NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

WIRELESS SECURITY WITHIN HASTILY FORMED NETWORKS

by

Bryan L. Bradford

September 2006

Thesis Advisor:	Carl Oros
Second Reader:	Brian Steckler

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

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 2006	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Wireless Security within Hastily Formed Networks	**5. FUNDING NUMBERS**
6. AUTHOR Major Bryan L. Bradford	
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)

One of the main purposes of a Hastily Formed Network (HFN) is to provide immediate access to networked voice, data, and video services for as many users as possible. Following terrorist attacks like those in September 2001 or devastating natural disasters like the December 2004 Indian Ocean Tsunami and Hurricane Katrina in August 2005 users of the HFN will likely include survivors; first responders; local, state, and federal government agencies; non-government organizations; militaries; and others. These varied users will have different purposes for accessing HFN services; some will require their information to remain private while others will not. These needs for privacy and openness appear to present conflicting requirements: provide unrestricted access for many users but ensure "privacy" or security of at least some information within the network. The purpose of this thesis is three-fold: first, to explore methodologies for securing the HFN; second, to examine commercial off-the-shelf (COTS) products and accepted best practices that provide the necessary security; and third, to provide a limited implementation example and a more robust target architecture that could provide security on the wireless segments while maintaining open access to the HFN and minimizing installation, operation, and maintenance complexity.

14. SUBJECT TERMS Wireless Security, WLAN Security, Hastily Formed Network (HFN), Complex Humanitarian Disaster (CHD)	**15. NUMBER OF PAGES** 113
	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 SECURITY WITHIN HASTILY FORMED NETWORKS

Bryan L. Bradford
Major, United States Air Force
B.S., Texas A&M University, 1991
M.A., Bellevue University, 2000

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS AND OPERATIONS

from the

NAVAL POSTGRADUATE SCHOOL
September 2006

Author: Bryan L Bradford

Approved by: LtCol Carl Oros
Thesis Advisor

Brian Steckler
Second Reader

Dr. Dan Boger
Chairman, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

One of the main purposes of a Hastily Formed Network (HFN) is to provide immediate access to networked voice, data, and video services for as many users as possible. Following terrorist attacks like those in September 2001 or devastating natural disasters like the December 2004 Indian Ocean Tsunami and Hurricane Katrina in August 2005 users of the HFN will likely include survivors; first responders; local, state, and federal government agencies; non-government organizations; militaries; and others. These varied users will have different purposes for accessing HFN services; some will require their information to remain private while others will not. These needs for privacy and openness appear to present conflicting requirements: provide unrestricted access for many users but ensure “privacy” or security of at least some information within the network. The purpose of this thesis is three-fold: first, to explore methodologies for securing the HFN; second, to examine commercial off-the-shelf (COTS) products and accepted best practices that provide the necessary security; and third, to provide a limited implementation example and a more robust target architecture that could provide security on the wireless segments while maintaining open access to the HFN and minimizing installation, operation, and maintenance complexity.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ABBREVIATIONS AND ACRONYMS

ACRONYM	DEFINITION
3DES	Triple Data Encryption Standard
AAA	Authentication, Authorization, and Accounting
AES	Advanced Encryption Standard (used in CCMP)
CBC-MAC	Cipher-Block Chaining with Message Authentication Code
CCMP	Counter Mode with CBC-MAC Protocol (based on AES)
CHD	Complex Humanitarian Disaster
CONOPS	Concept of Operations
COTS	Commercial Off-The-Shelf
CWNP	Certified Wireless Network Professionals
DES	Data Encryption Standard
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
EOC	Emergency Operations Center
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
FLAK	Fly Away Kit
HA/DR	Humanitarian Assistance / Disaster Relief
HFN	Hastily Formed Network

ACRONYM	**DEFINITION**
HMC	Hancock Medical Center
HWIC	High-speed Wide Area Network Interface Card
IA	Information Assurance
IOS	Internetwork Operating System (Cisco)
IP	Internet Protocol
IPSec	Internet Protocol Security
ISR	Integrated Services Router (Cisco)
L2TP	(OSI) Layer 2 Tunneling Protocol
LAN	Local Area Network
LWAP	Lightweight Access Point
LWAPP	Lightweight Access Point Protocol
MAC	Medium Access Control
Mbps	Megabits per second
MRF	Mobile Research Facility
NAVO	Naval Oceanographic Center
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NPS	Naval Postgraduate School
OS	Operating System
OSI	Open Systems Interconnect
PPTP	Point-to-Point Tunneling Protocol
RADIUS	Remote Authentication Dial-In User Service
ROI	Return on Investment

