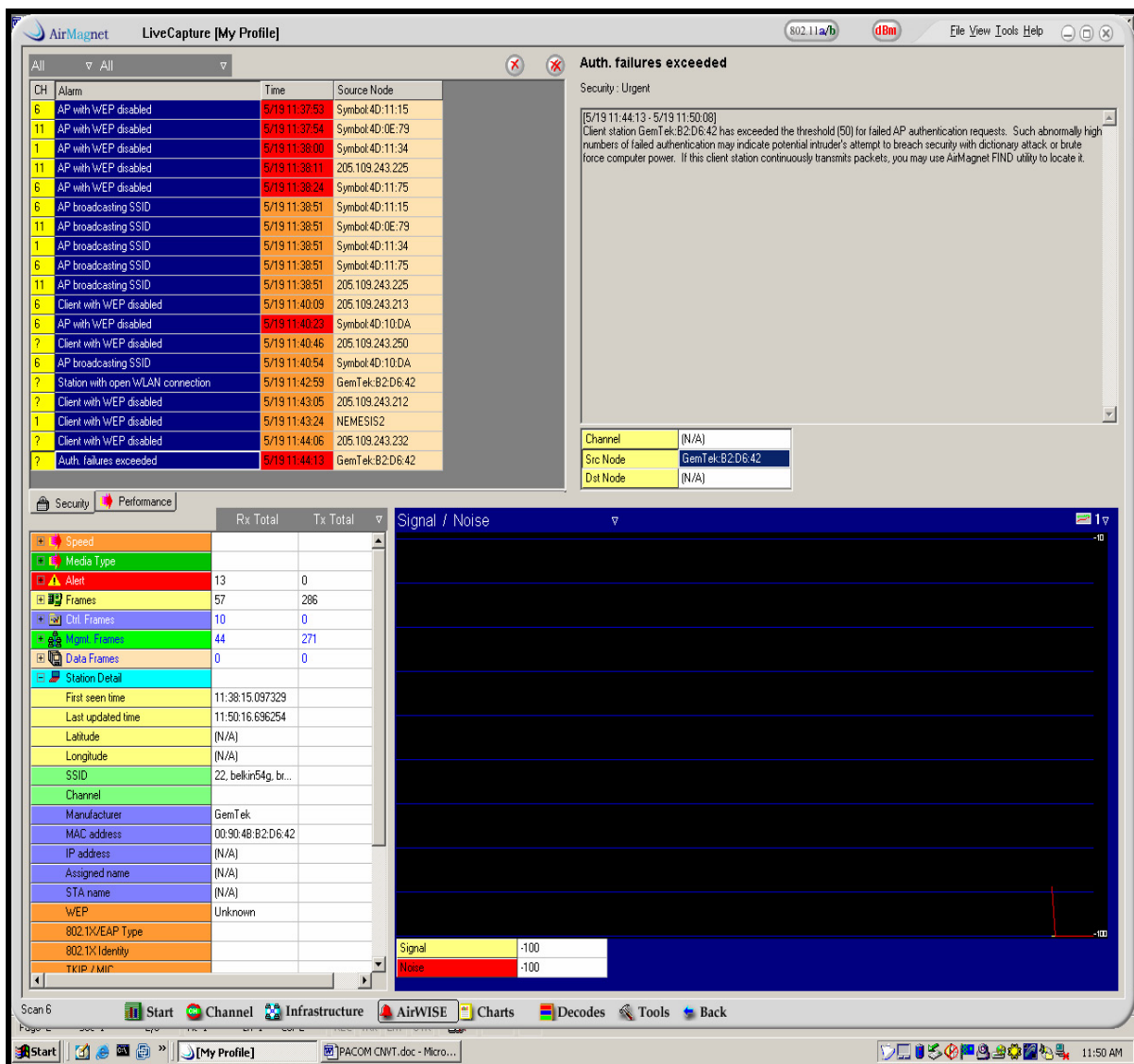


Figure 10. AirMagnet Alarm Notification at Organization One (From Ref. 31)

b. WLAN Exploitation and Expanding Privileges

Since the network did not have WEP enabled, we next attempted to gain access to STRATIS using a standard IPAQ with internal wireless card. Figure 11 displays the IPAQ Network Connections list of available networks by SSID. Organization One was broadcasting the SSID “22”. We quickly connected to the network and gained access to the internet using the STRATIS wireless network.

³¹Adam K. Kessel, Captain USMC, Naval Postgraduate School, AirMagnet Screen Shot, May 19, 2004.

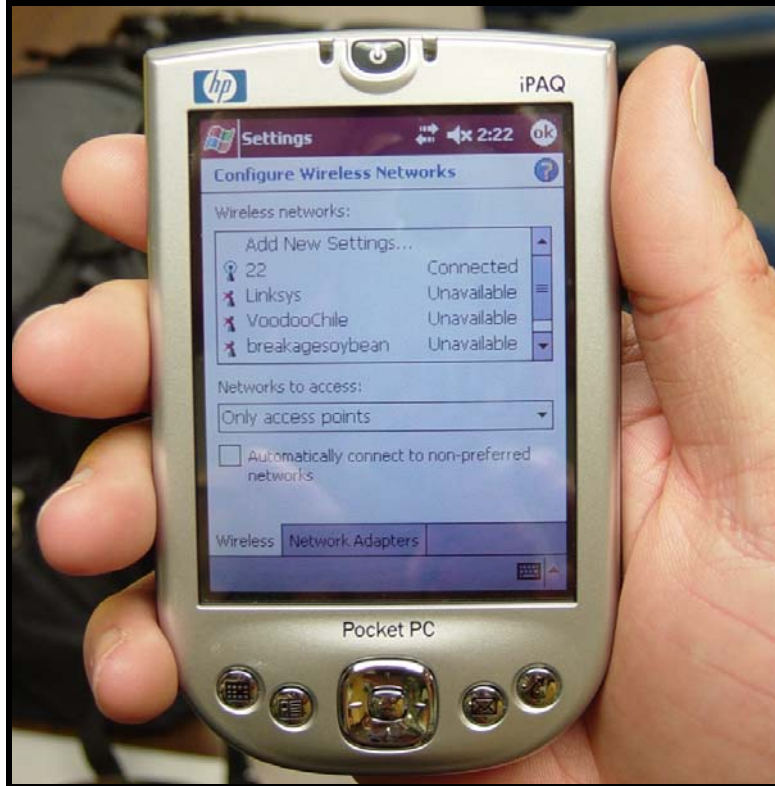


Figure 11. IPAQ Screenshot showing connection to SSID 22 (From Ref. 32)

Once we associated to the network and gained access to the internet, we scanned the network to get a range of IP addresses for the STRATIS network. With IP addresses in hand, we searched the internet for default AP configurations in our first attempt to increase privileges. Figure 12 below shows the IP of one of the six access points which was plugged into the browser to display the Symbol Access Point configuration page. This page shows basic system statistics with very little sensitive information other than the known access points, their IP addresses and MAC addresses. After attempting to click on any of the configuration links, you are prompted for a user name and password.

³²Shane Goodwin, Captain USMC, Naval Postgraduate School, IPAQ Network Connections Screen Shot, May 19, 2004.

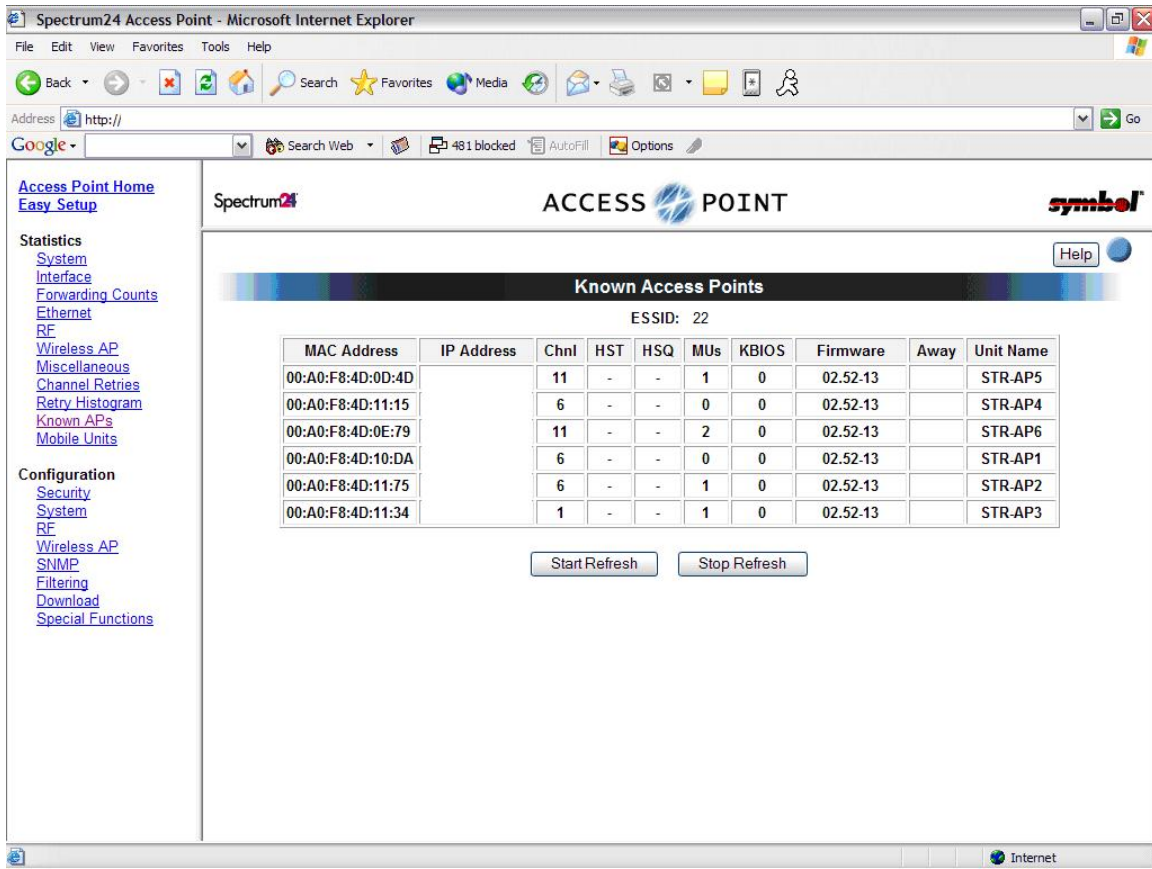


Figure 12. Symbol AP Configuration Webpage (From Ref. 33)

In order to figure out the user name and password, the Symbol's corporate web site was accessed. The Symbol Access Point manual and reference guide, which is in Figure 13 below, contained the default settings.

³³Shane Goodwin, Captain USMC, Naval Postgraduate School, Symbol AP Configuration Webpage Screen Shot, May 19 2004.

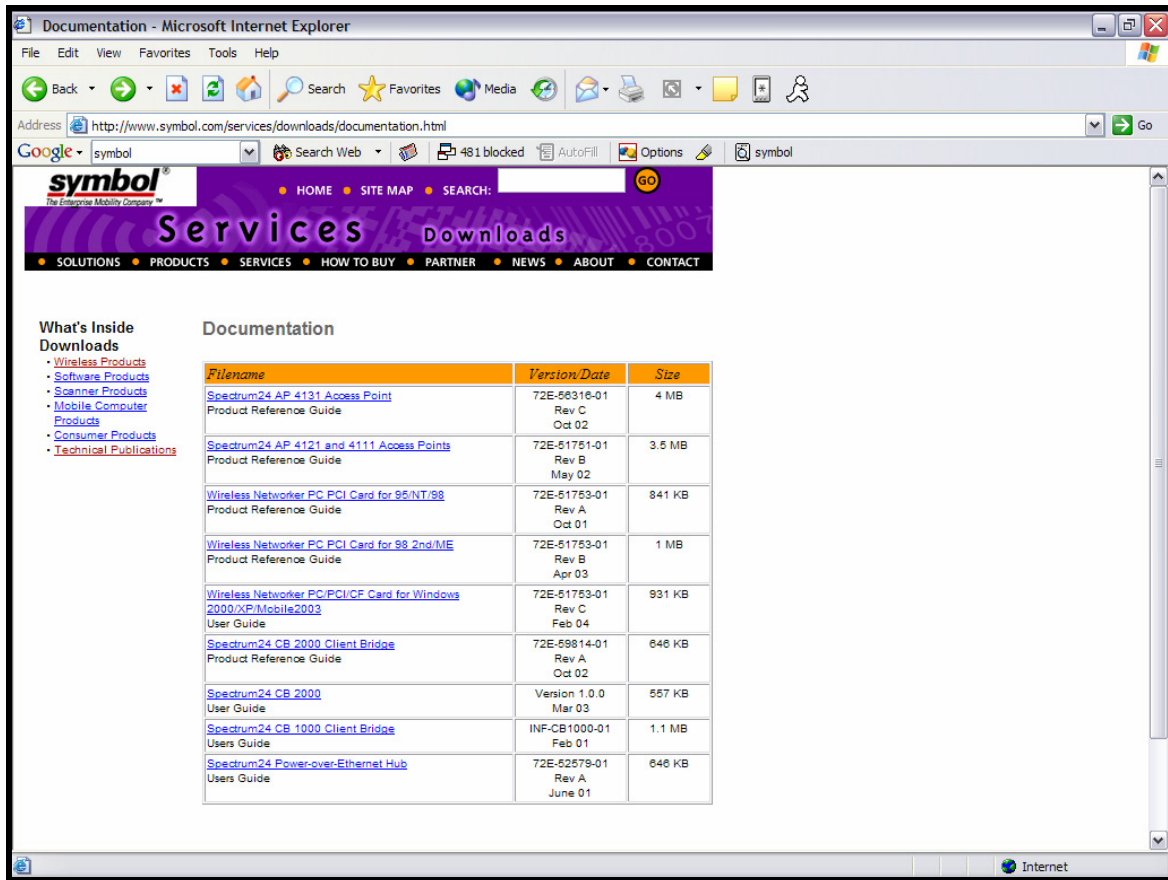


Figure 13. Symbol Website Containing AP Configuration Guidelines (From Ref. 34)

After a quick document search of the reference manual, the default login and password were found. The reference manual indicated that the default userid was Admin and the default password was Symbol. Figure 14 is a screenshot from Symbol's reference manual which documents this information.

³⁴Shane Goodwin, Captain USMC, Naval Postgraduate School, Symbol AP Configuration Webpage Screen Shot, May 19 2004.

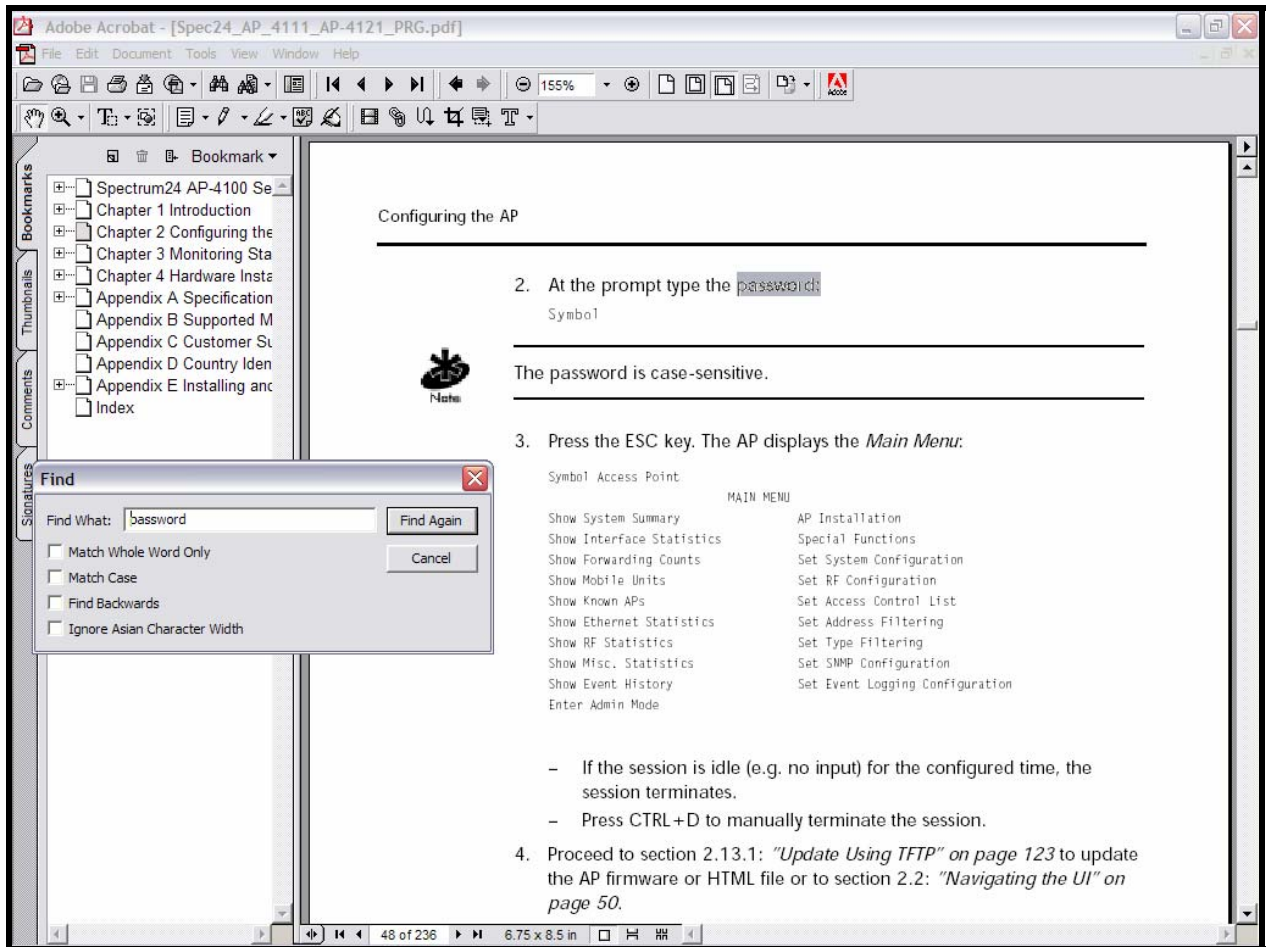


Figure 14. Symbol Reference Manual Reflecting Default AP Configuration (From Ref. 35)

The next step was to attempt to use this default password. As shown in the following Figures 15 and 16, the default userid and password allowed a connection to the STRATIS AP's configuration page with full access to the configuration links. This included access to encryption keys as well as modifying any option and setting the AP configuration password.

³⁵Shane Goodwin, Captain USMC, Naval Postgraduate School, Symbol AP Configuration Reference Manual Screen Shot, May 19, 2004.

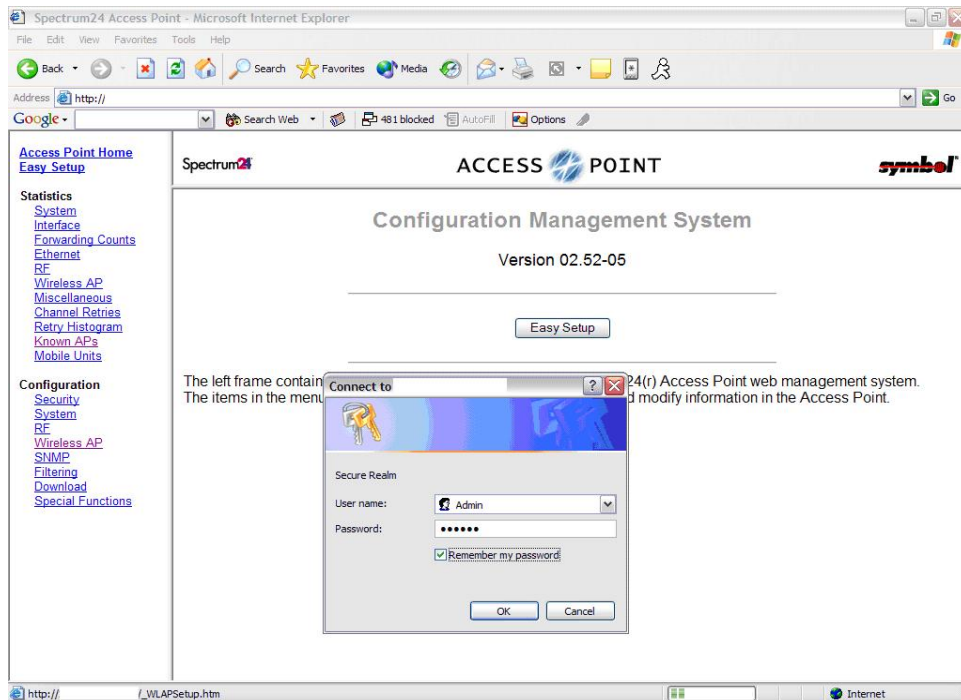


Figure 15. Symbol AP Configuration Webpage (From Ref. 36)

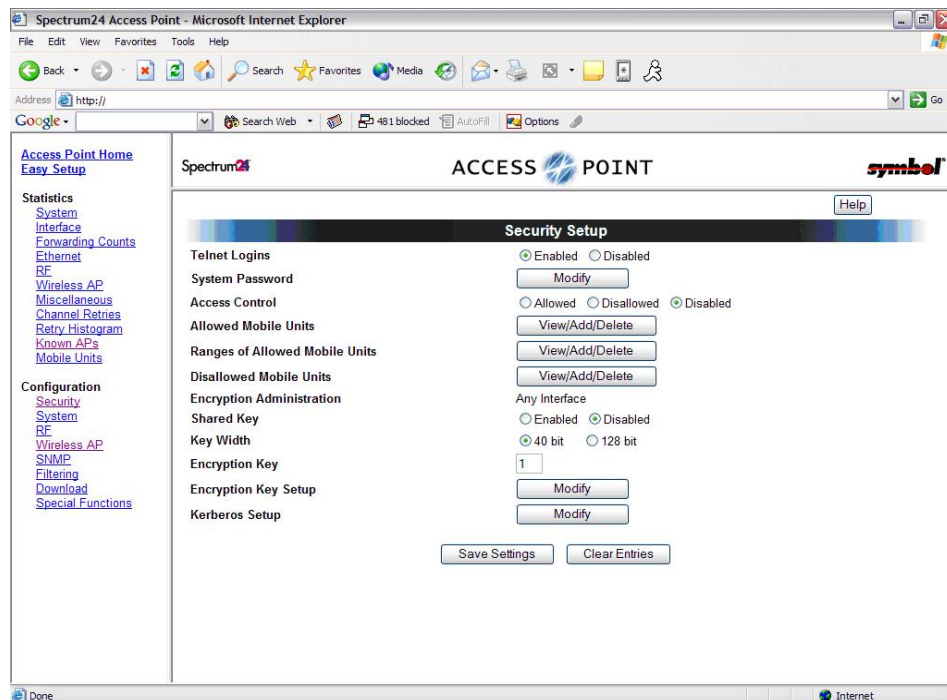


Figure 16. Symbol AP Configuration Webpage (From Ref. 37)

³⁶Shane Goodwin, Captain USMC, Naval Postgraduate School, Symbol AP Configuration Webpage Screen Shot, May 19, 2004

From Figure 17, it was apparent that the telnet feature could be exploited. With the telnet logins enabled, an adversary could telnet to the access point and have the same control using the command prompt as with the web enabled configuration page. Figure 17 is a screenshot from the telnet interface. From this interface, almost any desired configuration changes could be made to the AP. This access represents a significant vulnerability to the STRATIS wireless network.

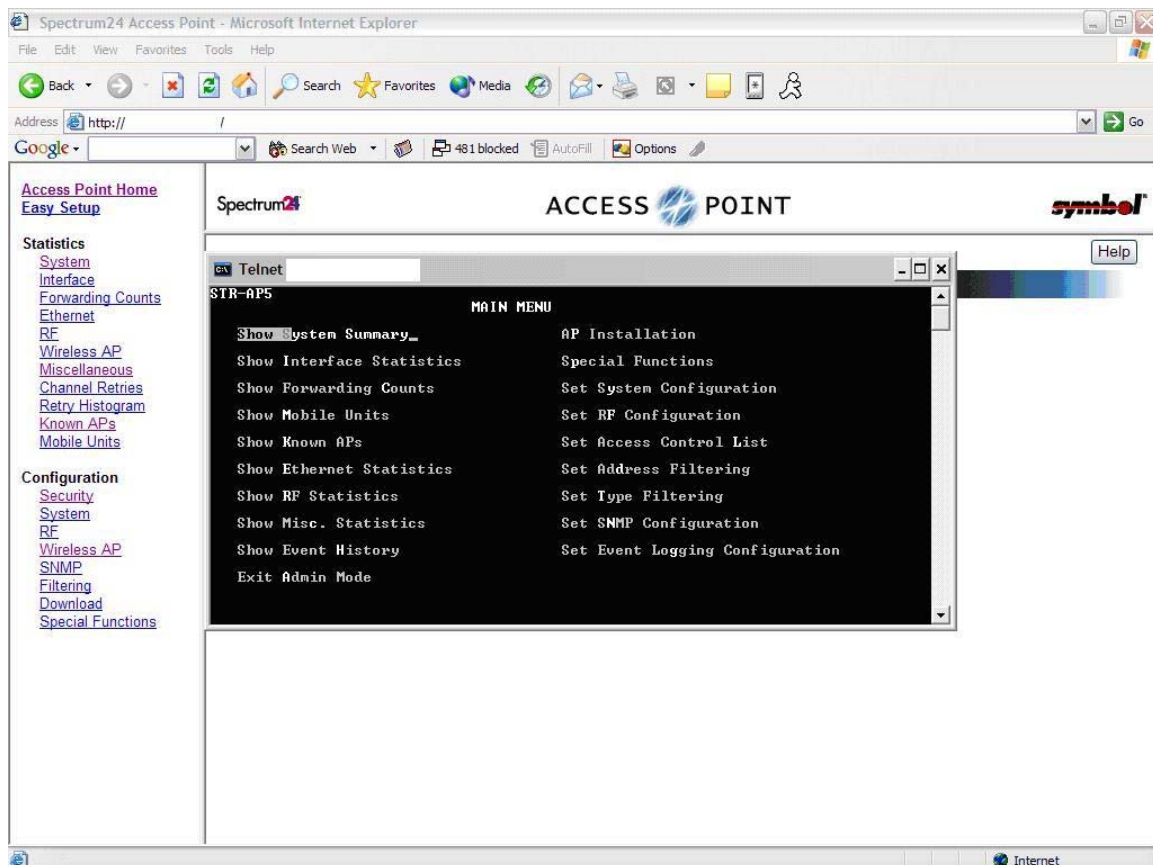


Figure 17. Telnet AP Interface (From Ref. 38)

³⁷Shane Goodwin, Captain USMC, Naval Postgraduate School, Symbol AP Configuration Webpage Screen Shot, May 19, 2004.

³⁸Shane Goodwin, Captain USMC, Naval Postgraduate School, Symbol AP Configuration Telnet Screen Shot, May 19, 2004.

5. Recommendations

Based on the poor security posture of Organization One's STRATIS implementation there were many recommendations that could be made to improve security for the wireless network.

a. Turn Encryption On.

This will require individually configuring each of the access points as well as each handheld device that connects to this network.

b. Change the Default Password on Each Access Point.

NSA currently recommends a minimum 12-character password using four different character sets.

c. Turn the Broadcast Power Down.

The STRATIS APs allow varying power settings. By setting the power to a lower level, the distance at which a signal may be accessible is reduced.

d. Restrict Access to the Access Points by MAC Address.

Each wireless device allowed to access the network must be identified to each access point. Create an access control list for the APs to specifically authorize clients to communicate on the network.

e. Do Not Broadcast the SSID.

By broadcasting the SSID, a required piece of information to access the network is automatically provided to an unauthorized user.

f. Separate STRATIS From the NIPRNET and Base Networks.

Logically separate the STRATIS network. Logically separate the wireless portion. Physically separate building infrastructure.

C. ORGANIZATION TWO

1. Background

Organization Two was carefully selected in order to compare results found from Organization One approximately two years later. Both organizations are very similar

with regard to geography, military and civilian activity, authorized wireless networks and network size. This particular organization has very few areas that are susceptible to the threat of off-base wireless scanning due to the majority of the units being tucked away in between very high elevation ridgelines. Classified and Unclassified networks are resident on this installation with no wireless classified networks detected.

2. Wireless Discovery

In the time span of two years, between 2003 and 2005, not only has access to wireless equipment increased but the number of unauthorized WLANs on DoD installations has dramatically increased. The Kismet scanner found over 75 different WLANs not including base housing. A small amount of these are legitimate networks that have been authorized because they are not on the NIPR network and are operating in an official capacity such as the Commissary, Post Exchange, and specific financial relief organizations. Otherwise, there are only two authorized WLANs allowed by the DAA on this installation with waivers because they do not abide by the Marine Corps' wireless policy.

The following checklist represents a short list of wireless attributes observed during the wireless discovery phase.

3. WLAN Assessment Checklist

Network Type

DSSS	FHSS	Bluetooth	Broadband
802.11a	802.11	802.15	802.16
802.11b			
802.11g			

Network Structure

Independent / Adhoc

Infrastructure / Managed

Network Topology

Point to Point

Point to Multipoint

Channel Usage

1 2 3 4 5 6 7 8 9 10 11

Access Points

Number 14

Vendor(s)
1) Symbol
2) Linksys
3) Netgear

MAC Filtering

Yes

No

Physical Access

Yes

No

Configuration Access

Wired

Wireless

Excessive Signal Strength

Yes No

Antenna(s)

Type(s)

Omni-directional
Yagi (directional)**Wireless Hosts/Clients**

Number

56

Type(s)

1) Symbol handhelds

2) Laptops

3) PDAs

SSID

Names of ESSIDs

1) ESSID

4)

2) linksys

5)

3)

6)

Broadcasting in Clear

Yes

No**Encryption**

Type

WEP

WEP

Yes

No

Frequency of Key Changes

Monthly

WPA

Yes

No

Frequency of Key Changes

N/A**IDS**

Type

None

4. Results

Overall, there were more wireless networks on this particular installation than on any other installation that was assessed.

As mentioned in the previous chapter, the STRATIS wireless inventory system is of particular interest due to its unsecured implementation. It was found that the STRATIS system on this installation did have WEP enabled. This is an improvement from what was seen 2 years ago where the WLAN was wide open with no encryption or WEP enabled. In addition, nothing was established to ensure RF signals did not propagate outside of the work area. These vulnerabilities were addressed by Headquarters United States Marine Corps C4/IA with the STRATIS Wireless Networking Configuration message which states the requirements that each system must meet within 30 days of the release of the message.

According to the message, “Wireless networking technologies are approved for use with the STRATIS system only when configured in accordance with the approved SSAA, wireless security best practices, and other DoD/DoN/USMC policies/procedures. If the wireless component of the STRATIS system is operated without the appropriate security measures in place, severe vulnerabilities would be introduced to the data, as well as the enterprise network.³⁹” In this case, STRATIS is approved for use in accordance with the Marine Corps Information Assurance Operational Standard⁴⁰ that provides waivers for certain networks that the DAA deems appropriate. This wireless network did not comply with the requirements within the message in a few different areas. The message states that WPA should be enabled if available and WEP was still in place at this installation. The Symbol website displayed firmware upgrades that were available with WPA security for certain APs but not for legacy devices which are installed in this case. This would require the replacement of old APs with newer technology and higher security features. It is recommended that all organizations with the legacy APs installed, purchase new hardware that is certified to be compatible with the IEEE 802.11i standard which enables WPA security. Finally, the WEP was being changed once a month which

³⁹Jeffrey Watts, STRATIS message from Headquarters Marine Corps C4/IA, STRATIS Wireless Networking Configuration, July 2004.

⁴⁰United States Marine Corps (USMC) Information Assurance Operational Standard, (2005), 014 *Wireless Local Area Networks V 1.0*, (USMC IA OPSTD 014).

is better than not changing at all but the message requires rotating the key weekly. Although this helps to ensure someone would not have access to the network for more than a week, most WEP implementations can be cracked very quickly due to one of the many weaknesses in WEP. This security weakness involves the recovery of the secret key after intercepting and analyzing only a relatively small amount of traffic. This attack is publicly available as an attack script and open source code⁴¹.

Figures 18 and 19 display the Symbol Access Point web configuration Security Setup and Access Control List.

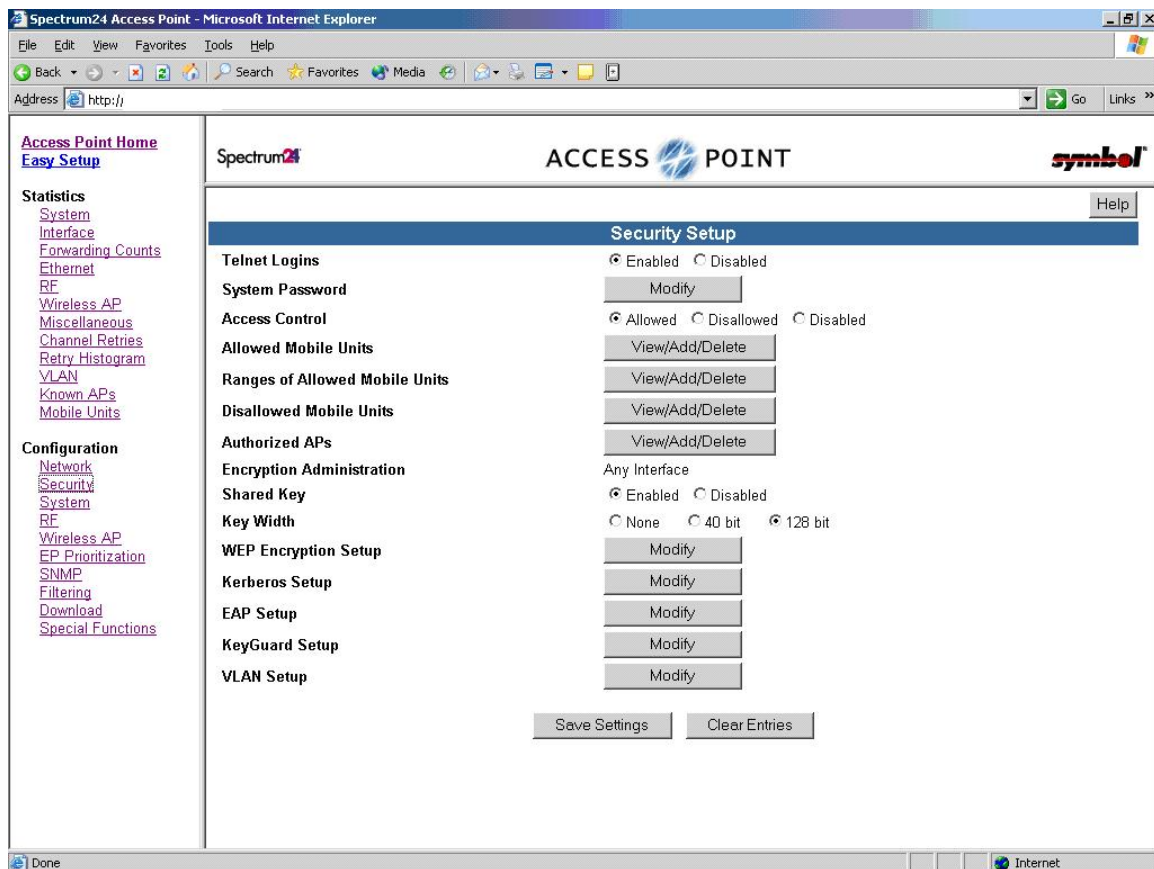


Figure 18. Symbol AP configuration Telnet Login enabled (From Ref. 42)

⁴¹National Institute of Standards and Technology (NIST), (2002), *Wireless Network Security; 802.11 Bluetooth and Handheld Devices*, (Special Publication 800-48).

⁴²Adam K. Kessel, Captain USMC, Naval Postgraduate School, Symbol AP Configuration Webpage Screen Shot, August 4 2005.

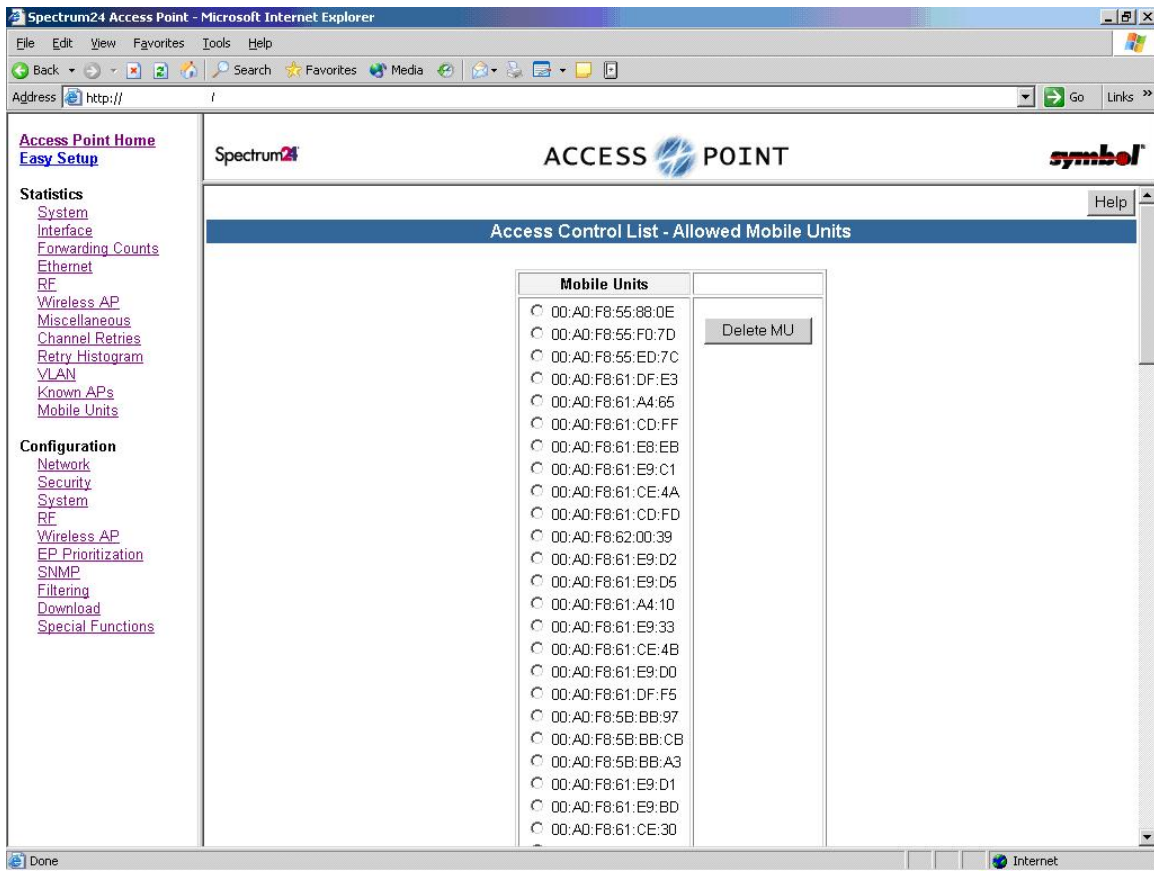


Figure 19. Symbol AP Access Control List (From Ref. 43)

Figure 20 displays a Kismet screenshot which shows STRATIS access points whose SSIDs were changed from the default to “ESSID” as well as the linksys AP with WEP disabled.

⁴³Adam K. Kessel, Captain USMC, Naval Postgraduate School, Symbol AP Access Control List Webpage Screen Shot, August 4 2005.

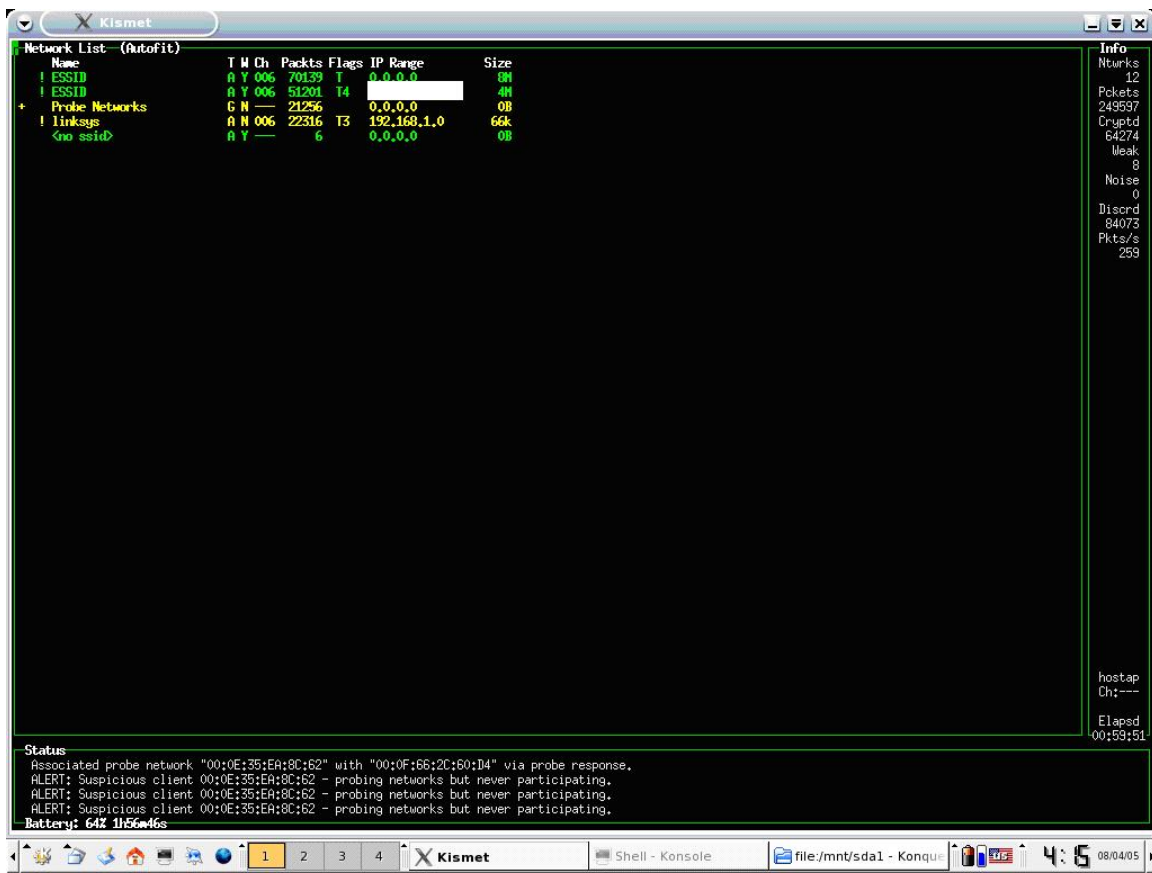


Figure 20. Kismet screen capture linksys WEP disabled (From Ref. 44)

Figure 21 shows the network details of a single STRATIS AP with its MAC address.

⁴⁴Adam K. Kessel, Captain USMC, Naval Postgraduate School, Kismet Screen Shot, August 4 2005.

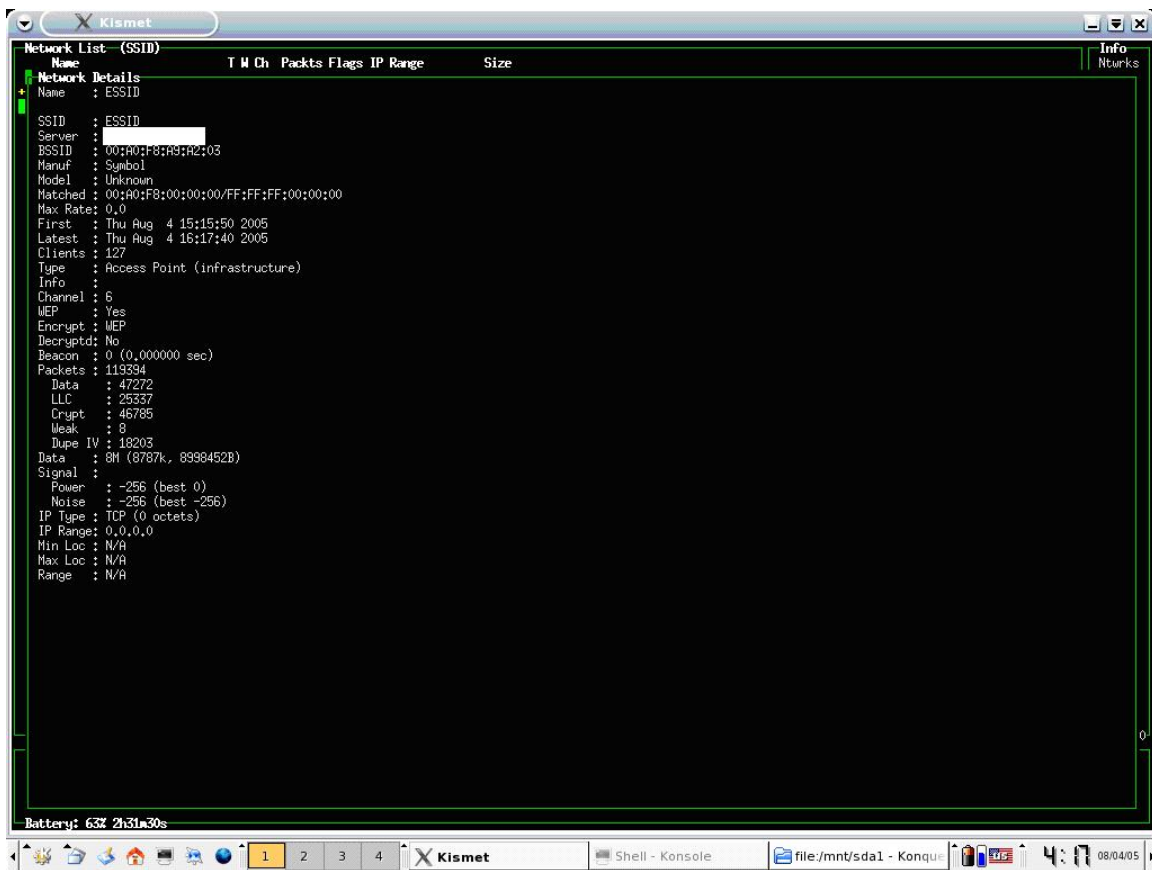


Figure 21. Kismet screen capture ESSID network details (From Ref. 45)

A serious vulnerability that was observed within the STRATIS system was a stand-alone Linksys wireless AP within the confines of the warehouse which was connected to a Cox cable commercial ISP. Although this was separated from the NIPR network, not only was the AP open with no WEP enabled, but they were transmitting information from the STRATIS system. This basically subverts all security mechanisms that are enabled on the STRATIS network because they are transmitting unencrypted, official traffic over an unapproved wireless network.

Figure 22 displays an Airopeek capture screenshot of the two Linksys Access Points.

⁴⁵Adam K. Kessel, Captain USMC, Naval Postgraduate School, Kismet Screen Shot, August 4 2005.

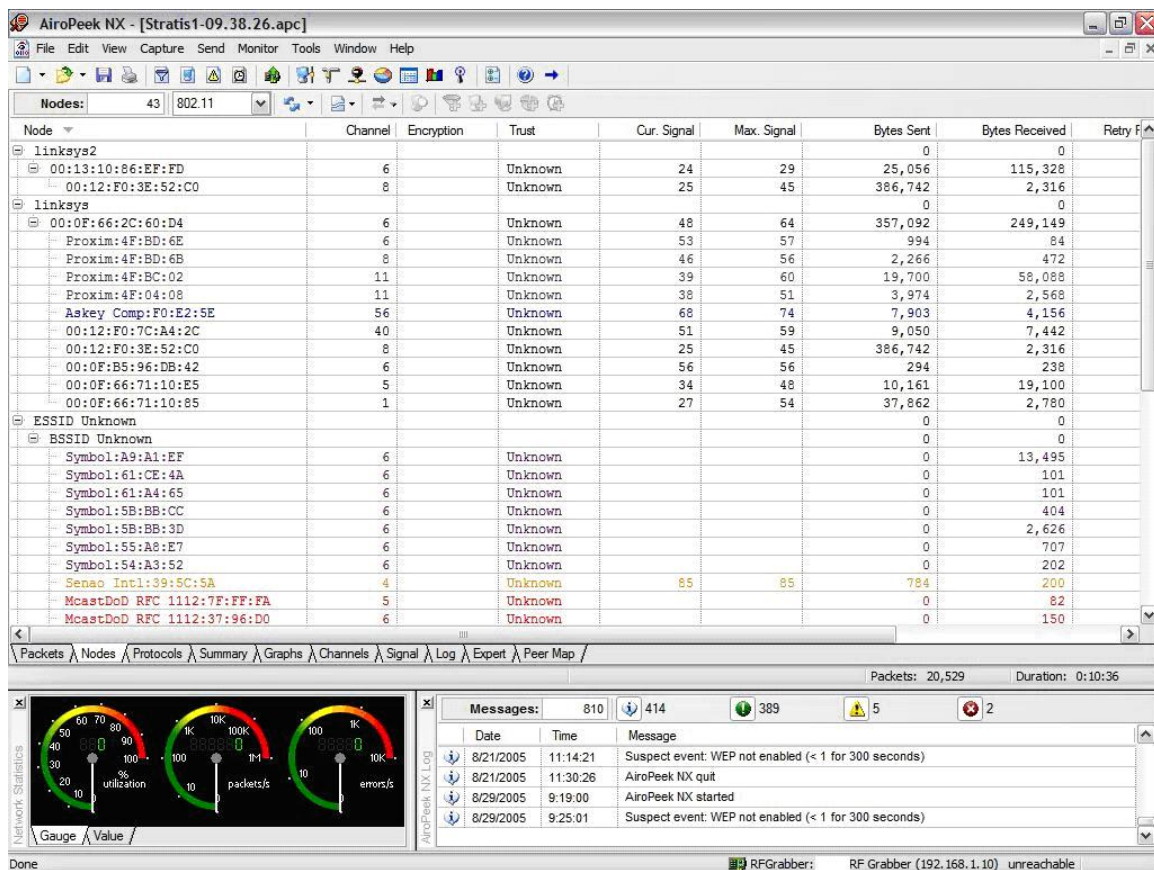


Figure 22. Airopeek screen capture linksys WEP disabled (From Ref. 46)

One final configuration issue that was observed was a connection to the NIPR network between warehouses which was used to connect the wireless networks together. This introduces the possibility of a wireless attacker gaining access to the NIPR network which otherwise could be prevented. A solution to this issue would be to switch the operating mode of the APs at the end of the warehouses from root to repeater mode. This essentially links the two APs together without adding a wired link between them. This can easily be done if they are relatively close together or a directional antenna can be installed on each end to ensure the appropriate RF range output.

The biggest problem that remains for these organizations is how to determine what wireless networks are authorized or unauthorized and if they are authorized, how to locate and disable them on a regular basis. In the following two chapters a number of

⁴⁶Adam K. Kessel, Captain USMC, Naval Postgraduate School, Airopeek Screen Shot, August 4 2005.

recommendations will be discussed to help these organizations with finding solutions and procedures that will address wireless vulnerabilities.

D. ORGANIZATION THREE

1. Background

Organization Three was selected in order to assess the overall security of a well known unclassified secure wireless network. This organization's implementation will be discussed in detail in a complete chapter because of the significant security and well thought out layered defense structure of the wireless network. Many agencies have been involved in the testing and assessment of this network to include the NSA, FIWC, Naval Postgraduate School, and Mitre Corporation. This particular organization has a very small footprint with one building on the installation with wireless access and a remote facility with interconnected wireless roughly three miles away. The geography presents many opportunities for remote access to the RF medium due to the proximity of homes, businesses, and a major highway within a few hundred yards of the installation. All U.S. military services are represented at this installation and many foreign service representatives as well as a large population of civil service workers and contractors. At the time of the assessment the only authorized wireless networks was the WLAN which was assessed. Classified and Unclassified networks are resident on this installation with no wireless classified networks detected.

2. Wireless Discovery

The Kismet scanner found over 50 APs with many clients roaming between them. Although it was simple to scan the RF medium to view wireless traffic it was impossible to analyze any of the captured traffic due to the Layer 2 encryption employed through Air Fortress. We were able to see through an AiropEEK capture in Figure 23 that they were using Vocera communication devices over their wireless network. The phone network runs on Cisco's VOIP technology and the Vocera communicators have recently been implemented to extend the reach of the VOIP network to include mobile inter and intra-building communications. Initially it was thought that it may be possible to hack into the

network through this vulnerability due to VOIP's known vulnerabilities. Vocera software supported the 64-bit wired equivalent privacy (WEP) and 128-bit WEP protocols, as well as virtual LANs (VLAN) which would be easy to crack and develop as an attack vector. Recently Vocera added support for Cisco's lightweight extensible authentication protocol (LEAP) and temporal key integrity protocol (TKIP). In addition, the company has released support for Wi-Fi protected access (WPA) which will be implemented completely when the 802.11i protocol is ratified.

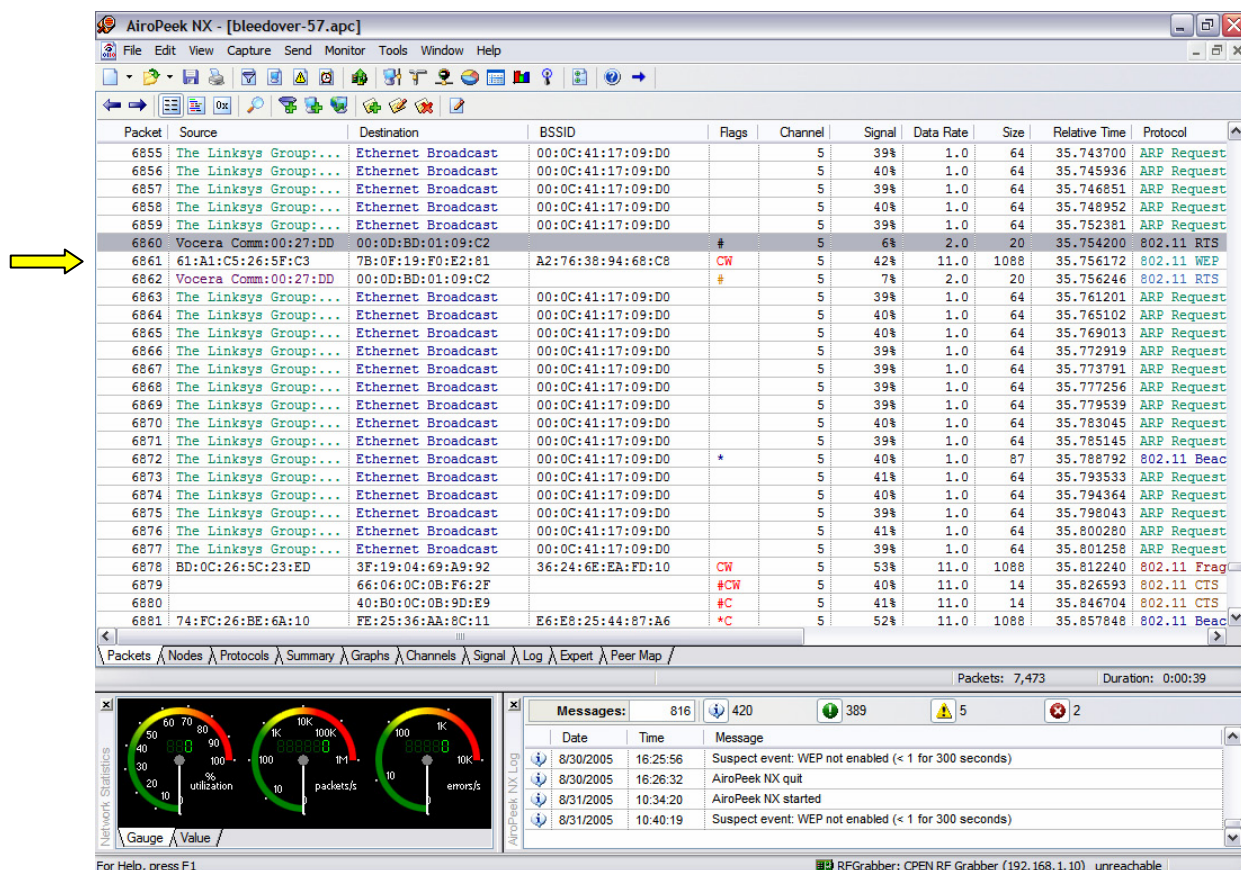


Figure 23. Airopeek screen capture Vocera devices on network (From Ref. 47)

The following checklist represents a short list of wireless attributes observed during the wireless discovery phase.