ACRONYM	DEFINITION
SATCOM	Satellite Communications
SOP	Standard Operating Procedure
SSH / SSH2	Secure Shell / version 2
SSID	Service Set Identifier
SSL	Secure Sockets Layer
TKIP	Temporal Key Integrity Protocol
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VoIP	Voice Over Internet Protocol
VPN	Virtual Private Network
WAP	Wireless Access Point
WEP	Wired Equivalent Privacy
WIDS	Wireless Intrusion Detection System
Wi-Fi	Wireless Fidelity
WIPS	Wireless Intrusion Prevention System
WLAN	Wireless Local Area Network
WLCM	Wireless LAN Control Module
WPA	Wi-Fi Protected Access
WPA2	Wi-Fi Protected Access 2
WPA-PSK	WPA Pre-Shared Key

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I owe thanks to many people. First, to my wife and daughter for their support during my time at NPS and the two PCS moves they endured in 12 months.

Thanks to my thesis advisor LtCol Carl Oros for his mentorship and guidance throughout my program.

Thanks to Brian Steckler for allowing me the opportunity to deploy with the NPS HFN team and for his guidance as my second reader.

Thanks to all my other instructors for their assistance and mentorship.

Thanks to Dr. Dan Boger, Lt Col Karl Pfeiffer, Ray Elliot, and Steve Iatrou for their advice and assistance.

Last, but certainly not least, thanks to Jim and Anne Hall who gave me a place to stay and fed me during my final quarter after my family had already moved on.

THIS PAGE INTENTIONALLY LEFT BLANK

DISCLAIMER

The software and hardware evaluations conducted within this research represent a limited assessment based on the specific criteria established by the author. The opinions expressed within this document solely represent the opinions of the author 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

I. INTRODUCTION

A. BACKGROUND

There have been numerous natural disasters in the last two years. Two of the largest were the December 26, 2004 Indian Ocean tsunami and the two devastating hurricanes that hit the U.S. Gulf Coast in late August and mid-September of 2005. The United States provided humanitarian assistance and disaster relief (HA/DR) in many ways to the victims of these Complex Humanitarian Disasters (CHD). A team of faculty and students from the Naval Postgraduate School (NPS) participated directly in relief of the Indian Ocean Tsunami and Hurricane Katrina victims by installing, operating, and maintaining Hastily Formed Networks (HFN) in Thailand and Mississippi. Each HFN consisted of satellite communications (SATCOM) and wireless network equipment that allowed disaster victims to make phone calls, send email, or use the Internet to contact loved ones and to file claims with the government. The author was a member of the team that assisted the victims of Hurricane Katrina. The following is a short summary of the situation the team faced and the support provided. [1]

On the morning of August 29, 2005, Hurricane Katrina came ashore along the Gulf Coast of Mississippi and Louisiana as a Category 4 storm. A few days later, NPS sent a team of faculty and students, along with the NPS Nemesis Mobile Research Facility (MRF)[2], to provide assistance to the Naval Oceanography Center (NAVO) at Stennis Space Center, MS. The intent was to use the Nemesis MRF and commercial off-the-shelf (COTS) gear to bring NAVO back online with SATCOM-based Internet access and provide voice, data, and video communications capabilities as soon as possible.

Upon arriving, the NPS advance team found that NAVO no longer needed help and the team was tasked to assist the Hancock County, MS, Emergency Operations Center (EOC). The EOC assigned the NPS team to assist in restoring communications

[1] See Steckler, Bradford, & Urrea (2005). This is an extensive lessons learned and after action report about the NPS efforts supporting Hurricane Katrina victims and provides much more detail. The full text of this report is available at http://www.nps.navy.mil/disasterrelief/docs/NPS-Katrina_AAR_LL.pdf with additional information about NPS's disaster relief programs at http://www.nps.navy.mil/disasterrelief.

[2] NPS Nemesis MRF is a 33-foot Class A Motor home converted for wireless networks research & operations support.

for the Hancock Medical Center (HMC), local government offices, police and fire stations, temporary emergency services locations, and relief shelters in the disaster stricken areas of Bay St. Louis and Waveland, MS. Figure 1 shows several pictures taken by team members of the scene that greeted the team upon arrival.