⁴⁷Adam K. Kessel, Captain USMC, Naval Postgraduate School, Airopeek Screen Shot, August 4 2005.

3. WLAN Assessment Checklist

Network Type

☒ DSSS	☐ FHSS	☐ Bluetooth	☐ Broadband
☒ 802.11a ☒ 802.11b ☐ 802.11g	☐ 802.11	☒ 802.15	☐ 802.16

Network Structure

☐ Independent / Adhoc

☒ Infrastructure / Managed

Network Topology

☒ Point to Point

☐ Point to Multipoint

Channel Usage

☒ 1	☐ 2	☐ 3	☐ 4	☐ 5	☒ 6	☐ 7	☐ 8	☐ 9	☐ 10	☒ 11
------------------------------------	-------------------------	-------------------------	-------------------------	-------------------------	------------------------------------	-------------------------	-------------------------	-------------------------	--------------------------	-------------------------------------

Access Points

Number 54

Vendor(s) 1) Cisco

MAC Filtering

Yes

☒ No

Physical Access

Yes

☒ No

Configuration Access

☒ Wired

Wireless

Excessive Signal Strength

Yes

☒ No

Antenna(s)

Type(s)

Omni-directional
Yagi (directional)**Wireless Hosts/Clients**

Number

500

Type(s)

1) Desktops

4) VOIP communicators

2) Laptops

3) PDAs

SSID

Names of ESSIDs

1) ESSID

Broadcasting in Clear

Yes

☒ No**Encryption**

Type

WEP & Layer 2 AES (FIPS 140-2 validated)

WEP

☒ Yes

No

Frequency of Key Changes

Monthly

WPA

Yes

☒ No

Frequency of Key Changes

N/A**IDS**

Type

Air Defense WIDS

4. Results

This organization built their wireless network from the ground up with security at the forefront. Although the scope of our wireless assessment was not meant to be a full spectrum assessment, it is clear that this WLAN is secure in the implementation of layer 2 data encryption and device/user authentication. We were able to detect the presence of 802.11 networks, the AP SSIDs being used, which channels each access point was operating on, and clients probing for an access point to associate to. In addition, we were able to ascertain from Airopeek data captures that they were using Vocera communicators within the WLAN. It was impossible to capture any IP addresses because of the encryption. The beginning stages of scanning, footprinting, and then enumeration generally require IP addresses to be visible in order to initiate any attack sequences. Due to strong encryption techniques it was impossible to read any IP level data or capture device/user logins.

a. Denial of Service

Although IP addresses were not visible we were able to capture the MAC addresses of the APs, as shown in Figure 24, which allows us to initiate various attacks including Denial of Service (DoS) attacks.

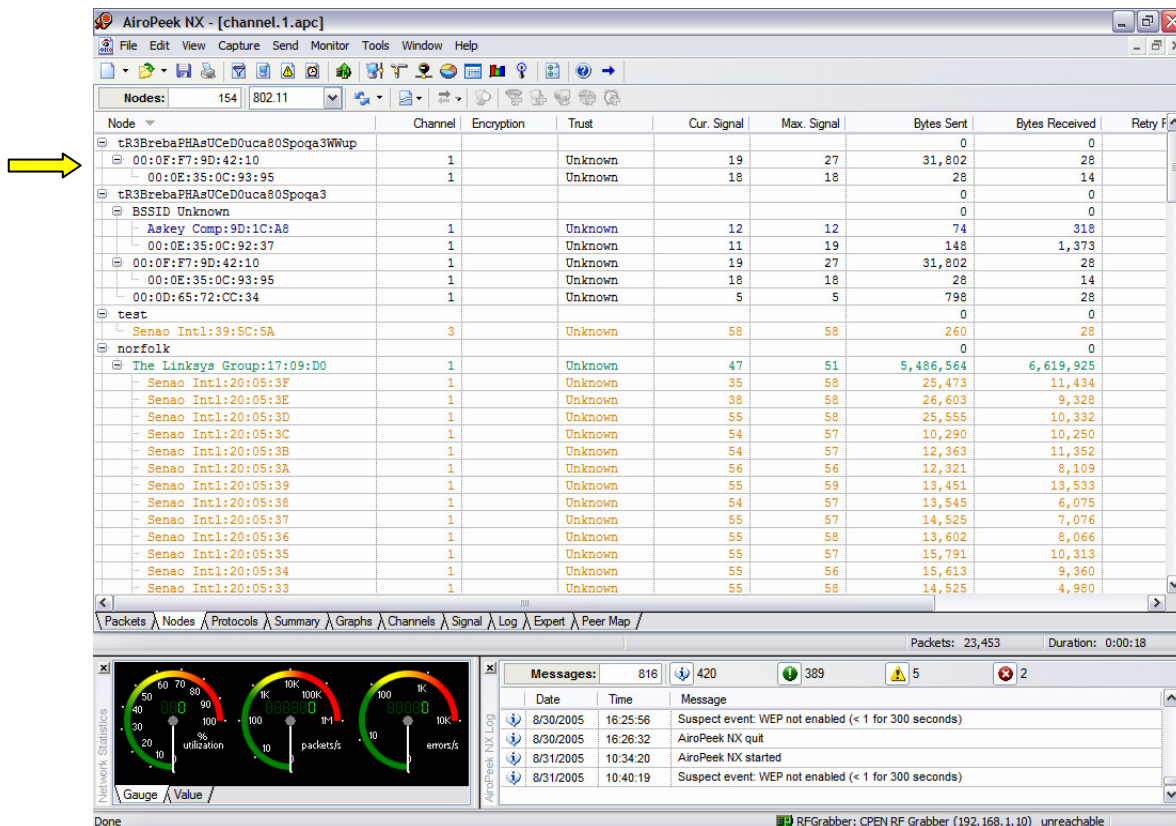


Figure 24. Airopeek screen capture AP MAC addresses visible (From Ref. 48)

Another weakness in Vocera communicator's configuration is the fact that it is possible to scan the entire IP subnet in which the VOIP network resides and a DoS results. This would be a subset of an actual physical layer DoS attack where the entire RF medium is taken up by a high powered RF signal. This means that although any specific DoS attack may accomplish the same objective, a physical layer DoS attack wipes out all traffic on the wireless medium.

One major discovery that was found during the course of this assessment was AirDefense's inability to detect and report on the active packet injection attack used in the process of cracking the WEP key. In addition, AirDefense did not report any abnormalities within the WLAN while we initiated the inaugural "MSAK attack.⁴⁹"

⁴⁸Adam K. Kessel, Captain USMC, Naval Postgraduate School, Airopeek Screen Shot, August 4 2005.

⁴⁹Adam K. Kessel, Captain USMC, Naval Postgraduate School, (Michael Shane Adam Kessel Attack), Term which defines the combination of a specific DoS attack and WEP cracking attack, 23 August 2005.

The MSAK attack involves the use of Communication Machinery Corporation's Emulation Engines which are used to emulate 128 wireless clients transmitting up to 1024 bytes of ICMP traffic every cycle on a targeted AP. This results in an overload of data on an AP with the resultant 725 packets-per-second and up to 6 Mbps per virtual station. This means an individual AP can receive up to 1024Mbps total with 128 vSTAs. This attack increases the total number of packets traversing the WLAN which dramatically decreases the amount of time needed to crack the WEP using Shmoo Group's open source WEP cracking tool AirCrack. The attack's intricate details are omitted. Figure 25 shows the result of the attack which reveals the secret WEP key.

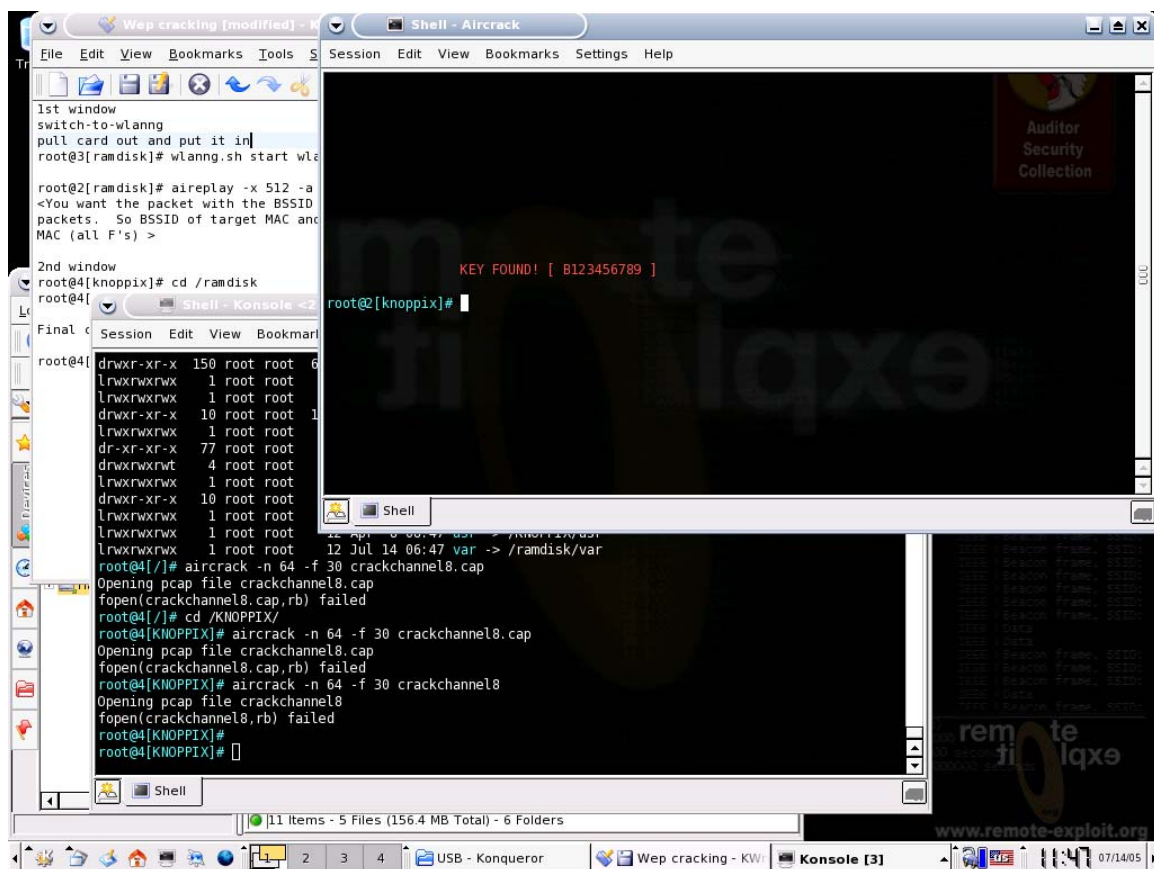


Figure 25. WEP attack using Aircrack 64 bit key (From Ref. 50)

Figure 26 displays an Airopeek capture of the 128 virtual stations which are represented by the MAC address of Senao Intl. The two Linksys Group points

⁵⁰Adam K. Kessel, Captain USMC, Naval Postgraduate School, Aircrack Screen Shot, August 2, 2005.

represent the two Emulation Engines which were connected via a Linksys WAP55AG access point.

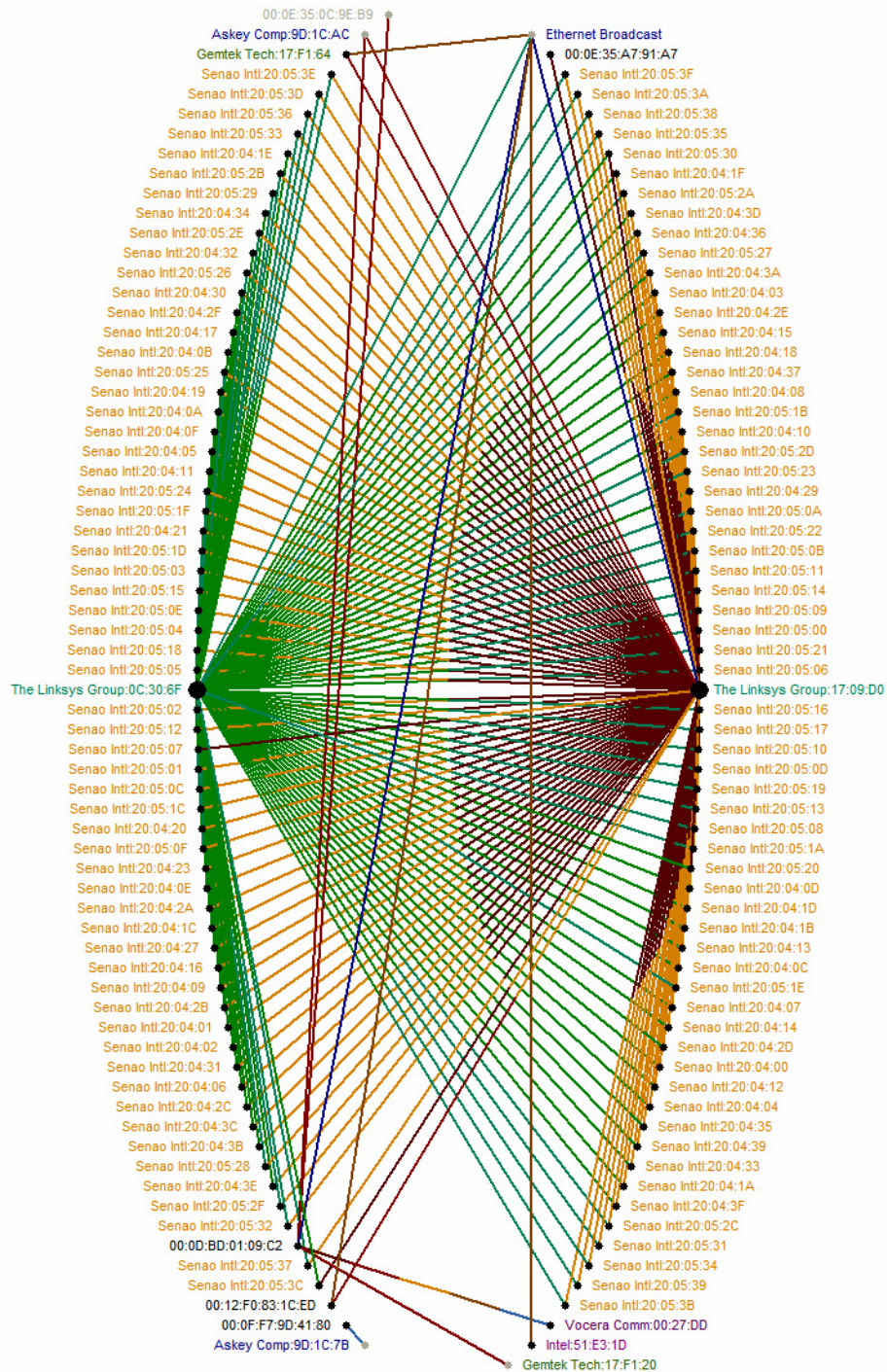


Figure 26. Airoppeek screen capture CMC Emulator DoS (From Ref. 51)

⁵¹Adam K. Kessel, Captain USMC, Naval Postgraduate School, Airoppeek Screen Shot, August 4 2005.

The Emulation Engine allows the user to create up to 64 configurable, concurrent, Virtual Stations (vSTA) that emulate 802.11 Wireless Local Area Network stations. Each vSTA has a unique, user configurable, MAC and IP address allowing it to fully Authenticate, Associate, Deauthenticate and Disassociate as well as transmit and receive frames using IEEE 802.11 a/b/g. Test data traffic can be generated per individual concurrent vSTA and actively injected through these 802.11 vSTAs into AP and WLAN systems under test in two different modes: 1. Internal - traffic is generated internally by each vSTA as configurable Ping traffic; 2. External - Data is sourced from various industry standard third party load generators over 802.3 Ethernet, mapped to each vSTA by IP address, and forwarded over 802.11a to the WLAN device under test by the emulator⁵².

This organization's implementation plan will be explored in more detail in Chapter VIII but it cannot be emphasized enough that availability always poses a serious security risk for even the most accomplished Wireless Administrators. The research found within this chapter concludes that even the most secure WLAN that has significant penetration testing completed, can be vulnerable to multiple types of DoS attacks which completely shutdown access to the network as it did in this case. It is recommended that all WLANs should either have a wired backup or should not be used for mission critical systems.

⁵²Robert Hoskins, (2005), CMC's New Wi-Fi Virtual Station Emulator Enables Load Testing of 802.11 Devices and WLAN Systems, *Broadband Wireless Exchange Magazine*, Retrieved August 31, 2005, <http://www.bbwxchange.com/news/2003/may/cmc052103.asp>.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. EVALUATION OF SOFTWARE AND HARDWARE SOLUTIONS

A. INTRODUCTION

The purpose of this chapter is to discuss the software and hardware tools that should be considered for use in assessing, monitoring and securing WLANs within the Marine Corps. We will consider open source shareware applications in addition to proprietary solutions. Both Windows and LINUX based software applications will be reviewed. These software tools will be evaluated on a wide assortment of criteria, ranging from cost and functionality to complexity and range of utility. The final result desired is the identification of a standard set of tools which, if adopted enable efficient and effective management of WLAN assets. This set of recommended tools will be presented in the form of an extremely capable toolkit which is designed to meet a diverse range of WLAN assessment requirements. Each tool will be evaluated in terms of the four critical attributes functionality, utility, complexity, and cost.

1. Functionality

The tool must possess critical and/or unique capabilities. These capabilities must be performed well and presented in manner that facilitates effective WLAN assessment. A robust functionality set will result in a tool receiving high scores under this criteria and more favorable overall assessment.

2. Utility

The tool must be able to perform a diverse range of tasks, therefore reducing the total number of tools needed for evaluating or monitoring WLANs. Tools that interface well with other applications or provide multiple useful products within a single product receive high scores under this criteria.

3. Complexity

The tool must present a user friendly interface that is relatively easy to use and is not inherently complicated. This tool would be appropriate for new WLAN administrators who would be overwhelmed by the complexity or technical use of the tool. Products with well organized and intuitive presentation styles will receive high scores under this criteria.

4. Cost

The tool must be a good financial investment. It should be provide significant “bang for the buck”. While each of the criteria is subjective, this category is not as straight forward as it may appear. Expensive tools can receive high scores as long as the tools represent strong value or good investments for the user. Conversely, cheap tools with limited functionality, poor utility, or excessive complexity could receive low scores under this criteria.

B. SOFTWARE/HARDWARE APPLICATIONS

1. Open Source Freeware or Shareware Applications

There are a plethora of tools that are available at no cost to the general public which were used at various stages of our research. Open source tools are unique in that their source code is made available to potential users for individual and unique modifications. Freeware applications are just as their name implies; made available to the public with only a recommendation to donate, but at no cost. These tools will be described in the below section.

a. *NetStumbler*

(1) Description. NetStumbler is a Windows based open source application for detecting WLANs. It was first made available to the public in 2001 and can be downloaded from the internet at <http://www.stumbler.net/>. NetStumbler was intended to be a relatively quick and simple tool that could be used for WLAN auditing,

WLAN coverage verification, site surveys, war driving, and antenna positioning. While its cost is very appealing, its capabilities are fairly limited to basic WLAN discovery. There is also a scaled down version of NetStumbler, known as MiniStumbler, which can be downloaded to and used in PDA's. Figure 27 provides a screen shot of the user interface for NetStumbler.

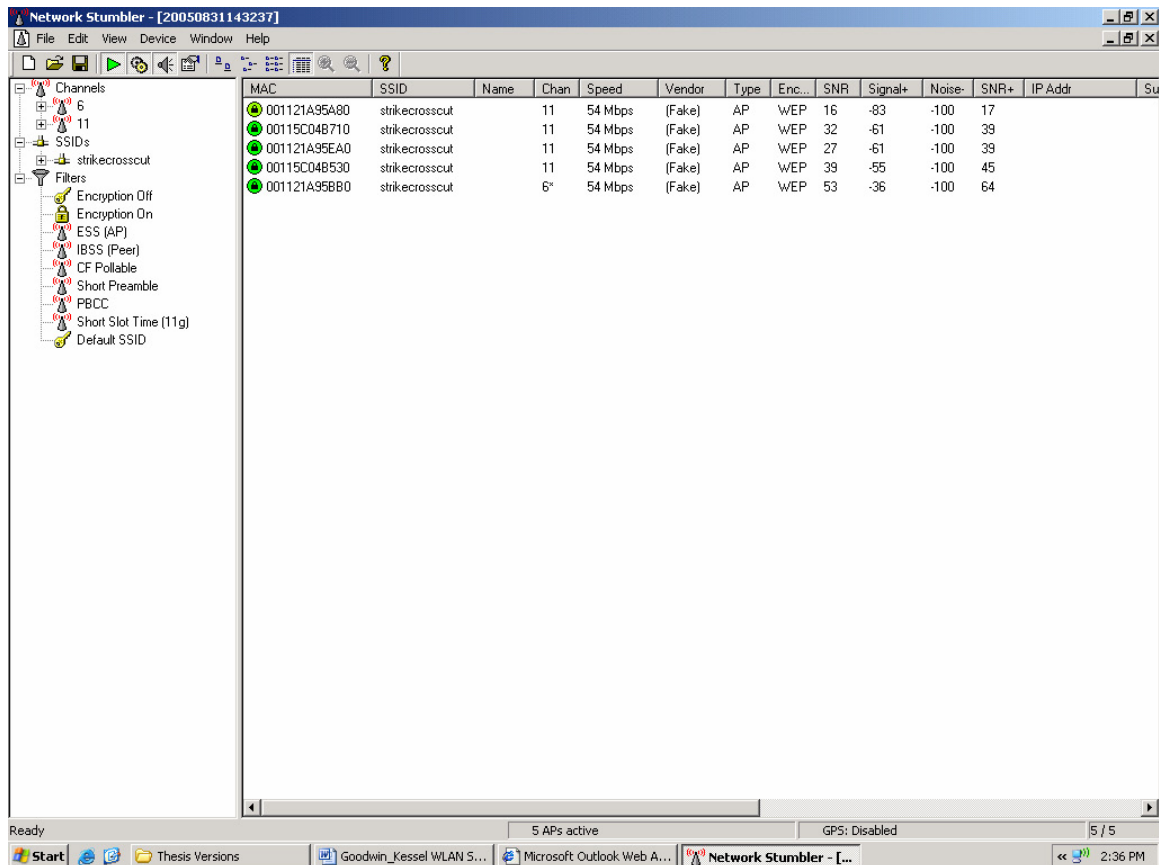


Figure 27. NetStumbler (From Ref. 53)

(2) Strengths. The primary strength of NetStumbler is the ability to conduct basic war driving with the use of the imbedded GPS feature. In addition, NetStumbler's relatively simple and user friendly interface is well suited for the detection of rogue access points.

(3) Weaknesses. The primary weakness of NetStumbler is its limited capabilities. In addition, it is not able to conduct any significant traffic analysis

⁵³ Shane Goodwin, Captain USMC, Naval Postgraduate School, NetStumbler Screen Shot, August 31, 2005.

(4) Summary. The functionality of NetStumbler is relatively weak since it is limited to identifying rogue AP's and WLANs and assessing signal strength. The overall utility of this software tool is closely related to its functionality. NetStumbler was not determined to have high utility since it does not perform a diverse range of tasks. In terms of complexity, NetStumbler is ideal for new users due to simple presentation of information. NetStumbler is freeware and so it receives high marks in the cost category.

b. Kismet

(1) Description. "Kismet is an 802.11 layer two wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of non-beaconing networks via data traffic"⁵⁴. Kismet is designed to work on a Linux based operating system although many free bootable CDs exist which allow a Windows system to boot into Linux with Kismet installed. These bootable CDs will be described in detail in the following sections. Kismet can be downloaded at the following website: <http://www.kismetwireless.net/code/kismet-2005-08-R1.tar.gz>.

Kismet has many features that are useful in different situations for monitoring wireless networks:

- Ethereal/Tcpdump compatible data logging
- Aircrack compatible weak-iv packet logging
- Network IP range detection
- Built-in channel hopping and multicard split channel hopping
- Hidden network SSID decloaking
- Graphical mapping of networks
- Client/Server architecture allows multiple clients to view a single

⁵⁴Kismet, *Documentation*, <http://www.kismetwireless.net/documentation.shtml>, Retrieved September 1, 2005.

Kismet server simultaneously

- Manufacturer and model identification of access points and clients
- Detection of known default access point configurations
- Runtime decoding of WEP packets for known networks
- Named pipe output for integration with other tools, such as a layer3 IDS like Snort
- Multiplexing of multiple simultaneous capture sources
- Distributed remote drone sniffing
- XML output
- Over 20 supported card types

Common applications Kismet is useful for:

- Wardriving: Mobile detection of wireless networks, logging and mapping of network location, WEP, etc.
- Site survey: Monitoring and graphing signal strength and location.
- Distributed IDS: Multiple Remote Drone sniffers distributed throughout an installation monitored by a single server, possibly combined with a layer3 IDS like Snort.
- Rogue AP Detection: Stationary or mobile sniffers to enforce site policy against rogue access points.

Figure 28 shows a screenshot of the main page when you open Kismet. The screenshot displays three different types of wireless networks.

- Two Encrypted Networks (SSID: 2WIRE521, 2WIRE514) using WEP
- One Hidden Encrypted Network (SSID: Zemfira) using WPA
- One unencrypted network with no SSID



Figure 28. Kismet main screenshot (From Ref. 55)

(2) Strengths. One of the primary advantages of Kismet is its ability to decloak hidden network SSIDs. In addition, it has a user-friendly, color-coded description of each SSID which helps to identify which APs are encrypted or unencrypted without drilling down into the actual network details. It also provides very useful details at the bottom of the screen which displays relevant status messages.

(3) Weaknesses. One major weakness is the fact that the majority of windows users do not have the ability to run Kismet on their computers. Also, the Graphical User Interface (GUI) is a bit clumsy and does not have point and click functionality. This requires the user to know the keys that represent commands in advance or at least know which key to press in order to find the help menu.

(4) Summary. Kismet is one of the most diverse and cost-effective WLAN analysis tools available. Its functionality as a scanner, sniffer, and IDS alone make it more diverse than most products. In terms of utility, Kismet is a very good choice to start with and with enough creativity and knowledge, it can be used as a

⁵⁵ Remote Exploit, *Research Kismet Primer Guide*, <http://new.remote-exploit.org/index.php/Research>, Retrieved September 1, 2005.

complete distributed IDS system including servers as well as mobile Kismet laptops or PDAs used for locating unauthorized clients or rogue access points. Finally, Kismet is unmatched in terms of price compared to functionality.

c. *Ethereal*

(1) Description. Ethereal is an open source network packet analyzer which can be used on either UNIX or Windows platforms. Ethereal was first released in 1998 and can be downloaded from the internet at <http://www.ethereal.com/>. It can be used to capture packet data from wired or wireless network interfaces. It enables users to import data from other packet capture tools or export Ethereal data to other programs. Ethereal also has some powerful search and filter options which enable detailed analysis of network traffic. Figure 29 shows a screen shot for the user interface Ethereal.

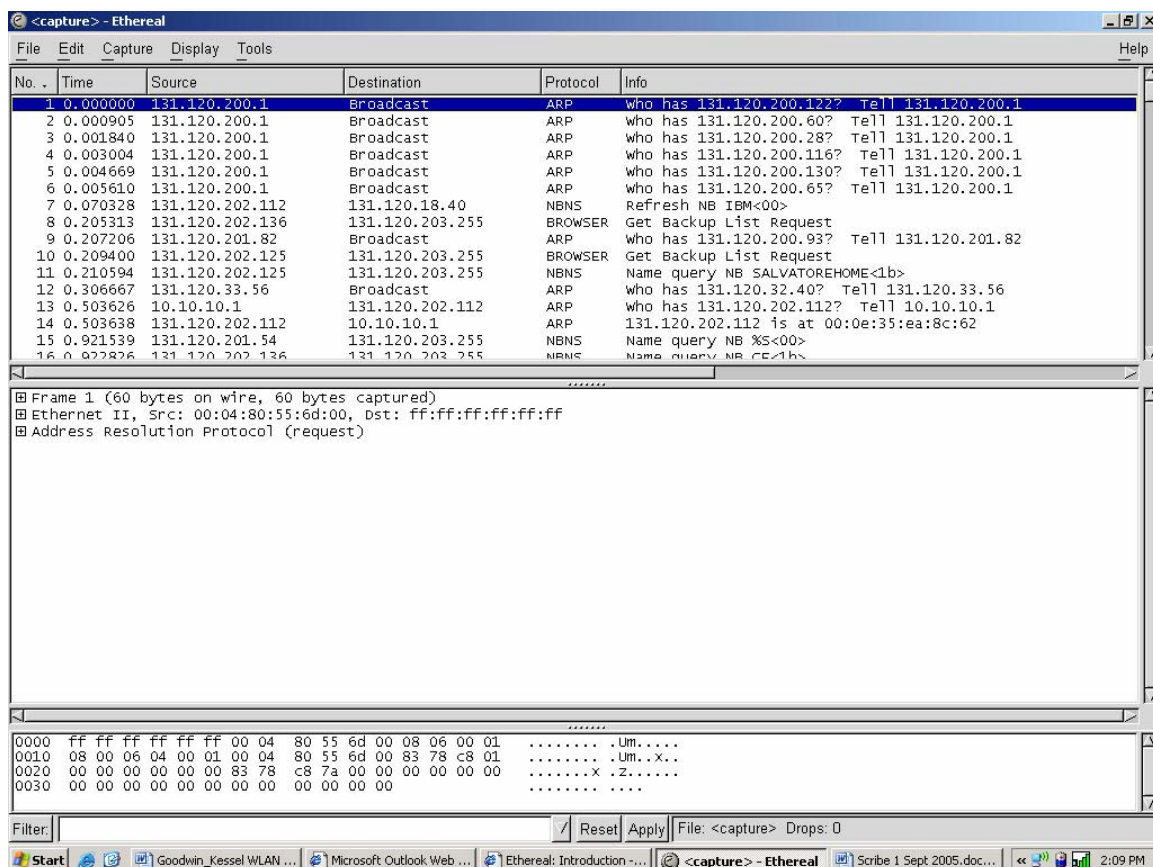


Figure 29. Ethereal (From Ref. 56)

⁵⁶ Shane Goodwin, Captain USMC, Naval Postgraduate School, Ethereal User Interface Screen Shot, September 1, 2005.

(2) Strengths. The primary strengths of Ethereal lie in its packet capture and filter capability and platform independence.

(3) Weaknesses. Ethereal has a rudimentary user interface which facilitates presentation of data via numerous searches and filters but provides no helpful analysis.

(4) Summary. The functionality of Ethereal is very solid with exceptional packet capture and filter capabilities. Ethereal also receives high marks in terms of utility due to its platform independence and its ability to be used on wired or wireless interface. Ethereal is not ideal for individuals new to network administration or traffic analysis and therefore received a poor complexity grade. As with the case of other freeware solutions, Ethereal's cost makes it an ideal candidate for government work.

e. Bootable CDs – (Auditor, Knoppix STD, PHLAK)

Bootable CDs are very useful because of the ability to load on any computer with a CD ROM. This means that if someone needed to use a network analysis tool that was only available on Linux and they are running the Windows operating system, it would be possible to load a version of Linux with the tool preinstalled. If the computer did not have a CD ROM there are currently software solutions that allow a user to convert a CD ISO image to a USB Flash bootable drive. An ISO image file is an image of a CD-ROM disk saved in ISO 9660 format. ISO image files are widely used to store CD content and transfer it through the Internet. ISO is a common CD image format for DOS, Windows (Joliet ISO extension), Linux (RockRidge ISO extension) and other operating systems. ISO images are generally duplicates of CDs rather than floppies or hard drives. Most popular CD recording programs can burn ISO images onto recordable CDs⁵⁷.

(1) Description. Auditor- The Auditor security collection is a Live-System based on KNOPPIX. With no installation whatsoever, the analysis platform is

⁵⁷Undisker, *Open, Create and Extract ISO files*, <http://www.undisker.com/creating-iso-images.html>, Retrieved September 2, 2005.

started directly from the CD-Rom and is fully accessible within minutes. Independent of the hardware in use, the Auditor security collection offers a standardized working environment, so that the build-up of know-how and remote support is made easier. Even during the planning and development stages, our target was to achieve an excellent user-friendliness combined with an optimal toolset. Professional open-source programs offer you a complete toolset to analyze your safety, byte for byte. In order to become quickly proficient within the Auditor security collection, the menu structure is supported by recognized phases of a security check. (Foot-printing, analysis, scanning, wireless, brute-forcing, cracking). By this means, you instinctively find the right tool for the appropriate task. In addition to the approx. 300 tools, the Auditor security collection contains further background information regarding the standard configuration and passwords, as well as word lists from many different areas and languages with approx. 64 million entries. Current productivity tools such as web browser, editors and graphic tools allow you to create or edit texts and pictures for reports, directly within the Auditor security platform. Many tools were adapted, newly developed or converted from other system platforms, in order to make as many current auditing tools available as possible on one CD-ROM. Tools like Wellenreiter and Kismet are equipped with automatic hardware identification, thus avoiding irritating and annoying configuration of the wireless cards. Listed below are the organized categories with only a few important tools displayed per category⁵⁸.

Footprinting

Whois

Traceroute

Nmap (Network scanner)

NmapFE (Graphical network scanner)

Scanning

Cisco global exploiter (Cisco scanner)

Nessus (Security Scanner)

Netmask (Requests netmask)

Nmap (Network scanner)

Scanning

Cisco global exploiter (Cisco scanner)

Analyzer

AIM-SNIFF (AIM sniffer)

⁵⁸Remote Exploit, *Auditor*, http://new.remote-exploit.org/index.php/Auditor_main, Retrieved September 2, 2005.

Nessus (Security Scanner)

Netmask (Requests netmask)

Nmap (Network scanner)

NmapFE (Graphical network scanner)

Unicornscan (Fast port scanner)

Protos (Protocol identification)

Mailsnarf (Mail sniffer)

URLsnarf (URL sniffer)

Etherape (Network monitor)

Ethereal (Network analyzer)

Ettercap (Sniffer/Interceptor/Logger)

Dsniff (Password sniffer)

Spoofing

Arpspoof (ARP spoofer)

Macof (ARP spoofer/generator)

Nemesis-Ethernet (Packet generator)

DNSSpoof (DNS spoofer)

Nemesis-DNS (DNS packet generator)

DHCPX (DHCP floodder)

Hping2 (Packet generator)

ICMPRedirect (ICMP packet generator)

Nemesis-IP (IP packet generator)

Wireless

apmode.sh (Act as accesspoint)

Hotspotter (Client penetration)

ASLeap (LEAP/PPTP cracker)

Void11-Hopper (Channel hopper)

Kismet (Ncurses wireless scanner)

Wellenreiter (GUI scanner)

aircrack (Modern WEP cracker)

Aireplay (Wireless packet injector)

Airsnort (GUI based WEP cracker)

Cowpatty (WPA PSK bruteforcer)

Bluetooth

Bluesnarfer (Bluesnarf attack)

Ghettotooth (Bluetooth scanner)

Kandy (Mobile phone tool)

Bruteforce

Guess-who (SSH bruteforc)

Obiwan III (HTTP bruteforce)

Figure 30 shows a screenshot of the Auditor Security Collection while running Shmoo Group's AirSnort tool which cracks WEP by passively capturing wireless transmissions.

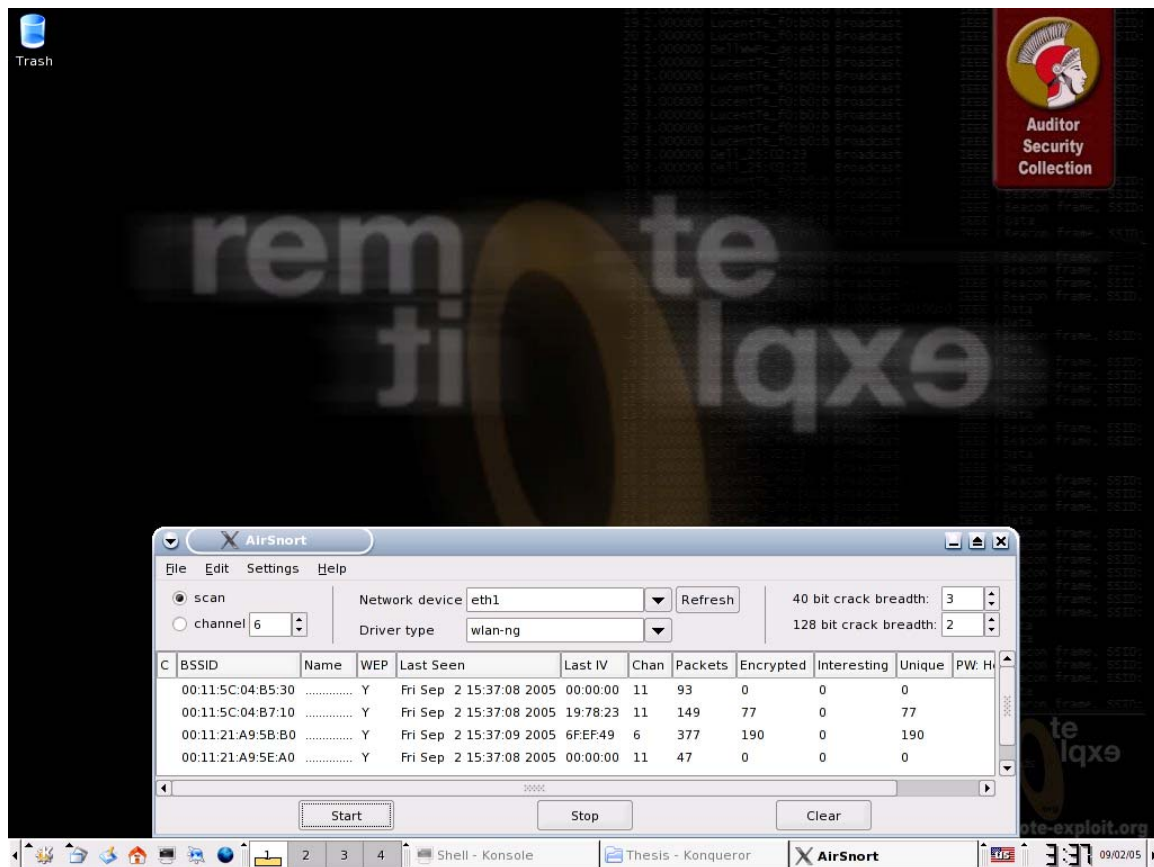


Figure 30. Auditor (From Ref. 59)

(2) Description. Knoppix STD- The Knoppix Security Tools Distribution is STD is a Linux-based Security Tool. Actually, it is a collection of hundreds if not thousands of open source security tools. It's a Live Linux Distro, which means it runs from a bootable CD in memory without changing the native operating system of the host computer. Its sole purpose in life is to put a great deal of security tools at your disposal with a savvy user interface. STD is meant to be used by both novice and professional security personnel but is not ideal for the Linux uninitiated. STD assumes you know the

⁵⁹ Adam K. Kessel, Captain USMC, Naval Postgraduate School, Auditor Security Collection, AirSnort screenshot, September 2, 2005.

basics of Linux as most of your work will be done from the command line. KNOPPIX is a bootable Live system on CD or DVD, consisting of a representative collection of GNU/Linux software, automatic hardware detection, and support for many graphics cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a productive Linux system for the desktop, educational CD, rescue system, or adapted and used as a platform for commercial software product demos⁶⁰.

Figure 31 shows a screenshot of KNOPPIX STD running a proprietary encryption algorithm called Megaencryption.



Figure 31. Knoppix (From Ref. 61)

(3) Description. PHLAK- PHLAK is a modular live security Linux distribution. PHLAK comes with two light gui's (fluxbox and XFCE4), many security tools, and a spiral notebook full of security documentation. PHLAK is a derivative of

⁶⁰Knoppix, *Knopper.net*, <http://www.knoppix.org>, Retrieved September 3, 2005.

⁶¹ Softpedia, *Knoppix STD 0.1*, Encryption screenshot, Retrieved September 3, 2005.

Morphix, created by Alex de Landgraaf⁶². Figure 32 displays the categories available for use with the PHLAK software suite.



Figure 32. PHLAK (From Ref. 63)

(4) Strengths. Auditor is by far the most useful and functional toolkit when it comes to network security combined with user-friendliness. It merges over 300 security tools with common utilities such as text and graphic editors which makes it the most complete and optimum choice of bootable network security CDs in this lineup. Auditor is based on the Knoppix bootable Live distribution so it has similar strengths such as very good hardware detection and a very organized assortment of menu options. Knoppix STD is very secure when booted and provides a secure workspace to use

⁶²PHLAK, *Professional Hacker's Linux Assault Kit*, <http://www.phlak.org/modules/news/>, Retrieved September 3, 2005.

⁶³ PHLAK, *Professional Hacker's Linux Assault Kit*, <http://www.phlak.org/modules/sections/>, Retrieved September 3, 2005.

without the need for additional tools. PHLAK currently includes two fast, light-weight window managers, from which the user has easy access to the documentation system. Currently included in the user interface are quick-start buttons to initiate services which helps Linux beginners who may not know many shell commands.

(5) Weaknesses. Auditor has a somewhat lengthy boot time and does not provide much in the way of documentation for the tools found on the CD. Knoppix STD does not provide many GUIs for its tools and most are command line tools. PHLAK's menu structure is very cumbersome and the tools are not organized in a logical manner. In addition, PHLAK has poor hardware support and detection.

(6) Summary. Auditor is recommended by the Authors due to its comprehensive network security solutions as well as its useful added utilities which make it closer to a normal operating system than any of the other bootable CDs reviewed. Although Knoppix STD comes in as a close second to Auditor, it does not provide many of the extra utilities that are useful in a normal operating system such as a screen capture tool. The builders of these security suites are often in competition with one another which is healthy in that they will add tools and functionality that may be found in the other distributions

2. Proprietary Commercial Software Applications

The number of proprietary or commercial tools which can assist in WLAN assessment and security is virtually endless. Throughout the conduct of our research we explored various commercial products for the purposes of evaluating their usefulness to Marine Corps WLAN assessment. We have selected five of the most common and useful tools for discussion below:

a. *AirMagnet*

(1) Description. AirMagnet is a Windows based software tool which can be used on a laptop or PDA to provide mobile WLAN analysis and management. It is intended to provide wireless intrusion detection, rogue access point detection, connection troubleshooting, trending, reporting, capacity planning, signal and

channel analysis and site survey preparation. Additional information regarding this WLAN tool can be found on <http://www.airmagnet.com/>. Figure 33 shows AirMagnet's description of alarms, which is one of the more useful screens within the application.

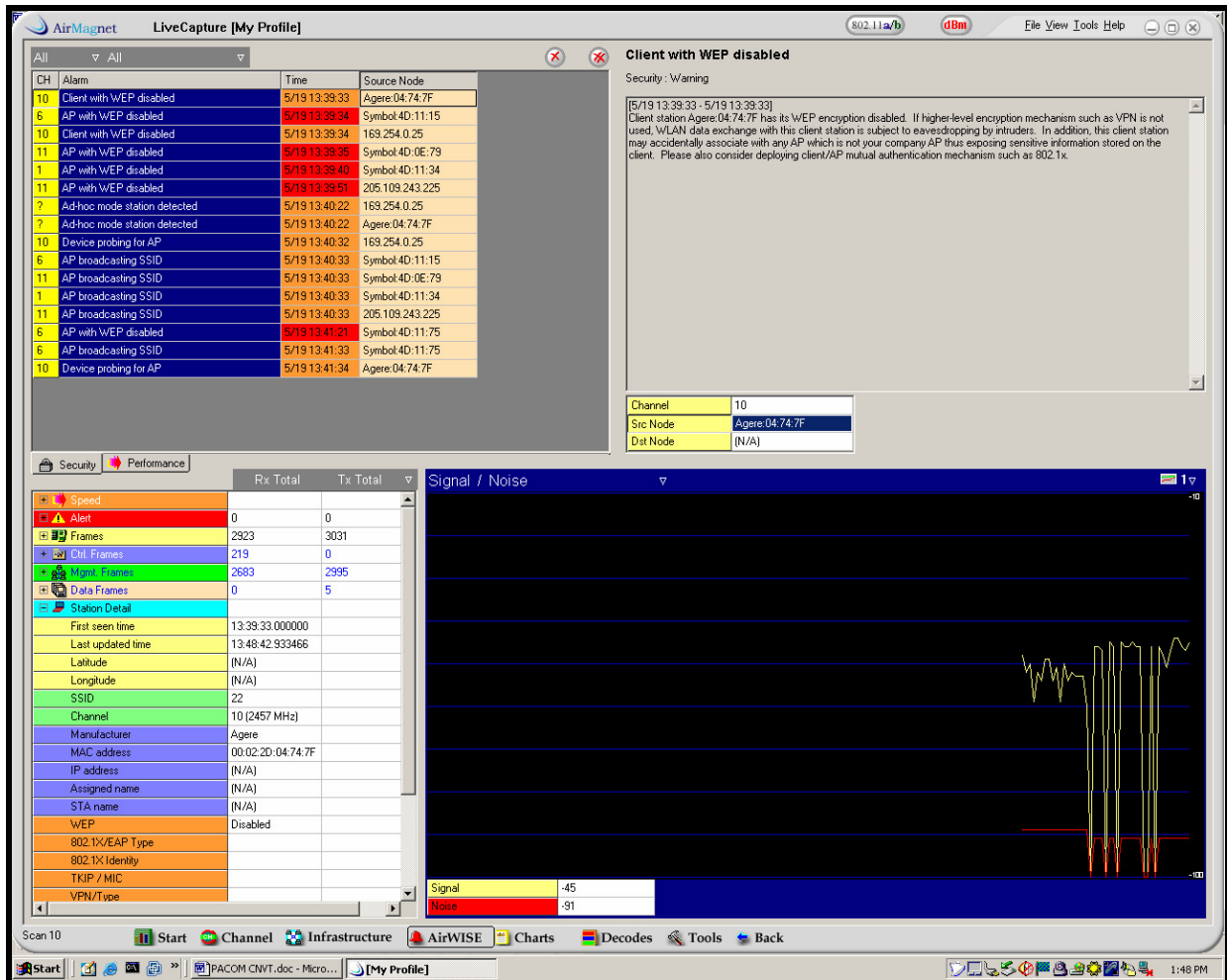


Figure 33. AirMagnet (From Ref. 64)

(2) Strengths. The strengths of AirMagnet are found in its diverse assortment of user interfaces which display a great deal of practical WLAN information. These dynamic graphical displays reveal WLAN data along with useful analysis on the same screen. It is ideal for new administrators who need to understand the “big picture” before they can delve into the WLAN details. It is also very useful for briefing or

⁶⁴ Shane Goodwin, Captain USMC, Naval Postgraduate School, AirMagnet Screen Shot, May 19, 2004.

communicating WLAN considerations and issues to non-technical individuals within your organization.

(3) Weaknesses. AirMagnet is not open source and so the source code is not able to be altered to meet individual organizational requirements. AirMagnet is not ideal for advanced WLAN vulnerability assessment. The cost of AirMagnet may be cost prohibitive for smaller organizations with minimal IT resources devoted to wireless networking.

(4) Summary. AirMagnet has a solid functionality set which leverages multiple useful and practical data views. It receives average grades in utility since its strength lies only in presentation of big picture oversight and assessment. In terms of complexity, AirMagnet's dependence on the graphical display of information results in excellent complexity scores, since even the most novice WLAN administrators will appreciate its simple user friendly presentation style. AirMagnet cost is only palatable for medium to large sized IT budgets.

b. AirDefense

(1) Description. AirDefense is yet another commercial Windows based program for WLAN assessment and monitoring and was designed to be a wireless intrusion detection system. It is available in Enterprise and Mobile versions to cater to various size organizations. The Enterprise version is server-based while AirDefense Mobile is Windows-based. AirDefense was designed to perform wireless network scans, device inventory, location tracking, and advanced rogue management. It will discover and identify all 802.11 devices and their transmissions within a given air space. Additional information regarding AirDefense can be found on the following website: <http://www.airdefense.net/>. Figure 34 is a screenshot from one of the many dashboard style displays within AirDefense.

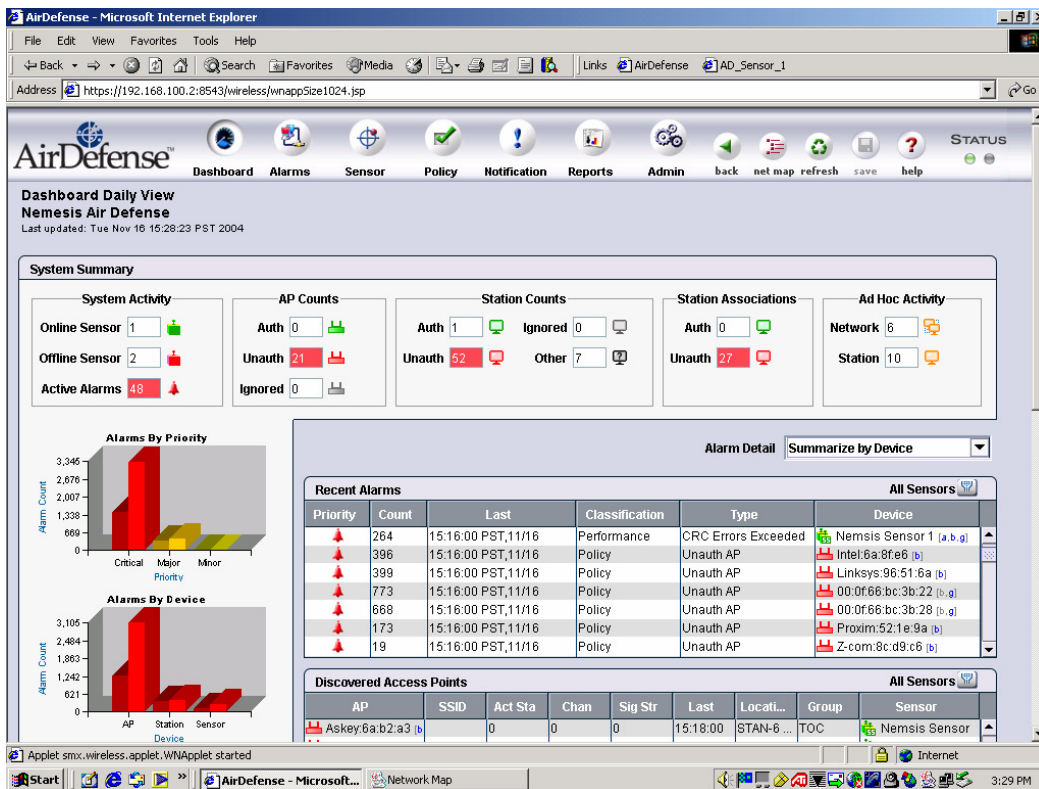


Figure 34. AirDefense (From Ref. 65)

(2) Strengths. Graphically designed interface is user friendly and well organized. Its strength lies in its ability to quickly scan the airspace for wireless activity to easily identify rogue access points.

(3) Weaknesses. Minimal traffic analysis capability compared to other software suites of its size and cost. AirDefense is not very flexible in terms of configuration to meet or research unique requirements.

(4) Summary. Functionality of AirDefense is adequate for basic WLAN administration. In terms of utility, AirDefense does not provide a diverse assortment of applications for advanced WLAN assessment. It does provide useful information which can be explored in further using other more in-depth tools. Lack of complexity is a significant advantage for AirDefense whose easy to use interface is well suited for basic WLAN administration. AirDefense is an expensive commercial off the shelf program which is certainly capable but not essential to WLAN assessment.

⁶⁵ Shane Goodwin, Captain USMC, Naval Postgraduate School, AirDefense Screen Shot, November 16, 2004.

c. *AiroPeek Nx*

(1) Description. Airopeek Nx is a Windows based expert WLAN analyzer. This software tool is designed to conduct site surveys, security audits, WLAN traffic analysis, and troubleshooting. In addition to fundamental packet analysis AiroPeek Nx provides advanced interpretations and diagnostics for WLAN traffic patterns. AiroPeek quickly isolates security problems, fully decodes all 802.11 WLAN protocols, and analyzes wireless network performance with accurate identification of signal strength, channel and other network statistics. Additional information about AiroPeek and other WildPackets products can be found at the following website: http://www.wildpackets.com/products/airopeek/airopeek_nx/overview/. As shown in Figure 35 below, WLAN information is presented in very methodical manner with the ability to drill down on specific items showing more and more descriptions and analysis.

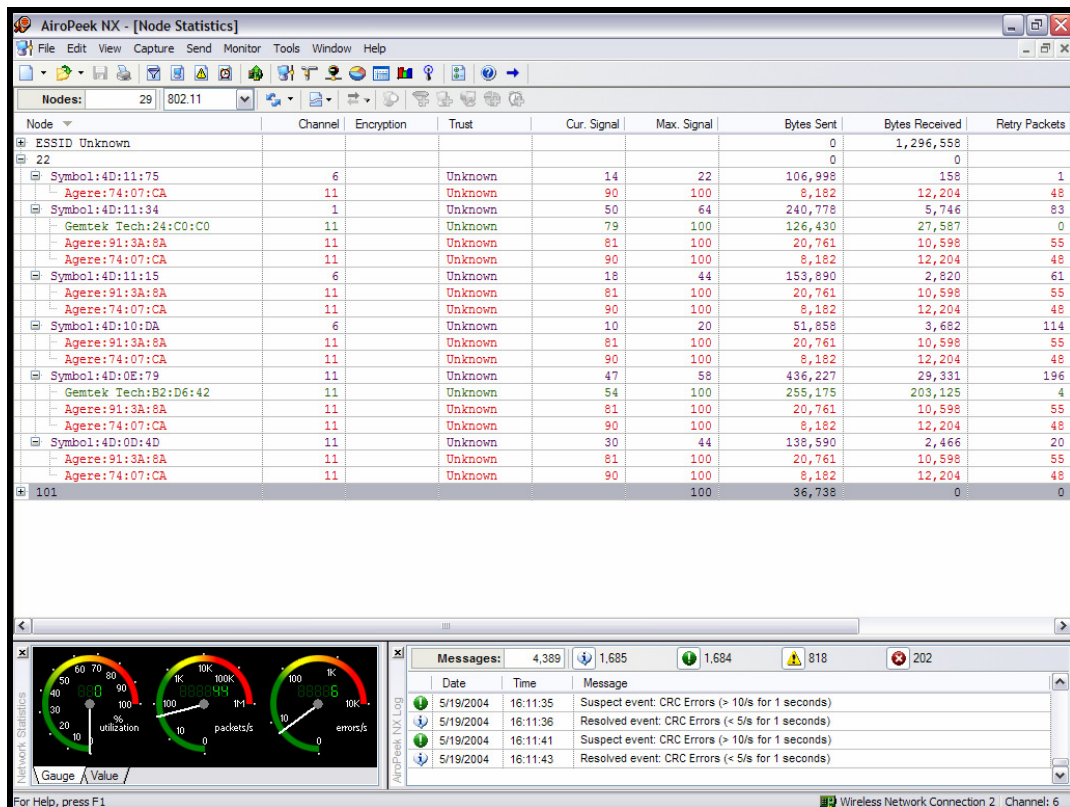


Figure 35. AiroPeek (From Ref. 66)

⁶⁶ Shane Goodwin, Captain USMC, Naval Postgraduate School, AiroPeek Screen Shot, May 19, 2004.