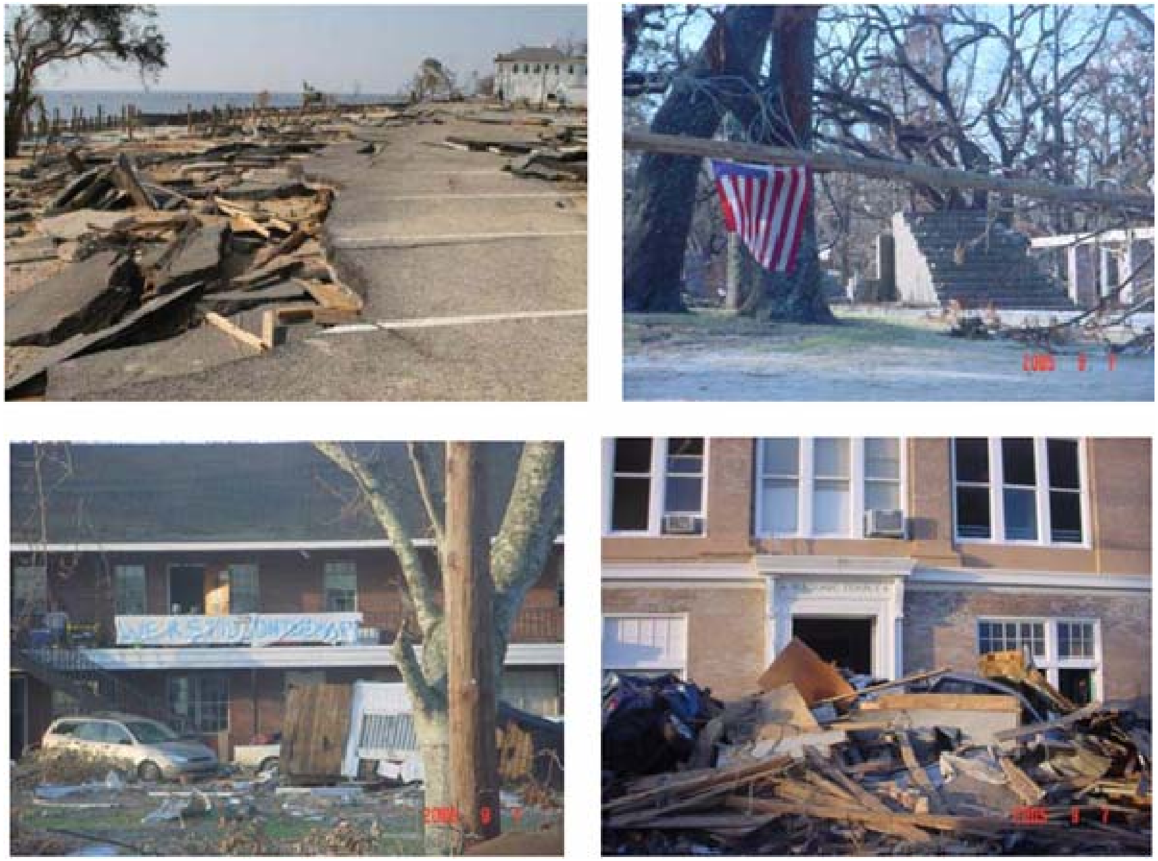


Figure 1. Photos of Devastated Areas in Bay St. Louis and Waveland, MS (From Steckler, Bradford, and Urrea, 2005)

Figure 2 shows the map of where the team installed the HFN and its relative location to New Orleans, LA.