(2) Strengths. AiroPeek Nx has numerous strengths which make it an ideal candidate for advanced WLAN assessment. AiroPeek provides intuitive user interface with critical information for WLAN problem resolution on each screen. It possesses many useful tools like a network peer map which enable users to quickly understand nodes operating in the WLAN and their traffic patterns.

(3) Weaknesses. The only weakness we could identify in Airopeek Nx was that it is designed for advanced or expert users. However, Wildpackets does offer AiroPeek SE , which is a slightly scaled down and more basic version.

(4) Summary. The functionality found within Airopeek is extremely strong and useful. It quickly became our tool of choice for conducting WLAN assessments because of its ability to facilitate advanced WLAN analysis. In terms of utility, AiroPeek received high marks for its peer node map and WLAN problem finder. Both of these capabilities could not be matched in comparable products we evaluated. Airopeek's user interface is not excessively complex but clearly is not designed for beginners. The cost of AiroPeek was comparable to other Windows based WLAN analyzers, but with more robust functionality it is worth the investment.

d. Cognio ISMS

(1) Description. The Cognio Intelligent Spectrum Management System (ISMS) solution provides RF spectrum analysis for troubleshooting and optimizing WLANs as well as The Mobile's Device Finder feature which is similar to an RF device "Geiger Counter" which makes it easy to locate troublesome or unauthorized devices, including rogue access points. Using patented spectral analysis and fingerprinting techniques, the Cognio ISMS Mobile measures, analyzes, and displays critical spectrum data and logs interference events in real-time⁶⁷. In addition, the Cognio ISMS provides real-time device detection and device identification by analyzing all RF activity and instantly detecting and identifying RF emitting devices using WiFi bands. Cognio's ISMS is one of the only solutions on the market that actually identifies the interfering device, greatly simplifying troubleshooting. Figure 36 shows two interfering

⁶⁷Cognio, *ISMS Mobile Datasheet*, http://www.cognio.com/solutions_mobile.html, Retrieved September 1, 2005.

devices as well as a settings screen that allows the user to pick specific frequency bands to monitor.

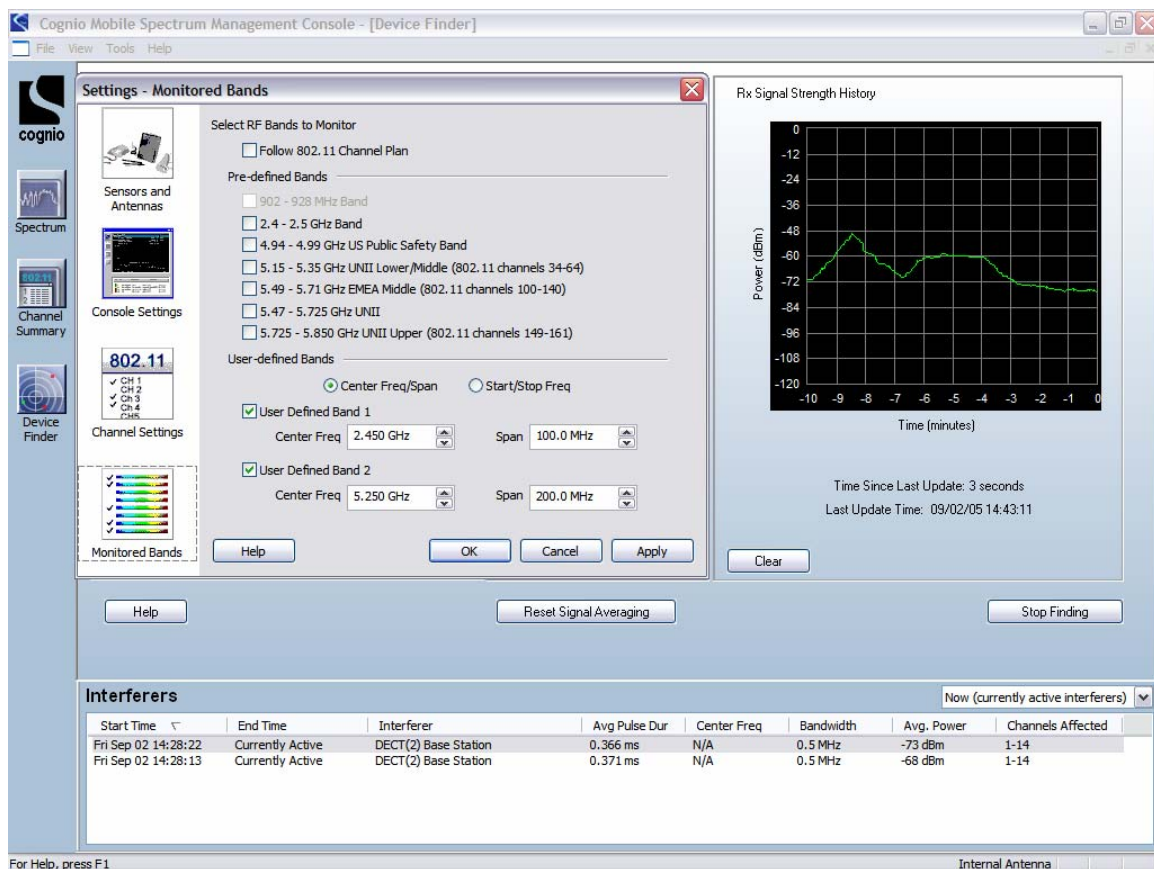


Figure 36. Cognio (From Ref. 68)

Figure 37 shows what kind of device was interfering with the 802.11 network in the 2.4 GHz frequency band which helps to locate the device itself.

⁶⁸ Adam K. Kessel, Captain USMC, Naval Postgraduate School, Cognio ISMS Device Finder screenshot, September 2, 2005.

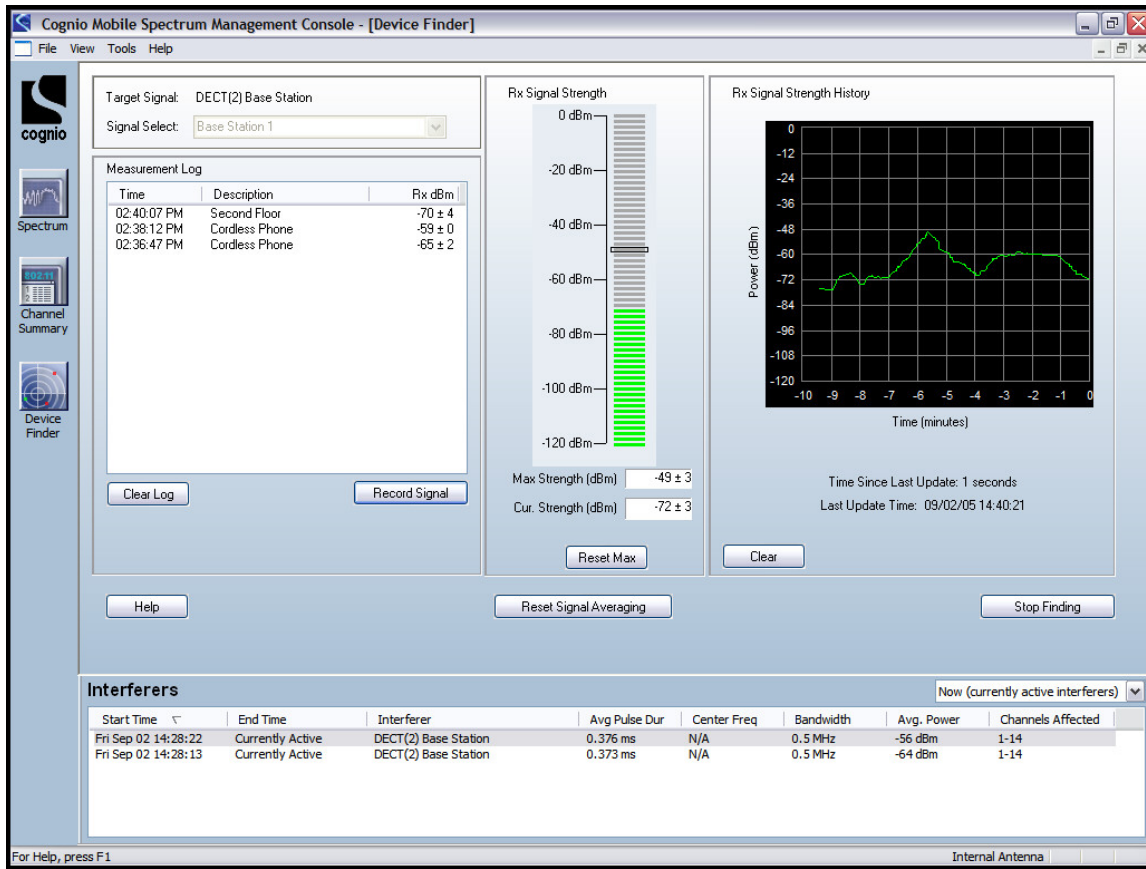


Figure 37. Cognio (From Ref. 69)

(2) Strengths. The Cognio ISMS is unlike other systems, which monitor only 802.11 packet flow, the Cognio ISMS monitors all activity in the RF spectrum, fully replacing a spectrum analyzer. Compared to other similar solutions the Cognio solution is extremely affordable at approximately \$3,600. An average spectrum analyzer can cost up to \$35,000 and does not even provide the other features found in this device.

(3) Weaknesses. One weakness that affects many proprietary solutions is the fact that it is very difficult to modify the software in order to suit the needs of the user. Another minor weakness that can be said of any new solution is that it is relatively unproven on the market.

(4) Summary. Overall, the Cognio ISMS provides excellent functionality with spectral analysis as well as the unparalleled diversity included in one

⁶⁹ Adam K. Kessel, Captain USMC, Naval Postgraduate School, Cognio ISMS Device Finder, September 2, 2005.

package. In addition, the ability to use the card in any device with a PCMCIA slot provides a very unique utility that allows any user to employ this solution without the need for special equipment.

e. YellowJacket

(1) Description. Yellowjacket is one of many wireless assessment tools created by Berkeley Varitronics Systems. Yellowjacket is a handheld 802.11b wireless receiver which can be used to sweep and analyze WLANs. It is able to identify SSIDs, locate access points, measure signal strength and signal-to-noise ratio, and report channel usage. Additional information about Yellowjacket can be found at the following website: <http://www.bvsystems.com/Products/WLAN/Yellowjacket/yellowjacket.htm/>. Figure 38 shows the Yellowjacket suite which is composed of the BVS receiver and PDA with Yellowjacket software.



Figure 38. Yellowjacket (From Ref. 70)

(2) Strengths. The strengths of the Yellowjacket suite clearly lie in its portable handheld design coupled with its ability to physically locate rogue APs.

⁷⁰ Berkeley Varitronics Systems, *Yellowjacket*, <http://www.bvsystems.com/Products/WLAN/YJ802.11bg/YJ802.11bg.htm>, Retrieved July 29, 2005.

(3) Weaknesses. The Yellowjacket software and hardware components are both extremely difficult to keep operational. The suite requires constant operational checks and is difficult to rely upon for consistent WLAN assessment. Also, Yellowjacket cannot be considered a complete WLAN analysis tool because it does not provide any Bluetooth analysis capability although another BVS tool names Mantis, does provide this capability.

(4) Summary. In terms of functionality, Yellowjacket is able to provide basic WLAN assessment information (SSID, MAC address, WEP, signal strength, channel usage, etc) in uniquely portable design. However, Yellowjacket is not able to perform a diverse range of WLAN tasks, in fact, just the opposite is true. Yellowjacket is not excessively complex, however keeping the ultra portable system up and running requires a technical genius. The cost of Yellowjacket Suite is significant considering its operational inconsistency.

C. EVALUATION CHART

Table 1 was used to evaluate the various software and hardware tools that were used to conduct our WLAN security and assessment research. As discussed previously, we used the acronym FUCC to represent the critical aspects of each tool that we wanted to evaluate; Functionality, Utility, Complexity, and Cost. Each of these criteria was rated below in Table 1 from one to ten for each WLAN tool with the resultant overall grade shown in the far right hand column. Higher scores are indicative of a more favorable evaluation. Poor performance in any criteria would be reflected with scores ranging from one to two. Below average performance would be indicated by scores ranging from three to four. An average performance in any criteria received a grade of five. Above average performance would be reflected with a scores ranging from six to seven, while excellent performance would be indicated with scores ranging from eight to ten. For example, a tool that had great functionality and range of utility coupled with a low level of complexity and excellent “bang for the buck” would receive grades of eight to ten in every criterion. High complexity from rudimentary user interfaces and overly technical presentation information were penalized with low scores. Finally high cost was not penalized if it made up for the cost by providing outstanding functionality with added utility as long as it could still be deemed a good value investment.

Software Solution	Functionality		Utility		Complexity		Cost		Evaluation Score	
NetStumbler	4		4		10		7		25	
Kismet	7		7		8		9		31	
Ethereal	7		6		5		8		26	
Bootable CD's										
PHLAK	5		4		4		7		20	
Knoppix	7		7		8		8		30	
Auditor	8		8		9		9		34	
AirMagnet	7		6		9		6		28	
AirDefense	7		6		9		6		28	
AiroPeek	9		9		6		9		33	
Cognio	8		8		9		6		31	
YellowJacket	7		8		4		6		25	
Poor	Below Average		Average		Above Average		Excellent			
1	2	3	4	5	6	7	8	9	10	

Table 1. Evaluation of Software / Hardware Applications

D. SUMMARY

During the course of this chapter we have discussed various tools which can be used to assess and monitor WLANs. Let's conclude our discussion by framing these tools in terms of the needs of a particular organization. Each organization with WLAN assets needs to have tools which provide basic packet sniffing and WLAN analysis, intrusion detection, and finally some sort of vulnerability self-assessment capability.

Each organization with wireless network will need to conduct wireless packet sniffing and basic WLAN analysis. We have introduced numerous tools which could be used to accomplish these tasks. Smaller organizations might consider using MiniStumbler or NetStumbler as a basic mobile WLAN packet sniffer. Although, Ethereal and Kismet are more desirable options from the standpoint of additional functionality. However, that additional functionality requires a slightly higher degree of technical WLAN experience and competence. Each of these software tools is free to the public which makes them ideal candidates for smaller organization with limited IT resources. Medium sized organizations with a few extra IT resources might consider using Yellowjacket as a mobile WLAN analyzer to locate rogue APs and conduct intermediate wireless traffic analysis. However, what medium sized organization really require is a tool like AirMagnet which provides some advanced WLAN assessment along with rogue AP identification and traffic analysis. Large organizations with mature WLAN implementations and advanced WLAN administrators need to use a product like Cognio or AiroPeek Nx. These tools are comparable and would properly equip network administrators with the requisite troubleshooting, monitoring and expert analysis applications for keeping their organization's WLAN functional and secure.

One important tool for any wireless implementation is some form of Wireless Intrusion Detection System (WIDS) functionality. Most businesses and military organizations agree that a WIDS is necessary regardless of whether WLANs exist on the organization's network in order to detect unauthorized wireless access and rogue access points. Two of the tools evaluated in this chapter worth mentioning that have WIDS functionality are Kismet and Air Defense. While Kismet can detect many of the top attack methods used on a wireless network, and a few not so common, Kismet goes one step further and can actually be used as a distributed WIDS system. By setting up a kismet drone, and pointing it to a central server, you can easily setup an enterprise wide WIDS that rivals solutions with a much higher price tag. AirDefense has a much higher price tag and requires the purchase of other hardware and software. Of course AirDefense offers more functionality and support from the company. Kismet would be recommended for a small to medium size organization while AirDefense would be recommended for larger organization looking for a more robust and supportable solution.

Assessing the wired and wireless vulnerabilities of a local area network internally is essential in determining network security and health. The vulnerability assessment tool of choice recommended by these Authors is the Auditor Security Collection bootable CD. This tool can be downloaded for free and used by any size organization in order to assess network vulnerabilities. This capability is necessary for organizations to replicate potential attackers and practice Information Assurance professional's response to them. Just as a military unit replicates its enemies in order to structure an appropriate response and must train to fight effectively, a network administrator or CTO must ensure they are prepared for the threats posed to organizations today.

VII. STANDARD PROCEDURES FOR DETECTING, ASSESSING AND SECURING WLANS

A. INTRODUCTION

One of the practical outputs that we wanted to achieve within the context of our thesis was the identification of a standard set of tools and procedures to conduct vulnerability assessments within the Marine Corps. This chapter builds on the previous introduction and evaluation of software solutions by coupling these tools together with the requisite step by step procedures to assess WLANS. We have selected several of the previously identified tools which we believe provides the most functionality, greatest utility, least amount of complexity, and represents the best value for conducting vulnerability assessment within the Marine Corps.

B. COORDINATING A WIRELESS VULNERABILITY ASSESSMENT

The first step in conducting a vulnerability assessment is to first determine what kind of advance coordination is required. For the vast majority of the scenarios, that question is answered by whether the assessment is aimed at evaluating internal or external assets.

1. Internal Assessment

An internal assessment represents a proactive attempt to conduct a self-evaluation. Internal assessments are valuable tools for many reasons. First and most importantly, they are a means to identify potential problem areas early, before they create actual vulnerabilities or before the vulnerabilities can be exploited by another party. Second, an audit of potential weaknesses or vulnerabilities is required to be conducted on an annual basis by Marine Corps Order 5200.24CW. The Internal Management Control Program (IMCP) states that “Commanders/managers are responsible for ensuring that resources under their purview are used efficiently and effectively, and that programs and operations are discharged with integrity and in compliance with applicable laws and regulations.” The IMCP program applies to all resources or programs not just those related to information or communication security. Finally, an internal assessment is

important because it reduces the likelihood that an external audit or evaluation will find significant vulnerabilities which could lead to negative attention to your command.

2. External Assessment

Assessment of external WLAN assets will generally come in two different scenarios. The first type of external assessment is the traditional audit which is conducted by a completely external agency. Evaluations conducted by the DOD Inspector General or Naval Audit Service would fall under this category. The second scenario for external assessments is when you are evaluating a subordinate unit which has its own command structure and operates independent of your organization. An assessment of Division assets by MEF personnel or evaluation of an installation by the appropriate Marine Forces Commander would both fall under this category. These assessments obviously require additional attention due to inherent sensitivities that are encountered when evaluating external programs and resources.

C. CONDUCTING A WIRELESS VULNERABILITY ASSESSMENT

This focus of this thesis is primarily on WLAN security issues and addressing methods to mitigate vulnerabilities and it is beyond the scope of this thesis to expound on every detail of network security. There are vast technical considerations involved in conducting a complete network security assessment. Outside of what is explained below regarding wireless vulnerability assessments, a complete network security assessment would involve initiating threat assessments, risk assessments, penetration assessments, application assessments and system security audits to name a few.

Vulnerability assessments focus on identifying weaknesses in a system that has the potential to be exploited by a threat. One important point to note is that not all vulnerabilities are “technical” in nature. For example, the lack of a solid security policy is a high-risk vulnerability that may or may not be obvious from the perspective of a technical vulnerability assessment. In this same manner, the fact that WPA is being used to encrypt wireless traffic does not completely address the overall security of the wireless network if the Pre-Shared Key is published on the organization’s website.

1. Formal Notification of Command

Formal notification of command is typically accomplished with a standard naval message from the Commanding Officer of the reviewing agency to the Commanding Officer of the organization to be evaluated. This message should possess all the formal requirements of the assessment to include the date, agenda, specific access requirements, and points of contact, in addition to any assistance or participation you will need from the organization. As with any other type of assessment, coordination for a WLAN assessment should begin well in advance of formal notification. This advance coordination is critical to communicate expectations and requirements from both sides of the assessment. Formal notification should be made a minimum of thirty to forty-five days in advance of the assessment.

2. In-brief

Assessing an external agency's WLAN almost always requires an in-brief with the organization to be evaluated. This in-brief can range from a formal presentation to just an introduction followed by informal discussion about the conduct of the WLAN assessment. The requirements of the assessment not to mention the personalities of the organizations involved will drive the formality or informality of the in-brief. Based on experience, the best question to ask the command you are visiting prior to the assessment is, do you have any wireless? Depending on the response, you know how extensive your search will have to be. When the answer to the question is a flat out no, the situation is one of two possibilities. Either the IT and/or IA staff is really on top of the wireless security state of affairs or they assume there is none because it has not yet been authorized. When the answer is yes, generally the installation has a decent grasp on what they are up against and are in need of a few pointers and/or some tools to assist them in securing their wireless circumstances.

3. Assessment

Before the actual conduct of the assessment takes place, an assessment team should have in their position an official message or letter from the specific command stating at a minimum where the assessment should be taking place, the names of the individuals on the assessment team and what authority is given to the them, what level of disclosure is permitted, and who to contact when assessment team presence and authority must be verified.

a. Wardriving

The SANS Institute (SysAdmin, Audit, Network, Security) defines Wardriving as the process of traveling around looking for wireless access point signals that can be used to get network access. Wardriving was named after Wardialing because it also involves searching for accessible computer systems. Wardriving can be used as a tool for Computer Network Defense (CND) or it can be categorized as a threat against a WLAN. This research will describe the former and how Wardriving should be a part of a sound network security approach regardless of the presence of any official or authorized WLANs.

(1) Hardware/Software Selection. The essential requirements for Wardriving include a laptop or PDA, a wireless card, and some type of scanning software. Of course to cover a wider area and to track noteworthy locations an external antenna, amplifier and a GPS device would be needed.

When choosing what type of laptop or PDA to use while Wardriving, one must keep in mind power requirements for different devices as well as what software will run on the various devices. Generally, most available programs will run on a Linux laptop while a Windows-based laptop will run some programs or will provide the ability to run CD bootable programs that are mostly Linux-based. MAC operating systems have a few options for Wardriving but are extremely limited. Finally, a PDA may provide more mobility, concealment, and battery life when compared to a laptop although the software that will run on most PDA's is very limited.

The next necessary component is the wireless card. The two most significant factors when choosing a wireless card are which chipset the card runs on and whether or not the card has an external antenna connector. Chipset must be known because of the various software requirements and which chipsets the software will support. Three of the most frequently used chipsets are Hermes, Prism, and Aironet. Without the ability to connect an external antenna, a Wardriver is very limited in the distance that he/she can cover without being within 50-100 feet of every point in which the Wardriving is taking place. Most Hermes based chipsets provide external antenna connectors on their wireless cards.

As mentioned previously, an external antenna is not required but anything used to extend the range of a wireless card allows a Wardriver to detect more wireless access points with less distance covered. When choosing an external antenna, one must ensure it operates on the same frequency as the potential wireless networks. If the antenna works in the 2.4Ghz (802.11b/g) or 5.8Ghz (802.11a) spectrum it will be able to acquire the signal of most WLANs with the majority being in the 2.4Ghz spectrum. In addition, a Wardriver must decide whether to use an omni-directional or directional antenna. Omni-directional antennas are mostly used because of their ability to cover a wide area as opposed to the directional antennas which direct the wireless reception into one specific direction.

The use of an amplifier may be required to sniff remote areas from a stand-off distance. Most antennas will provide the extra power levels needed to cover significant distances beyond what a wireless card alone could cover. Having said that, many wardrivers still choose to use amplifiers to cover even further distances without regard for the FCC power limit of 1 Watt.

It is useful to simply produce data on wireless access points operating in a given area but especially for larger areas, it becomes necessary to map out where the signals are picked up in regard to established maps. GPS devices with either serial or USB connections work with the majority of scanning programs as long as they are capable of NMEA output. Very inexpensive GPS units are available for strictly

Wardriving purposes with no added functionality other than providing coordinates from GPS satellites.

There are many options for scanning software ranging from very expensive to free but only a few of these programs will be described based on ease of use and functionality. Both Netstumbler (Windows-based) and Kismet (Linux-based) were evaluated in the previous chapter but due to the simplicity and limited functionality of Netstumbler, Kismet will be described in detail as a wireless scanner of choice.

(2) Kismet Scanning. As mentioned in the previous chapter, Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system. Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and can sniff 802.11b, 802.11a, and 802.11g traffic. Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic⁷¹.

Figure 39 shows a screenshot of Kismet with 4 wireless APs detected with varying levels of encryption including two encrypted networks (SSID: 2WIRE521, 2WIRE514) using WEP, one hidden encrypted network (SSID: Zemfira) using WPA, and one unencrypted network with no SSID.

⁷¹Kismet, *Documentation*, <http://www.kismetwireless.net/documentation.shtml>, Retrieved September 1, 2005.



Figure 39. Kismet main menu screenshot (From Ref. 72)

Using Figure 39 as a reference from left to right the Kismet basic interface consists of:

- **Name** : SSID of network
- **T** : Type of network
- **W** : Identifies if network is secured or not
- **Ch** : Channel on which the Access Point is on
- **Packts** : Number of packets captured
- **Flags** : Method in which IP was gathered (ex. A4 means IP was learned through ARP packet)
- **IP Range** : IP of the network
- **Size** : Total size of packets gathered from the Access Point

Identifying Security

Secured networks are always shown in green and the **W** column shows either **Y (Yes)** for WEP or **O (Other)** if any another type of security is used such as WPA/TKIP/LEAP/EAP/TLS. When you see an **O** in the **W** column select the network and press the **I (Network Information)** key and scroll down to the **Encrypt** : field and the specific type of security used is listed.

⁷² Remote Exploit, *Research Kismet Primer Guide*, <http://new.remote-exploit.org/index.php/Research>, Retrieved September 1, 2005.

Color Coding

Kismet colors the networks listed to make it easier to identify its configuration. The following are the possible color combinations:

- **Yellow** : Unencrypted network
- **Red** : Networks this color are still using factory defaults
- **Green** : This identifies secured networks using either WPA, WEP, or another form of security
- **Blue** : These are hidden networks which can either be open or encrypted so check the **W** column

Network Type

The **T (Type)** column can list six possible wireless network types.

- **A (Access Point)** - normal wireless access point
- **H (Ad-Hoc)** - ad-hoc point-to-point wireless network
- **P (Probe request)** - A wireless client that is not associated but is searching for a network
- **D (Data)** - Data network
- **T (TurboCell)** - TurboCell network
- **G (Group)** - Group of wireless networks

Command Reference

- **e** - Open popup window of Kismet servers. This lets you simultaneously monitor two or more Kismet servers on different hosts.
- **z** - Zoom network display panel to full screen (or return it to normal size if it is already zoomed)
- **m** - Mute sound and speech if they are enabled (or unmute them if they were previously silenced). You must have sound or speech enabled in your config to be able to mute or unmute them.
- **t** - Tag (or untag) the current network
- **g** - Group currently tagged networks
- **u** - Ungroup current group
- **c** - Open client popup window to display clients in the selected network
- **n** - Rename selected network or group
- **i** - Display detailed information about the current network or group
- **s** - Sort the network list differently
- **l** - Show signal/power/noise levels if the card reports them
- **d** - Instruct the server to start extracting printable strings from the packet stream and display them.
- **r** - Display bar graph of the packet rate.
- **a** - Show statistics about packet counts and channel allocation.
- **p** - Display packet types as they are recieved.
- **f** - Follow the estimated center of a network and display a compass
- **w** - Display all previous alerts and warnings.

(3) Procedures. The Joint Wireless Administrator Checklist⁷³ (JWAC) recommends mapping wireless signal strength quarterly and tracking authorized wireless devices as required. This process will help to determine what wireless networks are in the area of operations and if there are unauthorized wireless networks plugged into a network of interest.

A typical setup for Wardriving would be with the laptop on the passenger side seat or with two people, the passenger is in control of the laptop while the other drives. The GPS unit is placed on the dashboard while the external antenna is magnetically mounted to the roof of the vehicle. Most strategies for covering a specific area are sufficient but if you know what average distance your antenna covers you can organize how the route will be taken in order to maximize coverage and minimize driving time.

Many mapping programs exist that can convert wireless scanning data into points on a map. A Linux program called gpsmap which is meant to work with Kismet is a useful solution that can be used to plot where APs were seen. Using a Kismet GPS file, gpsmap will download a map from Expedia, Mapblast, or Terraserver and plot the wireless access points. Gpsmap also allows you to visualize the route taken during the wardriving session. Figure 40 shows a sample Gpsmap screenshot with multiple wireless networks present.

⁷³Joint Wireless Administrator Checklist, Version 1.0, <http://iase.disa.mil>, Retrieved August 22, 2005.

effectively to locate devices although Yellowjacket is more effective at finding access points while the Cognio solution is more adept at locating devices that interfere with the WLAN signal.

The most successful technique used for locating devices was with the assistance of a directional antenna combined with Yellowjacket and then isolating the MAC address of the given AP. Once that is done, it is useful to switch to a small, low powered omni-directional antenna to minimize the total number of signals that may interfere with the physical locating of the AP. The Cognio device was helpful in determining if a microwave or cordless telephone for instance in the 2.4GHz frequency spectrum was interfering with the wireless network's signal. This is particularly useful when attempting to locate an AP and the signal suddenly drops very low or completely out of range. This can cause an inexperienced user to either change directions or deceive the user into thinking that the device is somewhere much further away from their current position. When locating devices it is important to take into account what type of materials are nearby such as cement walls or lead objects and what devices may be operating in the same frequency that may cause the signal to decrease even though the AP could be within 10 feet. Finally, once the wireless network has been located, it must be determined whether or not it is authorized to be operating.

c. Access Point/Wireless Card Exploitation

The next step is to ensure that WLAN transmissions do not pose a threat to the Marine Corps Enterprise Network (MCEN). A few questions that must be answered for example are: Is the AP connected to the MCEN? Is the AP configured according to Marine Corps Policy and overarching DoD policy? Is a wireless card in a computer vulnerable to allowing unauthorized Ad-hoc connections to the network?

Once these types of questions have been answered, it is most useful to test the AP and/or wireless client for vulnerabilities. Some examples to begin with would be to check if MAC filtering is being used. If it is, check to see if a spoofed MAC of an authorized client can access the network. Next, check to see if encryption is enabled, and if it is disabled, check if it is possible for a client to associate to the WLAN. If

encryption is enabled, attempt to crack it with known WEP or WPA cracking programs. As a guide, the checklist below can be used by an internal or external assessment team to either exploit and/or ensure security within a given WLAN.

The following Figure 41, Wireless LAN Security Checklist, from the NIST Special Publication 800-48, provides users and implementers with detailed management, technical, and operational recommendations that should be addressed as a part of any WLAN implementation or vulnerability assessment.

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
Management Recommendations				
1.	Develop an agency security policy that addresses the use of wireless technology, including 802.11.	✓		
2.	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology.	✓		
3.	Perform a risk assessment to understand the value of the assets in the agency that need protection.	✓		
4.	Ensure that the client NIC and access point support firmware upgrade so that security patches may be deployed as they become available (prior to purchase).	✓		
5.	Perform comprehensive security assessments at regular and random intervals (including validating that rogue access points do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.	✓		
6.	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	✓		
7.	Deploy physical access controls to the building and other secure areas (e.g., photo ID, card badge readers).	✓		
8.	Complete a site survey to measure and establish the access point coverage for the agency.	✓		
9.	Take a complete inventory of all access points and 802.11 wireless devices.	✓		
10.	Ensure that wireless networks are not used until they comply with the agency's security policy.	✓		
11.	Locate access points on the interior of buildings instead of near exterior walls and windows as appropriate.	✓		
12.	Place access points in secured areas to prevent unauthorized physical access and user manipulation.	✓		
Technical Recommendations				
13.	Empirically test access point range boundaries to determine the precise extent of the wireless coverage.	✓		
14.	Make sure that access points are turned off when they are not being used (e.g., after hours and on weekends).	✓		
15.	Make sure that the reset function on access points is being used only when needed and is invoked only by an authorized group of people.	✓		

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
16.	Restore the access points to the latest security settings when the reset functions are used.	✓		
17.	Change the default SSID in the access points.	✓		
18.	Disable the broadcast SSID feature so that the client SSID must match that of the access point.		✓	
19.	Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products.	✓		
20.	Ensure that access point channels are at least five channels different from any other nearby wireless networks to prevent interference.	✓		
21.	Understand and make sure that all default parameters are changed.	✓		
22.	Disable all insecure and nonessential management protocols on the access points.	✓		
23.	Enable all security features of the WLAN product, including the cryptographic authentication and WPA, AES encryption feature.	✓		
24.	Ensure that encryption key sizes are at least 128-bits or as large as possible.	✓		
25.	Make sure that default shared keys are periodically replaced by more secure unique keys.	✓		
26.	Install a properly configured firewall between the wired infrastructure and the wireless network (access point or hub to access points).	✓		
27.	Install anti-virus software on all wireless clients. http://www.cert.mil/antivirus/av_info.htm	✓		
28.	Install personal firewall software on all wireless clients.	✓		
29.	Disable file sharing on wireless clients (especially in untrusted environments).	✓		
30.	Deploy MAC access control lists.		✓	
31.	Consider installation of Layer 2 switches in lieu of hubs for access point connectivity.	✓		
32.	Deploy IPsec-based VPN technology for wireless communications.	✓		
33.	Ensure that the encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.	✓		
34.	Fully test and deploy software patches and upgrades on a regular basis.	✓		
35.	Ensure that all access points have strong administrative passwords.	✓		
36.	Ensure that all passwords are being changed regularly.	✓		
37.	Deploy user authentication such as biometrics, smart cards, two-factor authentication, and PKI.		✓	
38.	Ensure that the "ad hoc mode" for 802.11 has been disabled unless the environment is such that the risk is tolerable. Note: some products do not allow disabling this feature; use with caution or use different vendor.	✓		
39.	Use static IP addressing on the network.		✓	
40.	Disable Dynamic Host Configuration Protocol (DHCP).		✓	

	Security Recommendation	Checklist		
		Best Practice	Should Consider	Status
41.	Enable user authentication mechanisms for the management interfaces of the access point.	✓		
42.	Ensure that management traffic destined for access points is on a dedicated wired subnet.	✓		
43.	Use SNMPv3 and/or SSL/TLS for Web-based management of access points.	✓		
Operational Recommendations				
44.	Configure SNMP settings on access points for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended.	✓		
45.	Enhance access point management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.	✓		
46.	Use a local serial port interface for access point configuration to minimize the exposure of sensitive management information.		✓	
47.	Consider other forms of authentication for the wireless network, such as RADIUS and Kerberos.		✓	
48.	Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.		✓	
49.	Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.		✓	
50.	Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.		✓	
51.	Enable use of key-mapping keys (802.1X) rather than default keys so that sessions use distinct WEP keys.	✓		
52.	Fully understand the impacts of deploying any security feature or product prior to deployment.	✓		
53.	Designate an individual to track the progress of 802.11 security products and standards (Internet Engineering Task Force [IETF], IEEE, etc.) and the threats and vulnerabilities with the technology.		✓	
54.	Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features.		✓	
55.	When disposing access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	✓		
56.	If the access point supports logging, turn it on and review the logs on a regular basis.	✓		

Figure 41. NIST WLAN Security Checklist (From Ref. 75)

⁷⁵National Institute of Standards and Technology (NIST), (2002), *Wireless LAN Security Framework Addendum to the Wireless Security Technical Implementation Guide*, (Special Publication 800-48), Wireless LAN Security Checklist, <http://iase.disa.mil/wireless/index.html>, Retrieved August 18, 2005.

d) Bluetooth and Infrared (IR)

Although the scope of this thesis limits the majority of our research in wireless security to 802.11, it cannot be emphasized enough the extreme vulnerabilities found in Bluetooth[®] and Infrared enabled devices. Vulnerability assessments should always scan for Bluetooth and infrared services. Bluetooth attacks can now be done from miles away as opposed to the limited distance of 30 feet as previously thought. On an average installation it would be virtually impossible to not find any Bluetooth or IR devices connected to the target network or transmitting data from the network.

4. Out-brief

Once the assessment is completed, the initial results will need to be briefed back to the organization. The out-brief is usually handled in similar fashion as the in-brief with regard to the level and the formality of the brief. It is important to be flexible; however it is equally important to ensure that the appropriate level of audience is present to hear and provide momentum for any actionable findings. During several of our assessments, it appeared as if we were not getting the attention of the necessary individuals during the either a respective in-brief or out-brief. It was our intention and ultimately our strong recommendation that these briefings be received by no less than the responsible Communications Officer within the organization. While this individual may not require the technical expertise of his Communications Chief or other WLAN administrators within his staff, it is imperative that the individual ultimately responsible directly understands any potential vulnerabilities that were found during the assessment.

5. Formal Report to Document Findings

While the initial results of the vulnerability assessment will be communicated during the out-brief, they will be formally documented in the final report. The report should be in standard Naval Letter format and addressed to the Commanding Officer of the organization. The report will identify the assessment date, the units and individual personnel involved, areas assessed, along with a detailed list of findings. An example of a WLAN vulnerability assessment finding could be something as simple as the organization not implementing an encryption scheme like WPA to protect their WLAN

data. However, the most important aspect of the formal report though is not the findings, it is the recommendations for corrective action. This will provide the organization with guidance on how to correct any vulnerabilities. The final critical piece of information in the final report is the date by which the corrective action must be implemented. Due to the nature of most WLAN vulnerabilities, quick and decisive corrective actions are imperative to protect adjacent communication infrastructure.

6. Conduct Follow-up Assessment on Deficiencies

The final step to accomplish with regard to any assessment or evaluation is appropriate follow-up to ensure that corrective action has been implemented. WLAN assessment follow-up is no less critical. Without proper follow-up, the efforts to conduct the assessment, to include the investment of valuable time and resources will be lost. For the most part, the follow-up assessment will not be nearly as thorough as the original assessment. You will only need to review the vulnerabilities identified in your final report to ensure corrective action was implemented.

D. RECOMMENDED TOOLKIT

1. WLAN Vulnerability Assessment Toolkit (WiVAT)

One of the practical outputs that we wanted to achieve within the context of our thesis was the identification of a standard set of tools and procedures to conduct vulnerability assessments within the Marine Corps. In that vain, we have selected several of the previously identified tools which we believe provide the most functionality, greatest utility, least amount of complexity, and represents the best value for conducting vulnerability assessment within the Marine Corps.

a. Hardware/Software

In order to have a mobile toolkit used for assessing wireless security we started with two #1600 Pelican[™] cases which provide unbreakable, waterproof, chemical resistant, corrosion proof, and buoyant protection for expensive and delicate electronic gear. Two cases provide the flexibility to load one case with the requirements for a small assessment or both cases for a larger assessment.

The following list represents a quality set of hardware and software tools to be used for WLAN vulnerability assessments:

- Pelican #1600 cases (2)
- IBM laptops (2) – with internal wireless and Bluetooth card
- HP iPaq PDA (2) – used with Yellowjacket and mini-stumbler
- Garmin 60C GPS – used with Kismet to log GPS coordinates
- Directional antenna (2) – with pigtails for different connectors
- Omni-directional antenna (2)
- BVS Yellowjacket
- Cognio Intelligent Spectrum Management System card
- Netgear 8 port 100Mbps Fast Ethernet Switch

- Remote-Exploit's Auditor Security Collection bootable CD and all accompanying software included
- Wildpackets AiropEEK NX WLAN analyzer
- Wildpackets RF Grabber distributed WLAN probe
- Netstumbler & Mini-Stumbler for iPaq
- Linksys WRT54GC Compact Wireless Router 802.11g
- Linksys USB wireless compact adapter
- Surge Protector (2)
- Ethernet cables (8) – crossover and straight-through
- Batteries and charging station
- 100GB external hard drive
- 1GB USB flash drive

Figure 42 and 43 show pictures of the individual hardware components laid out and packed into the Pelican cases.



Figure 42. WiVAT hardware components (From Ref. 76)



Figure 43. WiVAT packed (From Ref. 77)

⁷⁶Adam K. Kessel, Captain USMC, Naval Postgraduate School, WiVAT hardware components, September 10, 2005.

THIS PAGE INTENTIONALLY LEFT BLANK

⁷⁷Adam K. Kessel, Captain USMC, Naval Postgraduate School, WiVAT packed in Pelican cases, September 10, 2005.

VIII. EXEMPLAR WLAN IMPLEMENTATION GUIDE AND HARDWARE/SOFTWARE USAGE:

A. HIGH LEVEL HARDENED WLAN

1. Introduction to Wireless Implementation Research

Four DoD organizational WLANs were evaluated during the course of this thesis research. It should be noted that all four of these wireless implementations were found to have multiple weaknesses and associated vulnerabilities. Our goal was to find a relatively secure WLAN according to policy and compare this secure implementation to what is currently employed in the DoD. After extensive searching, it was possible to find one particular organization that was authorized to do this type of research and had funding available to implement a WLAN without operating restrictions or experimental constraints during the testing and implementation phases.

This organization described will be referred to as Organization 3 because of classification issues. This network took a total of two years to implement which required extensive research and budgeting for the requisite hardware and software to be purchased and installed. This organization started with a 100MB backbone which created latency when 100 or more users were on the wireless network. They were able to upgrade to a 2GB fiber backbone and added supplementary APs which allowed large amounts of users to use the wireless network without any observed latency. To date, no problems have occurred with this bandwidth and the goal is to have four buildings with a maximum of 750 users. It was determined that the costs savings for setting up a wireless network as opposed to wired was roughly \$55,000.

2. Defense in Depth

This well known security principle which was discussed in Chapter Three, is prescribed by DoD Directive 8500.1. This Directive requires the use Defense in Depth as a layered approach to network security. This concept is particularly important in the wireless arena because there is no need to access the medium as would be required in the wired world. The traffic is over-the-air and cannot be 100% secured by one layer of

defense. To this end, all wireless traffic must be secured by multiple techniques which will be displayed further in this thesis.

a. *First Level*

In order to accomplish Defense in Depth, each layer must be carefully planned out in advance to ensure that each security area of the network is covered by multiple levels of defense. For instance, in the first level of defense, the wireless network is physically and logically segmented to prevent easy access to the wired network. This is what is considered the first level of defense and is also the least complex. The second level is specifically dealing with encryption which in and of itself separates the wireless network from other unencrypted traffic. This is done at layer 2 of the OSI model which is universally considered the appropriate technique as opposed to layer 3 which will show all IP addresses traversing the wireless network. So between the first and second layer of defense, they synergistically make each other stronger by creating multiple obstacles to get past as opposed to one sole target to overcome. VLANs provide segmentation by separating networks with different levels of value and corresponding security mechanisms. For example, an organization's data network may be considered at the highest level of value while voice may be medium level and visitor's data may be at the lowest level of value. Figure 44 shows how one device is able to accomplish network segmentation with VLAN capability.

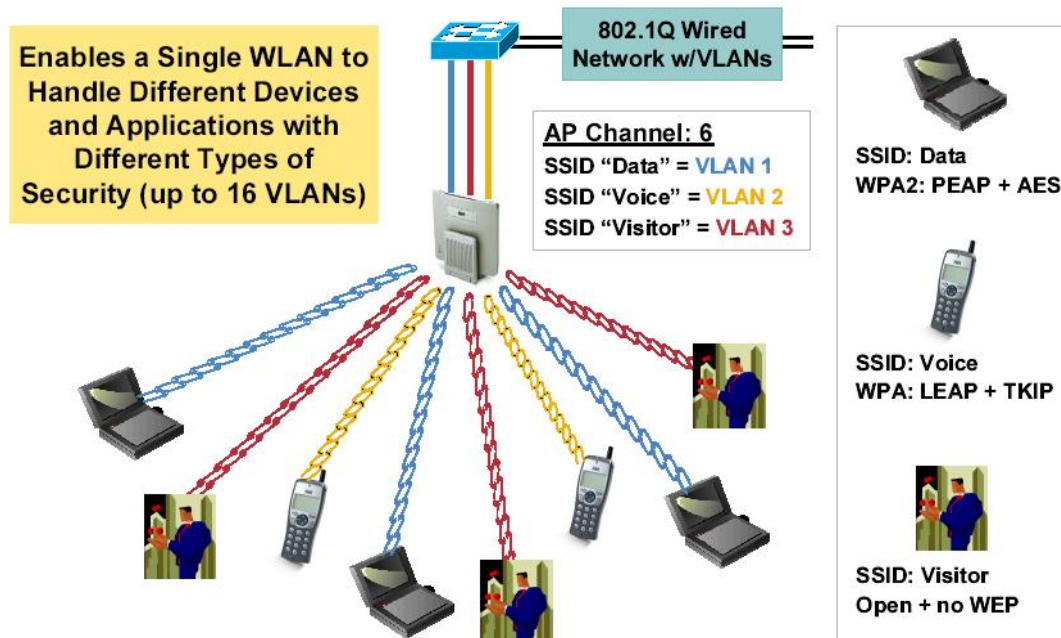


Figure 44. Network Segmentation (From Ref. ⁷⁸)

Organization 3 was able to use the network security principle of defense in depth by implementing what they consider, 5 levels of defense. As mentioned previously, level 1 starts with "Wireless Network Segmentation." This is accomplished by either the suggested route which is a power-over-Ethernet switched network or using VLANs which is acceptable according to DISA. In addition, the following levels combine to accomplish network segmentation.

b. Second Level of Defense

Level 2 is implemented using "Encryption Separation" also known as separation through encryption which means that no client can access the wireless network without a properly configured software client. The software and hardware used to attain level 2 defense is known as Air Fortress which is FIPS 140-2 certified and encrypts all traffic at layer 2 with 128 bit AES. At layer 2 of the OSI model the only observable traffic reveals MAC addresses in the clear. No IP addresses or broadcast traffic can be sniffed. Another advantage of layer 2 encryption is that clients inside the network cannot

⁷⁸ Cisco Tech Talk: *High-Security, High-Capacity Wireless Networks*, http://www.cisco.com/cgi-bin/sreg2/register/banner.pl?LANGUAGE=E&METHOD=E&TOPIC_CODE=2949&PRIORITY_CODE=127750_2, Retrieved July 22, 2005.

be attacked from outside of the encrypted network unless a Denial of Service attack is employed. In contrast, layer 3 traffic is easily identified by the IP addresses in the clear. Anything broadcast can still be sniffed including POP, ARP, DHCP, NETBIOS, etc. With layer 3 encryption you leave the majority of your most important devices open to attack including your firewall, wireless gateways, and your clients. Typical implementations of layer 3 encryption include IPSEC and VPN setups. Organization 3 concentrates on the maxim, “Maximum Security, Maximum Performance, Minimal Management⁷⁹.” Figure 45 shows how Air Fortress accomplishes encryption separation and how Organization 3 used the AF7500.

AF7500 Configuration

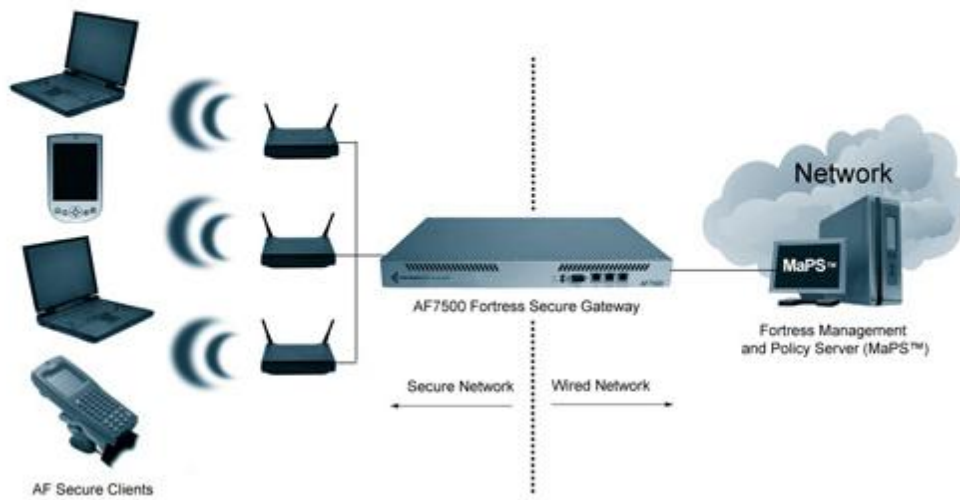


Figure 45. Air Fortress generic configuration (From Ref. ⁸⁰)

Fortress Technologies provides a comprehensive, robust wireless solution that is easy to implement and maintain. The Fortress solution offers complete protection of all platform investments by supporting the widest range of devices and existing networks. To efficiently and securely address the inherent risks and vulnerabilities of wireless, the Fortress solution works with multiple wireless standards. It installs easily into

⁷⁹ Derek Krein, Tony Cerri, Secure Wireless Networks Presentation, Norfolk, VA April 29, 2005.

⁸⁰ Fortress Technologies, *Fortress Enterprise Brochure*, <http://www.fortresstech.com/products/af2100.shtml>, Retrieved July 22, 2005.

mixed-vendor environments including DOS legacy systems, providing a single point-of-administration for all wireless networks⁸¹.

Figure 46 shows how Air Fortress encryption devices can be used operationally.

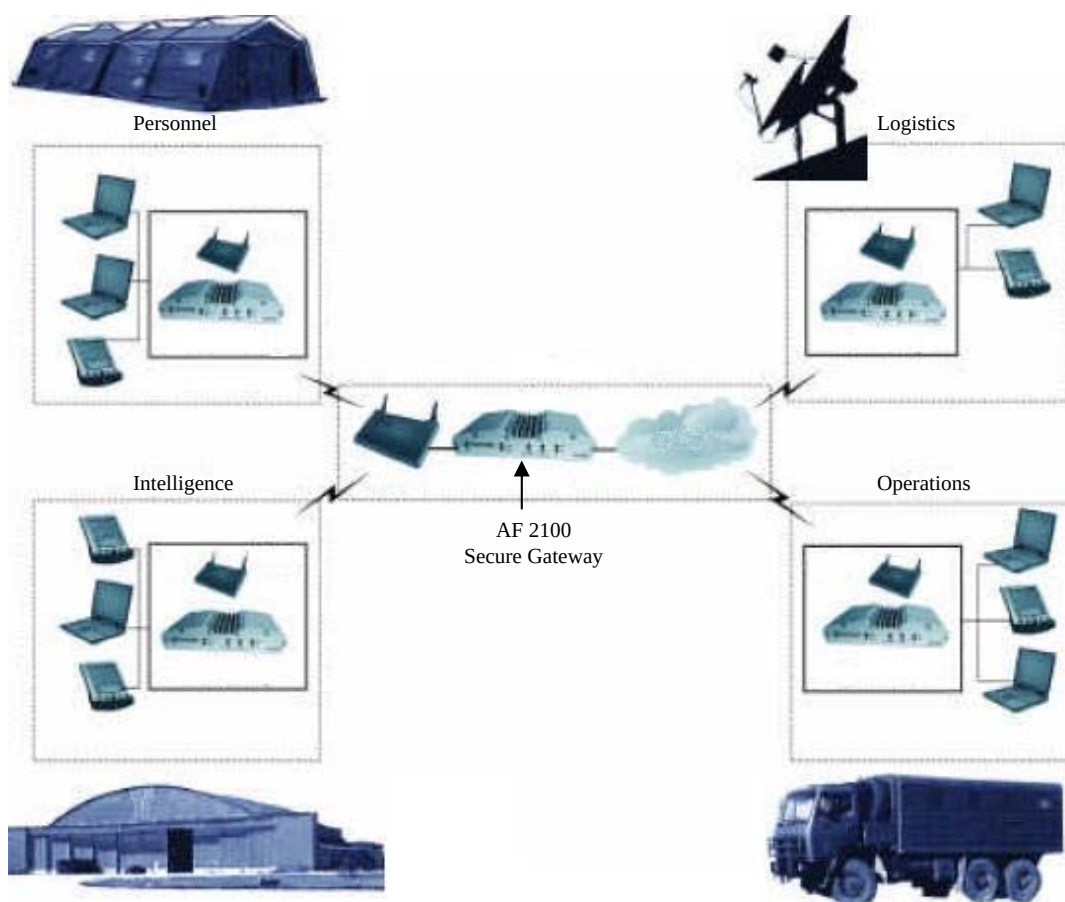


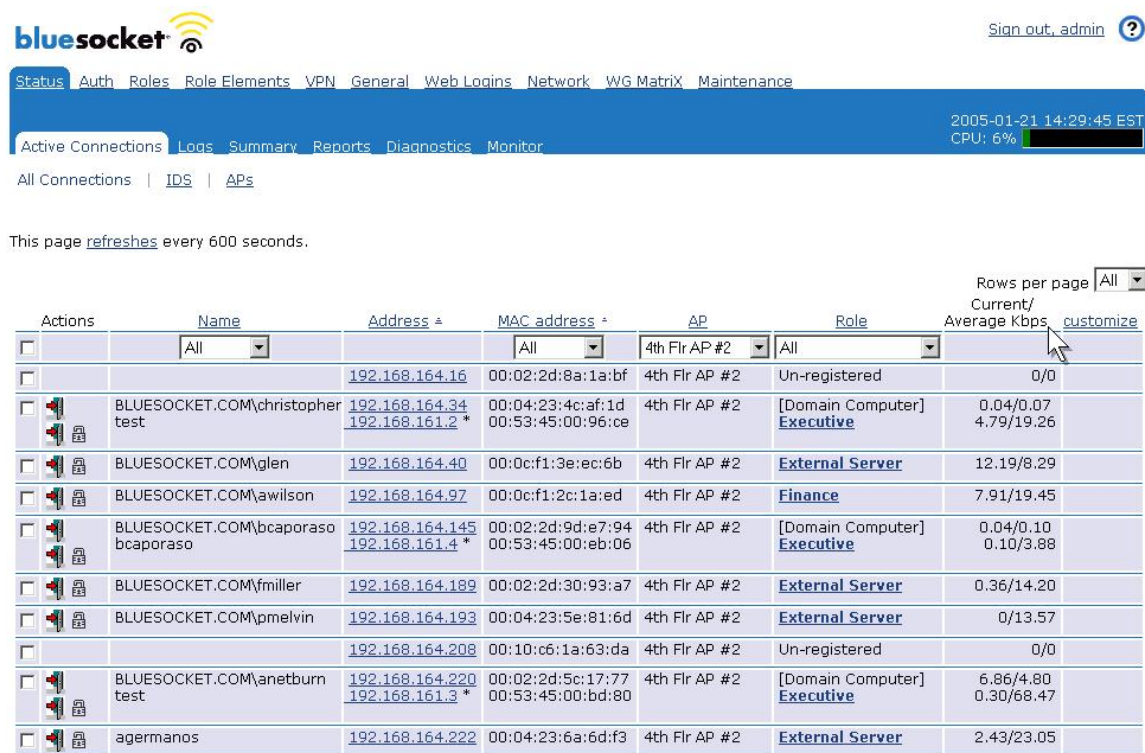
Figure 46. Air Fortress generic configuration (From Ref. ⁸²)

⁸¹ Ibid.