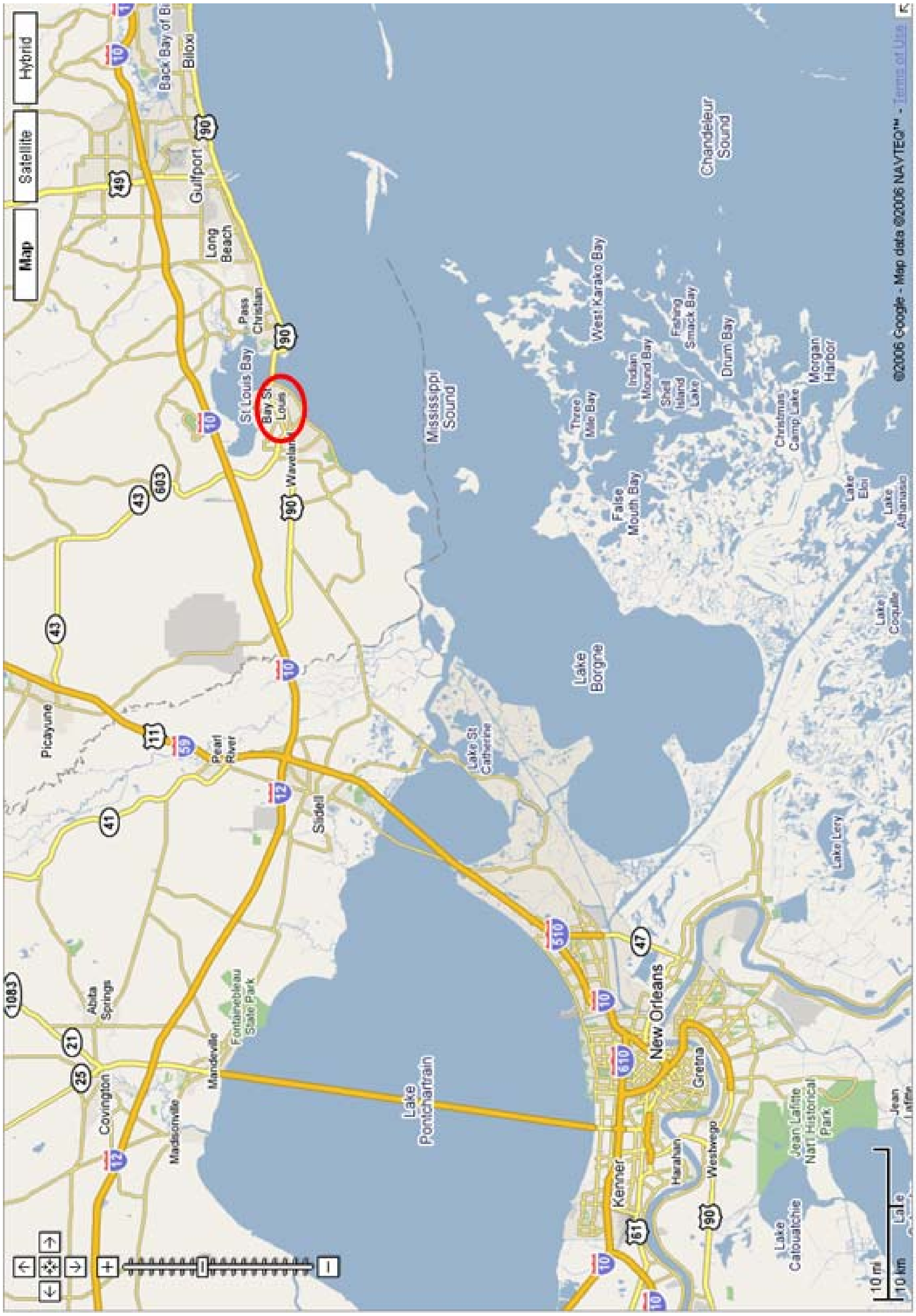


Figure 2. Map Showing NPS HFN Location[3]

[3] Map courtesy of Google Maps.

NPS teamed with the Office of the Assistant Secretary of Defense/Networks and Information Integration and several vendors (Cisco, Microsoft, Redline, and Mercury Data Systems) to create the first and only official and publicly accessible wireless network in an area that suffered virtually 100% disruption of all communications capabilities. The NPS-led team of industry and Department of Defense (DoD) entities successfully integrated key wireless technologies (e.g., 802.11, 802.16, SATCOM, Voice Over Internet Protocol [VoIP]) in the disaster zone, bringing the first Internet connectivity and dial-tone telephony to the entire region. First responders, many local hurricane survivors, relief agencies, city/county government officials, and hundreds of volunteers were able to communicate with the outside world for the first time as a result of the HFN this team set up.

The team worked quickly to establish the HFN by installing SATCOM and wireless equipment using the HMC parking lot as a base of operations. They had this first node of the network up within 5 hours of arrival providing voice and data communications for myriad agencies that had set up for emergency operations in the HMC parking lot (including the Federal Emergency Management Agency [FEMA], the Federal protective Service, Florida’s Disaster Medical Assistance Teams, National Guard Emergency Medical and Security units, a Disaster Mortuary Operational Response Team, regional ambulance service providers, and the medical center staff). In the next few days, the team systematically connected other key locations (e.g., food distribution points, public shelters, emergency facilities, and government buildings) via 802.16 WiMAX technology (see Figure 3).