⁸² Fortress Technologies, *Mobile LANs, Wireless Combat Information Systems Security*, <http://www.fortresstech.com/solutions/government.shtml>, Retrieved July 22, 2005.

c. Third Level of Defense

Level 3 defense capabilities consist of a wireless gateway with a firewall feature set. This particular wireless gateway which was decided upon is called Bluesocket. Bluesocket is a standards based solution which will work with most popular access points on the market today. It has strong authentication mechanisms which include 802.1x pass-through and NTLM/Active Directory pass-through. NTLM is Windows NT Challenge/Response authentication. This solution provides Role Based access control, schedule, and location control. In addition, it has extensive logging and packet capture capabilities. Figure 47 shows all active connections on a sample wireless network



Actions	Name	Address *	MAC address *	AP	Role	Current/Average Kbps	customize
☐	All		All	4th Flr AP #2	All	0/0	
☐	BLUESOCKET.COM\christopher test	192.168.164.34 192.168.161.2 *	00:04:23:4c:af:1d 00:53:45:00:96:ce	4th Flr AP #2	[Domain Computer] Executive	0.04/0.07 4.79/19.26	
☐	BLUESOCKET.COM\glen	192.168.164.40	00:0c:f1:3e:ec:6b	4th Flr AP #2	External Server	12.19/8.29	
☐	BLUESOCKET.COM\awilson	192.168.164.97	00:0c:f1:2c:1a:ed	4th Flr AP #2	Finance	7.91/19.45	
☐	BLUESOCKET.COM\bcaporaso bcaporaso	192.168.164.145 192.168.161.4 *	00:02:2d:9d:e7:94 00:53:45:00:eb:06	4th Flr AP #2	[Domain Computer] Executive	0.04/0.10 0.10/3.88	
☐	BLUESOCKET.COM\miller	192.168.164.189	00:02:2d:30:93:a7	4th Flr AP #2	External Server	0.36/14.20	
☐	BLUESOCKET.COM\pmelvin	192.168.164.193	00:04:23:5e:81:6d	4th Flr AP #2	External Server	0/13.57	
☐		192.168.164.208	00:10:c6:1a:63:da	4th Flr AP #2	Un-registered	0/0	
☐	BLUESOCKET.COM\anetburn test	192.168.164.220 192.168.161.3 *	00:02:2d:5c:17:77 00:53:45:00:bd:80	4th Flr AP #2	[Domain Computer] Executive	6.86/4.80 0.30/68.47	
☐	agermanos	192.168.164.222	00:04:23:6a:6d:f3	4th Flr AP #2	External Server	2.43/23.05	

Figure 47. Bluesocket Active Connection screen (From Ref. 83)

The Blue Secure Controller provides comprehensive authentication options utilizing username/password combinations or digital certificates, with the authentication database held locally or centrally in RADIUS, LDAP, NT Domain servers,

⁸³ Bluesocket, *BlueSecure Controllers Tour*, <http://www.bluesocket.com/products/controllerfamily.html>, Retrieved July 22, 2005.

or Windows Active Directories. Users can log into a Windows Domain and authenticate to the WLAN seamlessly with Bluesocket's unique "Transparent Windows Domain Login." Where AP-based WPA/802.11i authentication is required, Bluesocket complements the login process transparently, allowing appropriate access for the WLAN user. Where browser-based, secure (SSL) login is required (e.g. Hot Spots, Universities, Guests/Visitors), Bluesocket supports a customizable web-login page that allows end-user branding and an ability to upload third-party SSL certificates. Where "non-intelligent" devices need WLAN access, MAC-based authentication and role/VLAN assignment is supported, providing true wireless fire-walling capabilities. Figure 48 shows a Bluesocket sample topology configuration.

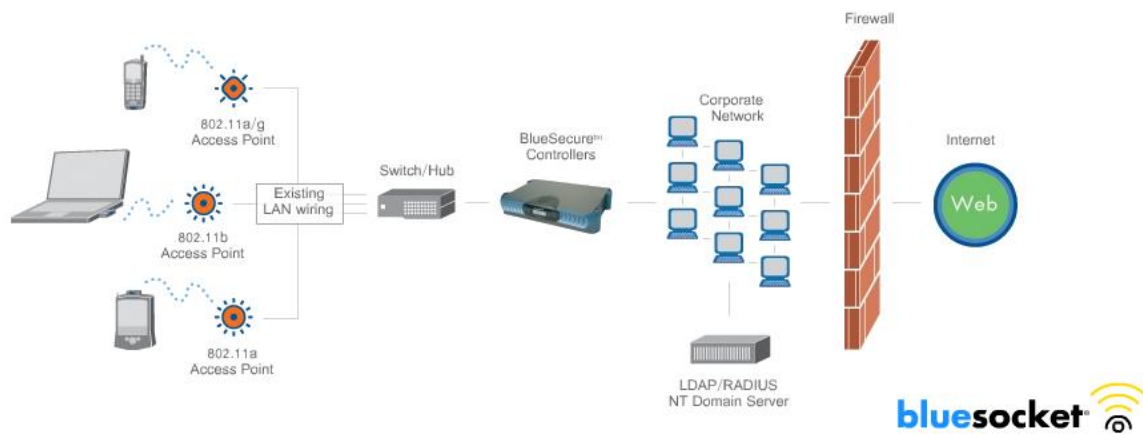


Figure 48. Bluesocket's suggested topology (From Ref. ⁸⁴)

d. Fourth Level of Defense

The 4th level of defense is a Wireless Intrusion Protection System (WIPS) previously known as a Wireless Intrusion Detection System (WIDS). Organization 3 employed the Air Defense WIPS solution which is a very well known product that has been proven to work well and continually improves. Improvements include modifications such as Air Termination or Containment which is automated through the Air Defense device in order to kick an unauthorized user or access point off of the network and keep them out.

⁸⁴ Bluesocket, *BlueSecure Controllers Tour*, <http://www.bluesocket.com/products/controllerfamily.html>, Retrieved July 22, 2005.

A key concept that Organization 3 points out is the fact that a WIPS should be used whether you have an authorized WLAN or not. The reason for this is to prevent rogue access points to set up wireless access to your wired network. Another serious threat other than rogue access points that must be addressed is to ensure that ad-hoc networks are not established which again, can give unauthorized access to the network. Without an established WIPS, it would be very difficult to keep aware of rogue access points if not impossible. These sensors are placed throughout the area of operations with enough coverage to assess all areas inside the buildings as well as any bleed-over outside of the buildings. The Air Defense servers which the sensors connect to are placed on the internal network to prevent interference on the wireless network. All sensor data is then sent to the server which can be accessed by the administrators via Secure Socket Layer (SSL). The server is preconfigured to control the individual security policy that must be enforced. Air Defense provides a near real-time performance view of the wireless medium.

Air Defense has the ability to communicate with existing wireless management platforms & mitigate threats from the wired-side (port or switch), or in some cases, turn off the access point completely which is what the company calls Wired-side Termination. Figure 49 shows sensor placement and an example topology.

Figure 50 displays a recent and fairly successful technique called Air Termination or Containment. After an intruder or attack is detected connecting to an access point, Air Defense can terminate the wireless connection from the intruder to the access point. Air Defense can mitigate detected threats through the air or by wired-side via its Active Defenses, either manually or automatically via a predefined policy. After the detection of an intruder or rogue device, Air Defense gives enterprises the ability to mitigate the threat by terminating the wireless connection between the intruder station and an authorized access point, or by terminating the connections of authorized stations to a rogue access point. This capability is enterprise-class, with role restrictions on who can terminate devices, and an audit trail of all termination activities, including time, device and user performing termination. This process is what is called Air Termination.

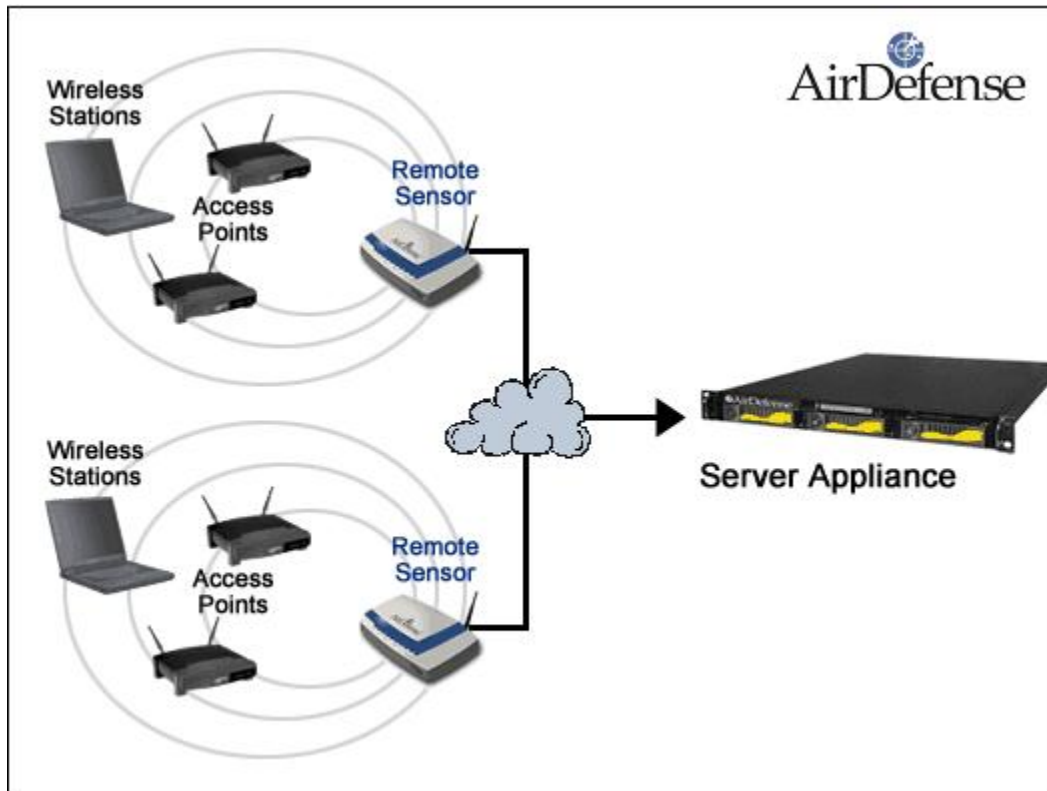


Figure 49. Air Defense example topology (From Ref. ⁸⁵)

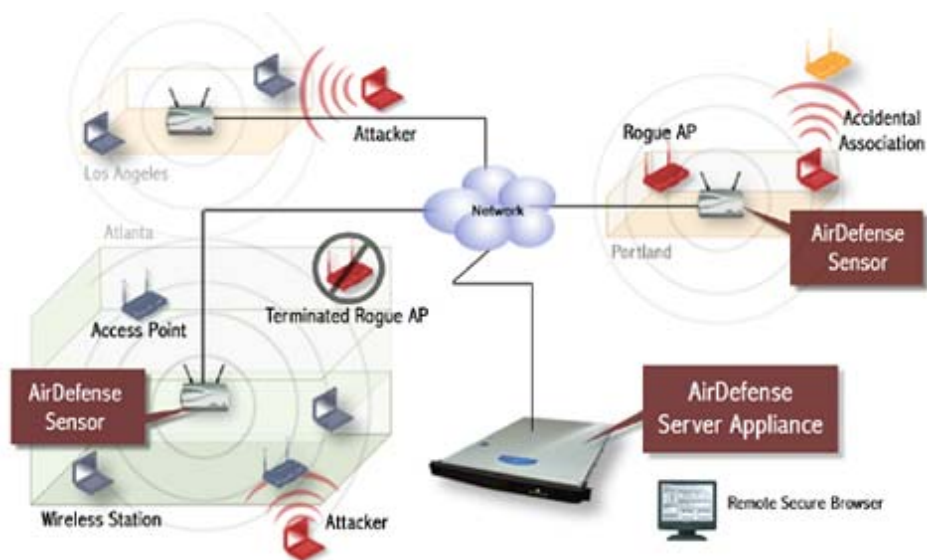


Figure 50. Air Defense Rogue AP and Termination techniques (From Ref. ⁸⁶)

⁸⁵ Air Defense, *Air Defense Topology*, <http://www.airdefense.net/products/enterprise.html>, Retrieved July 22, 2005.

⁸⁶ Ibid.

e. Fifth Level of Defense

The 5th level of defense is a Centralized Wireless Network Management solution called AMP by Airwave, which brings all the defense levels together and unites them into one interface. The AirWave Management Platform is a Linux-based software solution that installs quickly and easily on standard PC server hardware, typically in one or more network operations centers. Administrators and help-desk personnel can use AMP's web-based user interface to remotely monitor and manage their wireless networks, or they can fully integrate AMP with their existing Ethernet network management solutions (such as HP OpenView Network Node Manager).

AMP's high-speed data collector uses non-blocking SNMP, HTTP, and other protocols to gather granular data, enabling the ability to quickly locate and view real-time information on every wireless device and user connected to the network. AMP uses Simple Network Management Protocol (SNMP) to provide constant configuration management. Organization 3 is using SNMPv3 which protects management traffic with encryption. This is a great feature for large enterprise applications in which adding and removing of Access Points requires the most current configuration before you can put it on the network. With AMP, all you need to do is plug it in, Air Defense will recognize it as a misconfigured AP, determine whether it is authorized or not and will push the correct settings. AMP will also provide radio statistics at the AP and client level to determine number of users and percentage of bandwidth being used. AMP can be configured to send near real-time alerts of problems or down AP's, switches, Air Defense sensors, and other wireless network infrastructure components. It also provides the user with site plan management features such as power, throughput, and Electromagnetic Interference (EMI) reduction. Figure 51 shows AMP's ability to monitor APs activity.

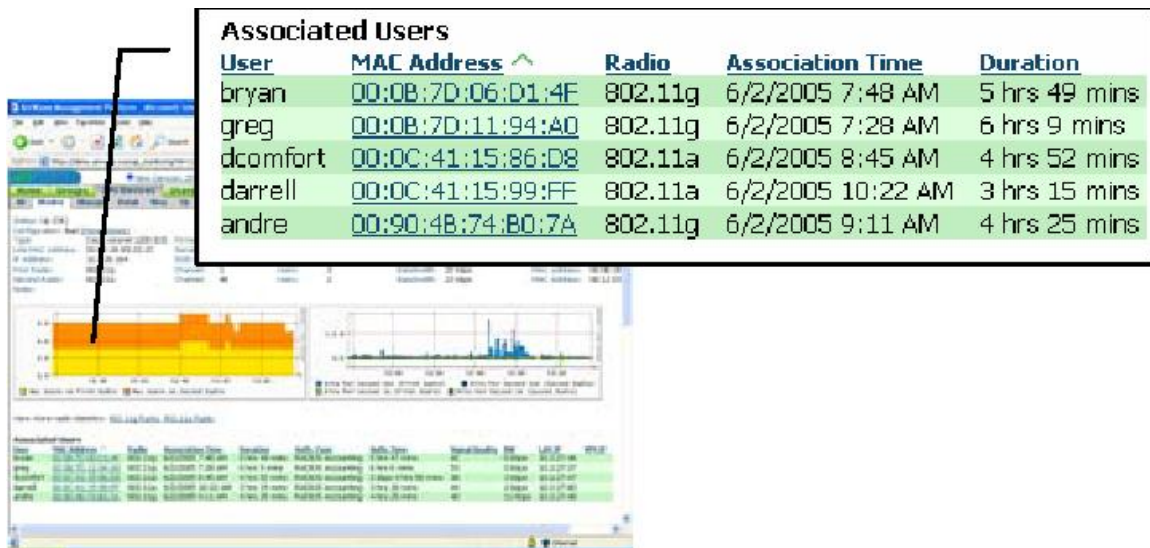


Figure 51. AMP's AP monitoring (From Ref. ⁸⁷)

Designed for efficiency, AMP's scalable, distributed architecture allows you to configure, manage, and monitor Wi-Fi equipment across a LAN or WAN of any size — from local networks with 25 or fewer access points to global networks with tens of thousands of wireless network devices.

AMP is a fully vendor-agnostic solution that supports new and legacy Wi-Fi hardware from leading vendors, including Avaya, Cisco (Aironet and Airespace), Colubris, Enterasys, Funkwerk, HP ProCurve, Intel, LANCOM, Nomadix, Proxim, Symbol, and others. AMP automatically handles all communication with multi-vendor devices, allowing administrators to monitor and configure diverse networks from the same easy-to-use web console. AP-based wireless scans using existing, authorized access points to scan the RF spectrum for other radios within range. AMP also includes an API for integration with third-party RF-based intrusion detection systems (such as Air Defense).

Figure 52 shows the ability to upload a floor plan with the AP's location and detect rogue access points in relation to the authorized AP's location.

⁸⁷ Airwave, *Airwave Product Line Overview*, http://www.airwave.com/prodserv_products.html, Retrieved July 22, 2005.

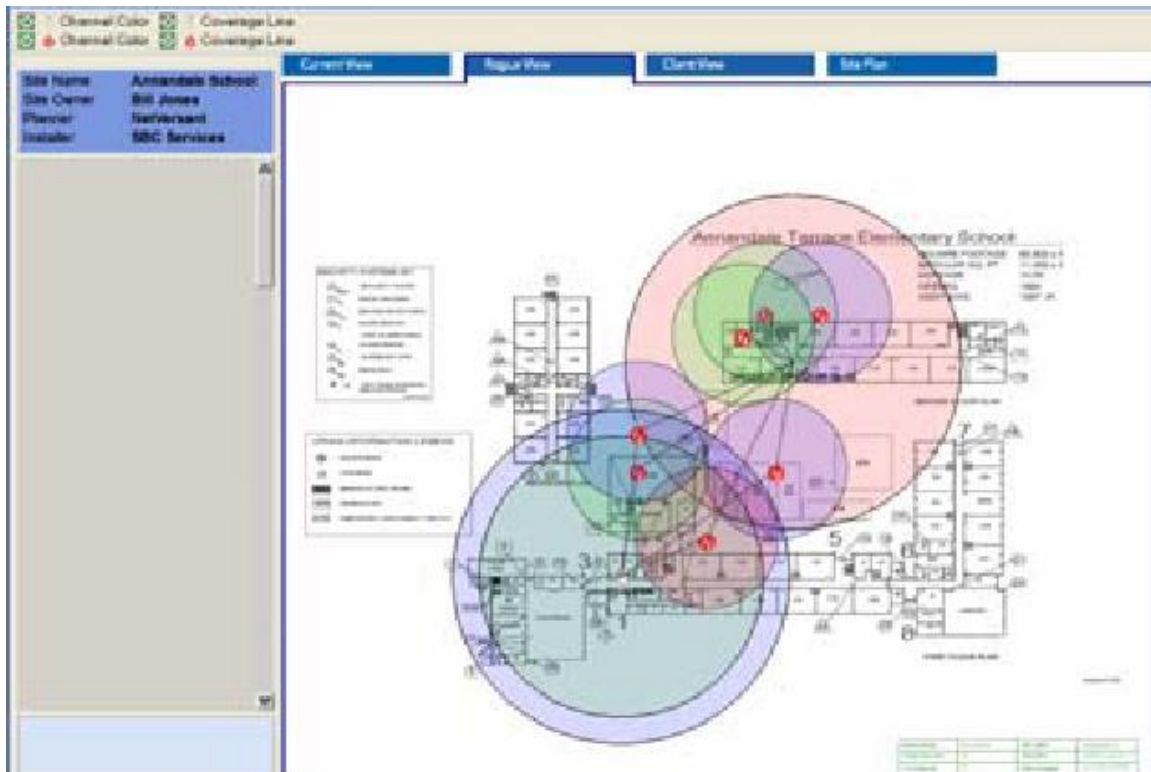


Figure 52. AMP's visualRF (From Ref. ⁸⁸)

Figure 53 and 54 show Organization 3's overall topology and a legend of device usage.

⁸⁸ Airwave, *Airwave Product Line Overview*, http://www.airwave.com/prodserv_products.html, Retrieved July 22, 2005.

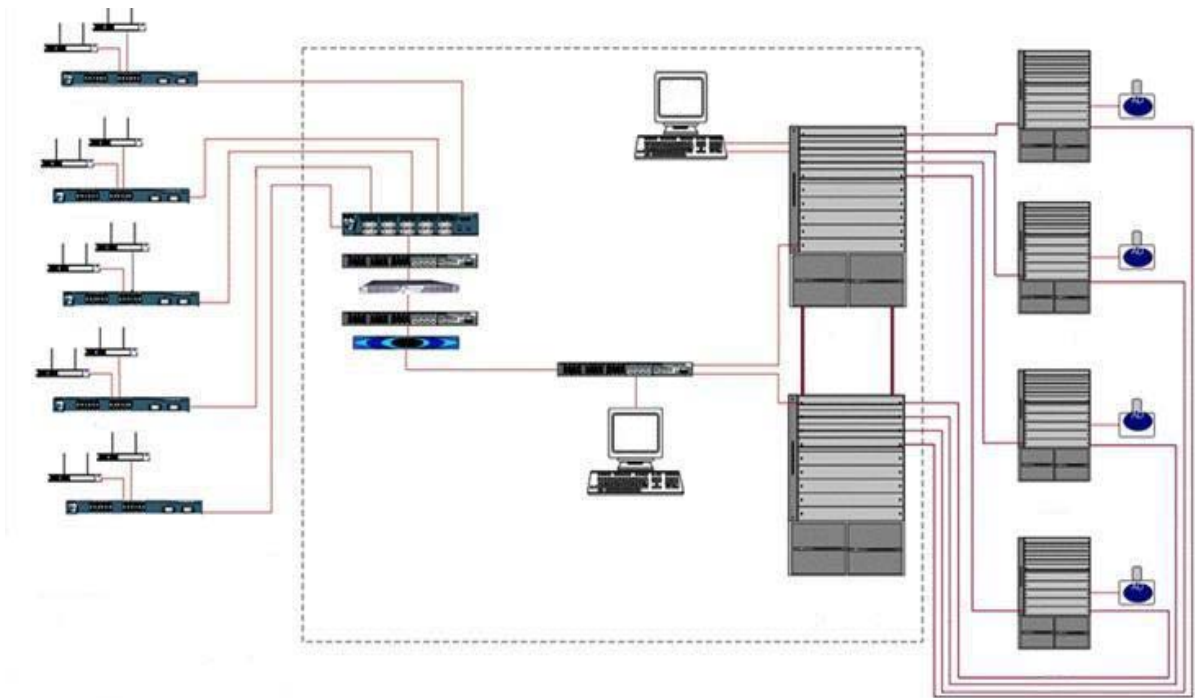


Figure 53. Organization 3 overall topology (From Ref. ⁸⁹)



Figure 54. Organization 3 device usage (From Ref. ⁹⁰)

⁸⁹ Derek Krein, Tony Cerri, Secure Wireless Networks Presentation, Norfolk, VA April 29, 2005.

⁹⁰ Ibid.

3. Voice over IP (VOIP)

Organization 3 found that VOIP was an excellent way to leverage their wireless network investment to include cost savings for telephone services. VOIP has been implemented on site with great success. The phone network runs on Cisco's VOIP technology which works well with the Cisco AP's. In addition, Vocera communicators have recently been implemented to extend the reach of the VOIP network to include mobile inter and intra- building communications. This technology provides simultaneous hands-free two-way communication. It has the capability to broadcast messages out to all users and conference call capabilities. As it was mentioned previously in Chapter 5, Vocera recently added support for Cisco's lightweight extensible authentication protocol (LEAP) and temporal key integrity protocol (TKIP). In addition, the company has released support for Wi-Fi protected access (WPA) which will be implemented completely by Organization 3 when the 802.11i protocol is ratified. Figure 55 shows a sample Vocera topology and Figure 56 shows a close-up of a badge communicator.

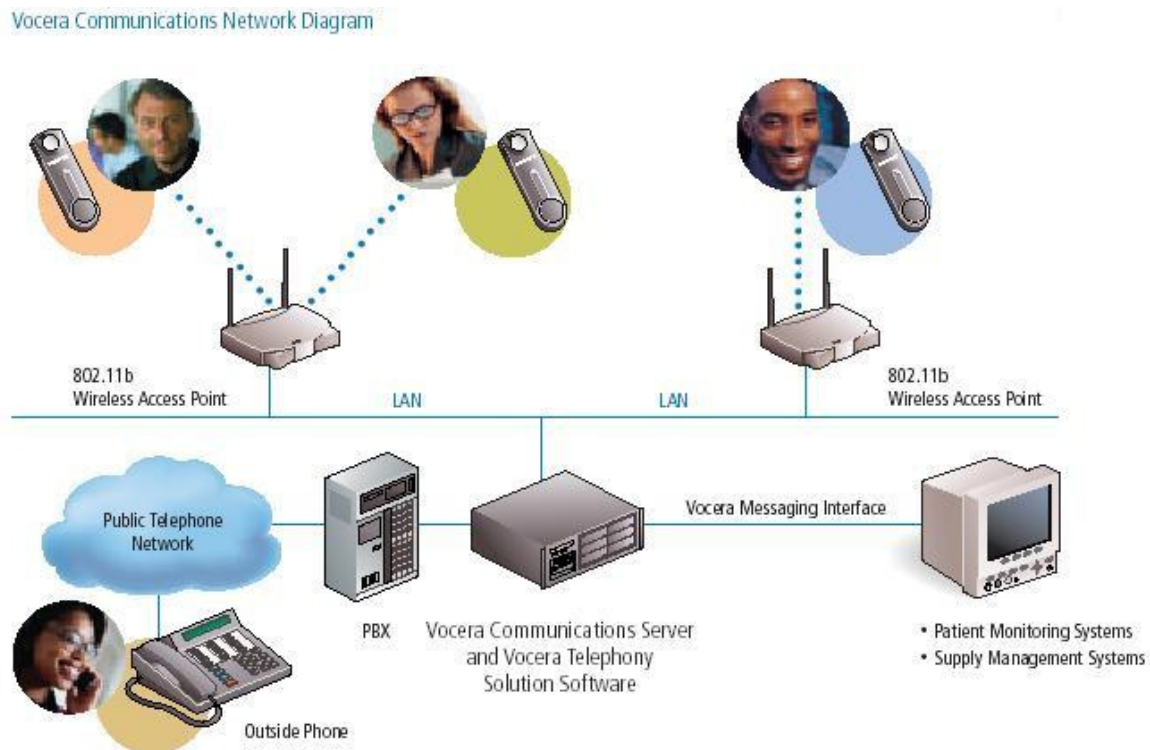


Figure 55. Vocera sample topology (From Ref. ⁹¹)

⁹¹ Vocera Communications, *Products*, <http://www.vocera.com/products/products.shtml>, Retrieved July 22, 2005.



Figure 56. Vocera communicator (From Ref. ⁹²)

4. Power Over Ethernet

In addition, Cisco's solution for Power over Ethernet (PoE) is being used to address power restriction issues and cost savings to power the majority of the wireless infrastructure. Organization 3 uses Cisco Catalyst switches to enable Power over Ethernet. Deploying Gigabit Ethernet ports with Power over Ethernet not only provides the incremental performance and productivity gains expected from Gigabit Ethernet, but also allows organizations to invest in scalable technology that will enable the deployment of new applications and services without the need for additional upgrades such as electrical installations. This gives the organization the ability to lower the overall cost of network ownership through optimal use of the LAN infrastructure, thereby reducing capital expenditures, simplifying manageability, and lowering operating costs. One risk that must be considered when deploying PoE throughout the entire wireless infrastructure is the possibility that the switch that provides power for the WLAN may go down due to some unforeseen surge in power or any other problem which could result in a Denial of Service throughout the entire wireless network.

⁹² Vocera Communications, *Products*, <http://www.vocera.com/products/products.shtm>, Retrieved July 22, 2005.

5. Remote Access

Remote access is at the forefront of security issues and the problem is ensuring the same security within your network when outside the network. Organization 3 uses SenForce and iPass encryption and policy enforcement solutions. SenForce is a Layer 2 policy enforcement agent while iPass prevents any client from connecting to the network without proper configuration such as up to date antivirus, patches or software. In addition, while data is resident on a roaming computer outside the network, it is secured with Mobile Armor's strong whole disk encryption. This encryption is centrally managed software that supports multi-factor authentication. Figure 57 shows iPass's remote access topology and Figure 58 displays the Senforce Security Client with Central Management and Reporting.

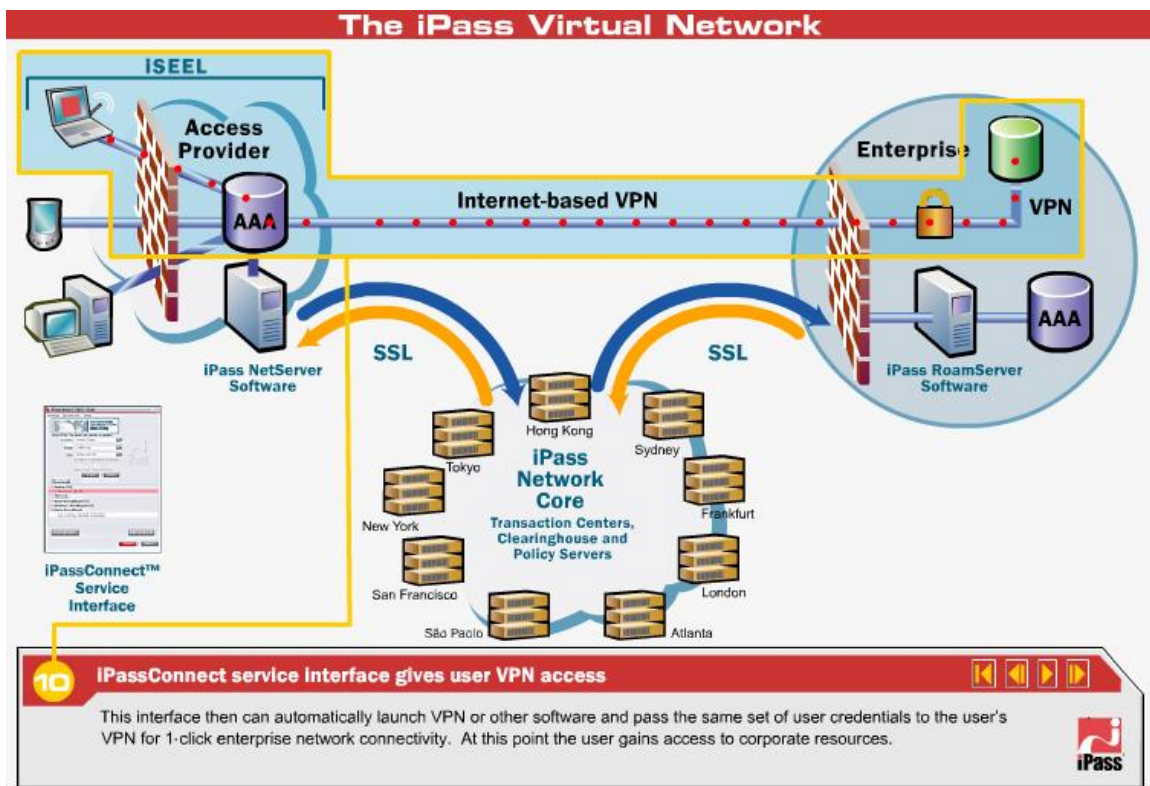


Figure 57. iPass remote access topology (From Ref. ⁹³)

⁹³ iPass, *Virtual Network Platform*, http://www.ipass.com/platform/platform_demo.html, Retrieved July 22, 2005.



Figure 58. Senforce Security Client (From Ref. ⁹⁴)

6. Wired vs. Wireless

One of the main reasons why it is decided to not use wireless networks is because the wireless network will not support certain features that the wired network does. Of course it was originally thought that wireless was much less secure than wired, but now that is not quite true. Another issue against wireless used to be bandwidth or throughput, which is often used for streaming audio, video, and video teleconferencing (VTC). The original specifications for 802.11b did not contain the capacity for quality streaming of audio and video. With 802.11a/g and other protocols being introduced, the ability to stream content is now possible on wireless networks. Organization 3 can now stream video or IPTV to the desktop for applicable news and other information such as training without requiring each individual to be on site, as well as VTC capability. VX30 is the java based software being used currently which also enables HTML over SSL for secure video streaming. Figure 59 shows a typical VX30 Streaming Video Session.

⁹⁴ Senforce, *Security Client*, <http://www.senforce.com/prodendsuite.htm>, Retrieved July 28, 2005.

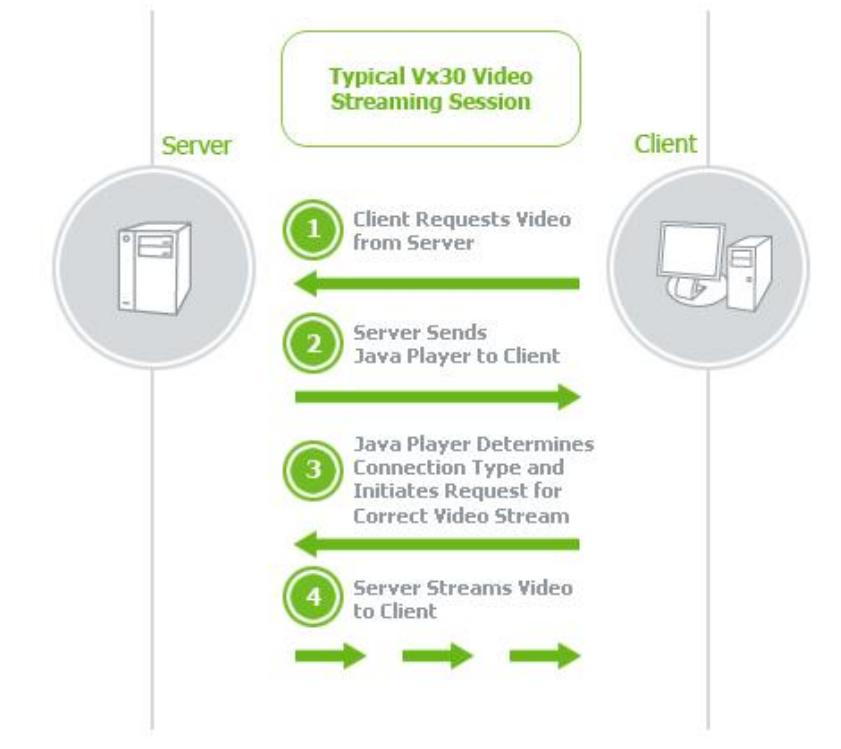


Figure 59. VX30 Streaming Video Session (From Ref. ⁹⁵)

B. SUMMARY

A diverse, high capacity and highly secure wireless network requires a skilled wireless network engineer along with extensive research and planning. This research and planning guides the success of the network. This organization demonstrated a very robust WLAN security implementation that can be extremely secure with little chance of interruption or vulnerabilities while reducing network costs significantly. Organization 3 researched the costs of wireless versus wired infrastructure and found that wireless is 40% - 50% cheaper than wired networks. Denial of Service attacks are always a concern whether it be wired or wireless and although wireless networks may be more vulnerable to this type of attack, WLANs will always have more powerful tools to combat this action. Many of the roadblocks that prevent wireless networks from being implemented stem from the question; how can we build a secure wireless network within DoD standards? This chapter provides one example of a potential WLAN implementation that strives to meet these standards.

⁹⁵ Maui X-Treme Inc., *VX30 Encoder*, <http://www.mxsinc.com/pages.php?cid=MDEwMDA0MDQy>, Retrieved July 22, 2005.

IX. CONCLUSION AND RECOMMENDATIONS

A. THE ROAD LESS TRAVELED

The overall purpose of our thesis was to improve the WLAN vulnerability assessment capability within the Marine Corps. We sought to meet this objective by progressively speaking to practical and fundamental issues related to the assessment and security of wireless networks. We began our research with a series of questions which we attempted to answer throughout the course of our thesis. The first question addressed the issue of why we need security in the first place. Chapter One presented the numerous threats, vulnerabilities and potential attacks which can bring a network to its knees. The second question we sought to answer was what can we do to mitigate those threats, vulnerabilities and attacks. The answer, found in Chapter Two, was to employ fundamental security principles like defense in depth, encryption, traffic filtering, restrict access to the WLAN, and employ firewalls and IDSs. The next question we asked was what 802.11 initiatives are currently employed within the Marine Corps. Chapter Three discussed STRATIS and SecNet-11, two prominent systems which have been implemented in the Marine Corps. The fourth question we sought to answer was, what is the security posture of WLANs within DoD. Chapter Four presented three real world WLAN assessments and detailed their vulnerabilities. Next, we asked what tools were available and best suited for conducting assessments. Chapter Five provided evaluations on 12 different WLAN tools which could be used by the Marine Corps for the purposes of conducting vulnerability assessments. The sixth question we sought to answer was how to conduct an assessment. Chapter Six detailed standard procedures which could be used to conduct an assessment and presented a recommended toolkit which is ideally suited for conducting vulnerability assessments. Our seventh research question queried the DoD landscape for a model of a secure WLAN. Chapter Seven presented a real world exemplar WLAN implementation which hosted secure wireless transmissions. Our final research question addressed what recommendations, based on our research, we would make to improve the security posture of WLANs within the Marine Corps. Our conclusion and recommendations will be presented in the following sections.

B. CONCLUSION

The convenience created by wireless devices coupled with their relatively low cost was largely responsible for the exponential growth of WLANs over the past decade. However, the conveniences of wireless technology came at a significant cost. WLANs have introduced vulnerabilities which must be countered in order to continue to reap the fruits of wireless labor. Policy designers realized the shortfalls inherent in the 802.11 standard and have subsequently released more security conscious standards. In addition, DoD has established guidance which levies even more stringent requirements upon wireless network implementations within DoD.

Unsecured WLANs are Cheap and Convenient

Secure WLANs are Complex & Expensive

Despite the presence of rigorous standards, which must be met in order to implement wireless networks, WLANs can be found on installations across the Marine Corps. The small strides made by additional security conscious standards and more stringent DoD and Marine Corps wireless policies have not slowed the growth of WLANs or eliminated the threats introduced by wireless technologies to Marine Corps information infrastructure. The plethora of WLANs in existence today was confirmed during the conduct of numerous WLAN vulnerability assessments aboard DoD and Marine Corps installations during the past year.

Secure WLANs are Scarce

Unsecured WLANs are Abundant

A critical investment of personnel, resources, and training is required to create a credible WLAN Vulnerability Assessment capability. Leaders, by and large, are not aware of the presence of WLANs or the threats introduced by them. In addition, personnel responsible for managing installation network resources are aware of wireless technology, but do not have the specific training or tools required to assess WLANs within their organizations. The widespread presence of WLANs aboard DoD

installations requires the development of a mature WLAN vulnerability assessment capability within the Marine Corps.

Awareness, Training and WLAN Tools are Insufficient

Need for Vulnerability Assessments is Critical

The combination of each of these factors creates substantial risks to information infrastructure aboard Marine Corps installations. The lack of awareness and training requires a dynamic and proactive training plan which leverages the WLAN expertise of external agencies. In addition, specific WLAN tools are needed to properly outfit organization IA personnel with the requisite tools to locate and assess WLANs. However, the most effective method to mitigate the risks associated with cheap, plentiful, unsecured wireless devices is to conduct WLAN vulnerability assessments. Effective training programs and capable tools combined with a proficient WLAN vulnerability assessment team will serve as an invaluable resource in mitigating the risks associated with wireless technologies.

Trained Personnel Equipped with Capable WLAN Tools Create a Proficient Vulnerability Assessment Capability

C. RECOMMENDATIONS

During the course of our research, we have observed weaknesses and/or deficiencies in the current WLAN landscape within the Marine Corps. This section will present those deficiencies along with recommendations on how to improve the WLAN vulnerability assessment capability within the Marine Corps.

1. Information Assurance (IA) Toolkits

The HQMC C4 IA has deployed toolkits to Major Subordinate Commands (MSCs) within the Marine Corps. These toolkits were assigned during an annual training conference to IA Chiefs. The toolkits were composed of a variety of open source and

commercial software tools which are hosted on a very powerful laptop. Even though, the majority of the software was aimed at assessing the wired infrastructure, there were several very important WLAN analysis tools which were included. As indicated in Chapter 6, NetStumbler, Kismet, and Ethereal are all capable software solutions. In addition, the bootable CD, Auditor, is perhaps the most capable wireless tool provided by HQMC. These tools should only represent a starting point towards outfitting IA Chiefs with the requisite tools required to conduct WLAN assessments. Figure 60 represents the IA Toolkit software suite which was distributed to IA Chiefs.

Open Source Tools		
Category	Tool	Potential Impact
Vulnerability Scanner	Nessus	DoS, OS Crash, Bandwidth
Web Application Testing	Nikto	OS Crash, Bandwidth
OS Fingerprinting/Port and Application Scanner	NMap	Bandwidth
Wireless	NetStumbler	None
Wireless	Kismet	None
Wireless	Ethereal	None
Password Cracker	John the Ripper	Account Lockout
Network Discovery	Sam Spade	None
Port Scanner	Grinder	Bandwidth

Commercial Tools		
Category	Tool	Potential Impact
Vulnerability Scanner	eEye Retina	DoS, OS Crash, Bandwidth
Configuration Scanner	Mitre Baseline Tool Kit (BTK)	DoS, OS Crash, Bandwidth
Password Cracker	L0pht Crack	Account Lockout
Enumeration	Solarwinds	Bandwidth
Network Discovery	Fluke LAN Mapshot	Bandwidth

Figure 60. IA Toolkit Software Suite (From Ref. ⁹⁶)

⁹⁶ HQMC C4, (2005), *Information Assurance Toolkit Software Suite*.

Recommendation: IA Chiefs will also need higher gain directional antennas which can be used to scan larger areas and pick up significantly more wireless traffic than external wireless cards with small omni-directional antennas. In addition, the directional antenna should be coupled with a tool which can help physically locate rogue access points. Handheld tools like Yellowjacket and AirMagnet Mobile offer “Geiger-like” meters which easily locate wireless devices which could compromise your WLAN. More powerful WLAN assessment software would also provide a powerful deterrent to unauthorized wireless activity. Tools like AiropEEK and Cognio, which were introduced in previous chapters, would strengthen the IA tool inventory.

2. WLAN Training

The IA Toolkits are a solid point of departure for tackling WLAN assessment. Individuals charged with information assurance need certain fundamental tools in order to identify WLANs within their areas of responsibility. The next critical requirement is to provide these individuals with specific training on how to use these tools and more advanced WLAN assessment education.

The DoD Directive 8570.1 delegates training responsibilities on the individual service components. It specifies that initial IA awareness orientation and annual IA refresher awareness be administered to all authorized users. More importantly, DoD 8570.1 charges the individual services with the responsibility to “establish, resource, and implement IA training and certification programs”. The Directive goes on to specify that “these programs shall train, educate, certify, and professionalize personnel commensurate with their responsibilities to develop, use, operate, administer, maintain, defend DoD Information Systems.” The Marine Corps has subsequently mandated that each IA Chief complete the Information Assurance Technician Course at Twenty-nine Palms, California in order to receive the 0689 Military Occupational Specialty (MOS). HQMC C4 IA has also recommended additional training and certification for IA Chiefs for professional development, although to date these additional training requirements are not directed. Figure 61 provides a summary of these IA Chief training recommendations.

TRAINING	POC
GIAC Security Essentials Certification (GSEC)	SANS.org
GIAC Certified Incident Handler (GCIH)	SANS.org
GIAC Certified Windows Handler (GCFW)	SANS.org
GIAC Certified Intrusion Analyst (GCIA)	SANS.org
GIAC Certified Windows Security Administrator (GCWN)	SANS.org
GIAC Certified Firewall Analyst (GCFW)	SANS.org
GIAC Security Expert (GSE)	SANS.org
Network +	Comptia
Security +	Comptia
Certified Information Systems Security Professional (CISSP)	ISC2.org
Systems Security Certified Practitioner (SSCP)	ISC2.org
GIAC Security Leadership Certification (GSLC)	SANS.org

Figure 61. IA Chief Training Requirements (From Ref. ⁹⁷)

Recommendation: While the above recommended certifications provide foundational and advanced network and security training, WLAN specific training is not included. Certified Wireless Network Administrator (CWNA) certification would provide IA personnel with basic WLAN orientation and fundamental WLAN management skills required to assess wireless networks.

⁹⁷ HQMC C4, (2005), *Information Assurance Chief Training Requirements*.

Recommendation #2: In order to facilitate advanced training opportunities, we recommend the use of mobile training teams (MTTs) to provide on the job training for IA Chiefs in their actual work environments. The MTT concept can provide expert assistance at a very reasonable cost. The MTTs can be staffed from Marine Corps Network Operations Security Command, Defense Information Systems Agency (DISA), or the National Security Agency (NSA). Each of these organizations has the requisite skills to impart advanced WLAN assessment training, not to mention inherent responsibilities for IA training from DoD 8570.1.

Alternative Recommendation: Request an MTT from the Naval Postgraduate School for basic wireless subjects, WLAN security and WLAN vulnerability assessment training. Students and faculty at NPS consistently seek opportunities for real world applications not to mention practical relevance within DoD. These individuals possess the technical acumen and a wide assortment of commercial software and hardware tools at their disposal. The application of these individuals and tools at a decisive point could generate significant interest and energy towards WLAN assessment and security.

3. Special Education Program (SEP) Payback Utilization

Marine Corps Officers graduating NPS normally serve a payback or utilization tour at designated organizations within the Marine Corps. These organizations have individually identified advanced education requirements and provided justification for SEP billet structure within their Table of Organization (T/O). The majority of Marine Corps Officers serve utilization tours in less technical, more managerial roles like program managers or supervisory network positions. While these billets serve critical functions within the Marine Corps, the technical skills learned from two years of an advanced technical education often goes unused.

Recommendation: Assign Marine NPS SEP billet structure to MCNOSC or HQMC C4 IA or other comparable organizations. This structure would bring advanced education and experience with cutting edge technology that is well suited to tackle current WLAN vulnerability challenges faced by these organizations. Organizations with

SEP billet structure could also require specific network security or wireless tracks be completed by students entering those billets. Similar certification requirements are levied upon Contracting and Acquisition SEP students prior to filling Contracting and Acquisition billets. NPS currently offers five Committee of National Security Systems (CNSS) certificates from the Center for Information Systems Security Studies and Research (CISSR). These certificates are sponsored by the National Security Agency (NSA) and exceed national training standards for IA professionals.

Alternative Recommendation: Given the scarcity of SEP billet structure and the difficulty in gaining new SEP structure without removing it from another organization; HQMC C4 IA and MCNOSC could supplement or augment workforce with NPS students seeking thesis research opportunities. These agencies could literally field an entire vulnerability assessment team from three or four students with the appropriate background and training at NPS. These students are searching for relevant subject matter, real world experience, and practical application to match their interest in advanced WLAN research.

4. Increased Investment in WLAN Security and Assessment

There are a tremendous amount of requirements that are now levied upon WLAN implementations within the Marine Corps by DoD Directives (8100.2, 8500.1, 8500.2), DISA's Security Technical Implementation Guide (STIG) and Wireless LAN Security Framework, NIST Wireless Network Security Special Publication 800-48 and USMC IA Operational Standard 014. These regulations are designed to ensure secure wireless transmissions and slow WLAN implementation until security technology matures. Natural inclination would assume that authorized WLAN implementations would be significantly reduced by the infusion of very stringent security requirements. However, the overwhelming majority of our research suggests that authorized WLAN implementation is not slowing down. In fact, our research suggests that an increase in unauthorized WLANs is a direct result of these stringent policies. When an inexpensive and functional technology emerges, the natural inclination is to make use of it in order to increase efficiency without regard to upper-level policies and procedures.

Recommendation: Invest more personnel and resources into developing a mature wireless vulnerability assessment capability within the Marine Corps. Seek expertise from private industry where required. Leverage security agencies within the Department of Defense for assistance until internal vulnerability assessment capability is mature and capable. Leverage NPS students, faculty, and tools to conduct assessments and provide training to IA Chiefs, Network Administrators, and Communications Officers. Increase awareness amongst installation commanders, MSC Commanders, and their respective Communications Officers. These leaders require more training regarding the substantial presence of WLANs and their corresponding threats within and/or adjacent to MCEN resources.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Air Defense, *Air Defense Topology*, <http://www.airdefense.net/products/enterprise.html>,

Retrieved July 22, 2005.

Airwave, *Airwave Product Line Overview*,

http://www.airwave.com/prodserv_products.html, Retrieved July 22, 2005.

Berkeley Varitronics Systems, *Yellowjacket*,

<http://www.bvsystems.com/Products/WLAN/YJ802.11bg/YJ802.11bg.htm>,

Retrieved July 29, 2005.

Bluesocket, *BlueSecure Controllers Tour*,

<http://www.bluesocket.com/products/controllerfamily.html>, Retrieved July 22, 2005.

Cisco Tech Talk: *High-Security, High-Capacity Wireless Networks*,

[http://www.cisco.com/cgi-](http://www.cisco.com/cgi-bin/sreg2/register/banner.pl?LANGUAGE=E&METHOD=E&TOPIC_CODE=2949)

[bin/sreg2/register/banner.pl?LANGUAGE=E&METHOD=E&TOPIC_CODE=2949](http://www.cisco.com/cgi-bin/sreg2/register/banner.pl?LANGUAGE=E&METHOD=E&TOPIC_CODE=2949)

[&PRIORITY_CODE=127750_2](http://www.cisco.com/cgi-bin/sreg2/register/banner.pl?LANGUAGE=E&METHOD=E&TOPIC_CODE=2949), Retrieved July 22, 2005.

Cognio, *ISMS Mobile Datasheet*, http://www.cognio.com/solutions_mobile.html,

Retrieved September 1, 2005.

Cox, John, (2002), Marine Tackle Paperwork with Wireless LAN, *Network World*,

Retrieved August 2, 2005, [http://www.networkworld.com/news/2002/132978_06-](http://www.networkworld.com/news/2002/132978_06-03-2002)

[03-2002](http://www.networkworld.com/news/2002/132978_06-03-2002).

Department of Defense (DOD) Directive 8100.2, (2004), *Use of Wireless Devices,*

Services, and Technologies in the DOD Global Information Grid (GIG).

Department of Defense, Defense Information Systems Agency, (2004), Wireless Security Support Program, *Wireless LAN Security Framework*, (sec. 3, p. 1).

Department of Defense, Defense Information Systems Agency, (2004), Wireless Security Support Program, *Wireless LAN Security Framework*, (sec. 2, p. 1).

Etter, Andrew, (2002) *A Guide to Wardriving and Detecting Wardrivers*, SANS Institute, <http://www.sans.org/rr/whitepapers/wireless/>, Retrieved September 3, 2002.

Fortress Technologies, *Fortress Enterprise Brochure*, <http://www.fortresstech.com/products/af2100.shtml>, Retrieved July 22, 2005.

Fortress Technologies, *Mobile LANs, Wireless Combat Information Systems Security*, <http://www.fortresstech.com/solutions/government.shtml>, Retrieved July 22, 2005.

Fulp, J.D., (2004), Center for Information Systems Security Studies and Research, *Course Notes for CS3690 Network Security*, Naval Postgraduate School.

Harris Secure Communications, *Secure Wireless Local Area Network*, http://download.harris.com/app/public_download.asp?fid=843, Retrieved August 6, 2005.

Hoskins, Robert, (2005), CMC's New Wi-Fi Virtual Station Emulator Enables Load Testing of 802.11 Devices and WLAN Systems, *Broadband Wireless Exchange Magazine*, Retrieved August 31, 2005, <http://www.bbwexchange.com/news/2003/may/cmc052103.asp>.

HQMC C4, (2005), *Information Assurance Chief Training Requirements*.

HQMC C4, (2005), *Information Assurance Toolkit Software Suite*.

Hughes, Dennis, (1997, February 3), Outsider Threats, *Fortune*, p.27.

IEEE, *IEEE 802.15 WPAN Task Group 1*, <http://www.ieee802.org/15/pub/TG1.html>,

Retrieved August 19, 2005.

iPass, *Virtual Network Platform*, http://www.ipass.com/platform/platform_demo.html,

Retrieved July 22, 2005.

Joint Wireless Administrator Checklist, Version 1.0, <http://iase.disa.mil>, Retrieved

August 22, 2005.

Kismet, *Documentation*, <http://www.kismetwireless.net/documentation.shtml>, Retrieved

September 1, 2005.

Knoppix, *Knopper.net*, <http://www.knoppix.org>, Retrieved September 3, 2005.

Mairs, John, (2002), *VPNs: A Beginner's Guide*, New York; McGraw-Hill Osborne.

Marine Corps Systems Command, (2001), *STRATIS Secure System Authorization Agreement Outline*.

Maui X-Treme Inc., *VX30 Encoder*,

<http://www.mxsinc.com/pages.php?cid=MDEwMDA0MDQy>, Retrieved July 22, 2005.

National Institute of Standards and Technology (NIST), (2002), *Wireless Network Security; 802.11 Bluetooth and Handheld Devices*, (Special Publication 800-48).

National Institute of Standards and Technology (NIST), (2002), *Wireless LAN Security Framework Addendum to the Wireless Security Technical Implementation Guide*,

(Special Publication 800-48), Wireless LAN Security Checklist,

<http://iase.disa.mil/wireless/index.html>, Retrieved August 18, 2005.

PHLAK, *Professional Hacker's Linux Assault Kit*, <http://www.phlak.org/modules/news/>,

Retrieved September 3, 2005.

PHLAK, *Professional Hacker's Linux Assault Kit*,

<http://www.phlak.org/modules/sections/>, Retrieved September 3, 2005.

Planet3 Wireless Inc., (2005), *Certified Wireless Network Administrator (CWNA) Study Guide*, New York; McGraw-Hill Osborne.

Remote Exploit, *Auditor*, http://new.remote-exploit.org/index.php/Auditor_main,

Retrieved September 2, 2005.

Remote Exploit, *Research Kismet Primer Guide*, [http://new.remote-](http://new.remote-exploit.org/index.php/Research)

[exploit.org/index.php/Research](http://new.remote-exploit.org/index.php/Research), Retrieved September 1, 2005.

SearchMobileComputing.com, *Definitions*,

http://searchmobilecomputing.techtarget.com/sDefinition/0,290660,sid40_gci961342,00.html, Retrieved August 8, 2005.

Senforce, *Security Client*, <http://www.senforce.com/prodendsuite.htm>, Retrieved July 28, 2005.

SG Automation, (2000), *STRATIS Functional Description*.

Softpedia, *Knoppix STD 0.1*, Encryption screenshot, Retrieved September 3, 2005.

The United States Computer Emergency Readiness Team (US-CERT), Vulnerability Note VU#106678, <http://www.kb.cert.org/vuls/id/106678>, August 8, 2005.

Undisker, *Open, Create and Extract ISO files*, <http://www.undisker.com/creating-iso-images.html>, Retrieved September 2, 2005.

United States Marine Corps (USMC) Information Assurance Operational Standard, (2005), *014 Wireless Local Area Networks V 1.0*, (USMC IA OPSTD 014).

Vladimirov, A.A., Gavrilenko, K.V., Mikhailovsky, A.A., (2004), *WI-FOO: The Secrets of Wireless Hacking*, (chap. 8, pp. 192-197), Addison-Wesley.

Vocera Communications, *Products*, <http://www.vocera.com/products/products.shtm>, Retrieved July 22, 2005.

Watts, Jeffrey, STRATIS message from Headquarters Marine Corps C4/IA, STRATIS Wireless Networking Configuration, July 2004.

WikiPedia, *The Free Encyclopedia*, <http://en.wikipedia.org/wiki/Encryption>, Retrieved July 27, 2004.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California
3. Marine Corps Representative
Naval Postgraduate School
Monterey, California
4. Chairman, Department of Information Sciences
Naval Postgraduate School
Monterey, California
5. Director, Training and Education, MCCDC, Code C46
Quantico, Virginia
6. Director, Marine Corps Research Center, MCCDC, Code C40RC
Quantico, Virginia
7. Marine Corps Tactical Systems Support Activity (Attn: Operations Officer)
Camp Pendleton, California