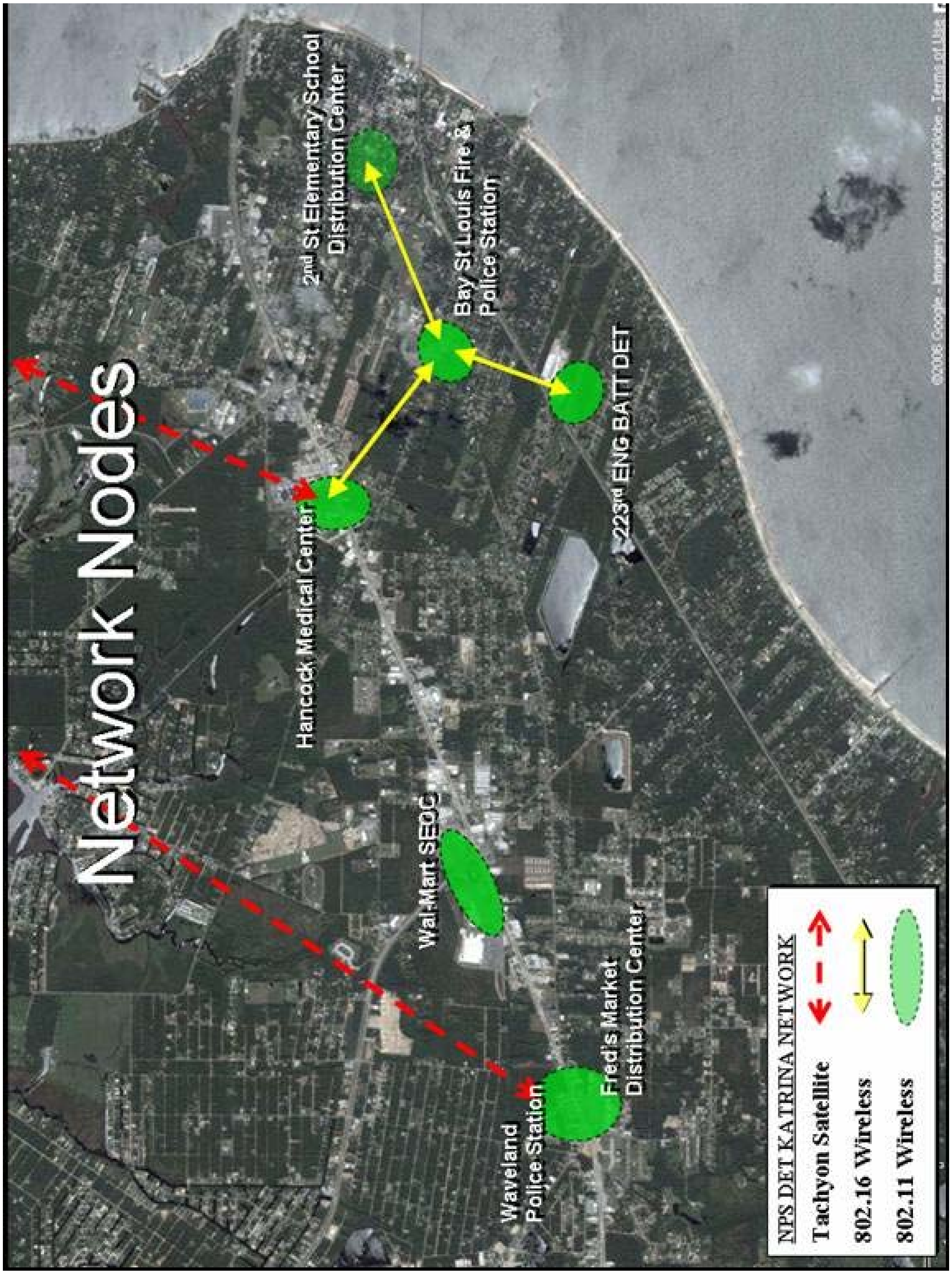

Network Nodes
2nd St Elementary School Distribution Center
Bay St Louis Fire & Police Station
223rd ENG BATT DET
Hancock Medical Center
Wal-Mart SEOC
Fred's Market Distribution Center
Waveland Police Station
NPS DET KATRINA NETWORK
Tachyon Satellite
802.16 Wireless
802.11 Wireless
©2006 Google - Imagery ©2006 DigitalGlobe - Terms of Use

Figure 3. NPS HFN Nodes (From Steckler, Bradford, & Urrea, 2005)[4]

[4]. Image courtesy of Google Maps.

Figure 4 shows a more detailed diagram of the HFN. It includes the SATCOM, 802.16 and 802.11 wireless, and management equipment.

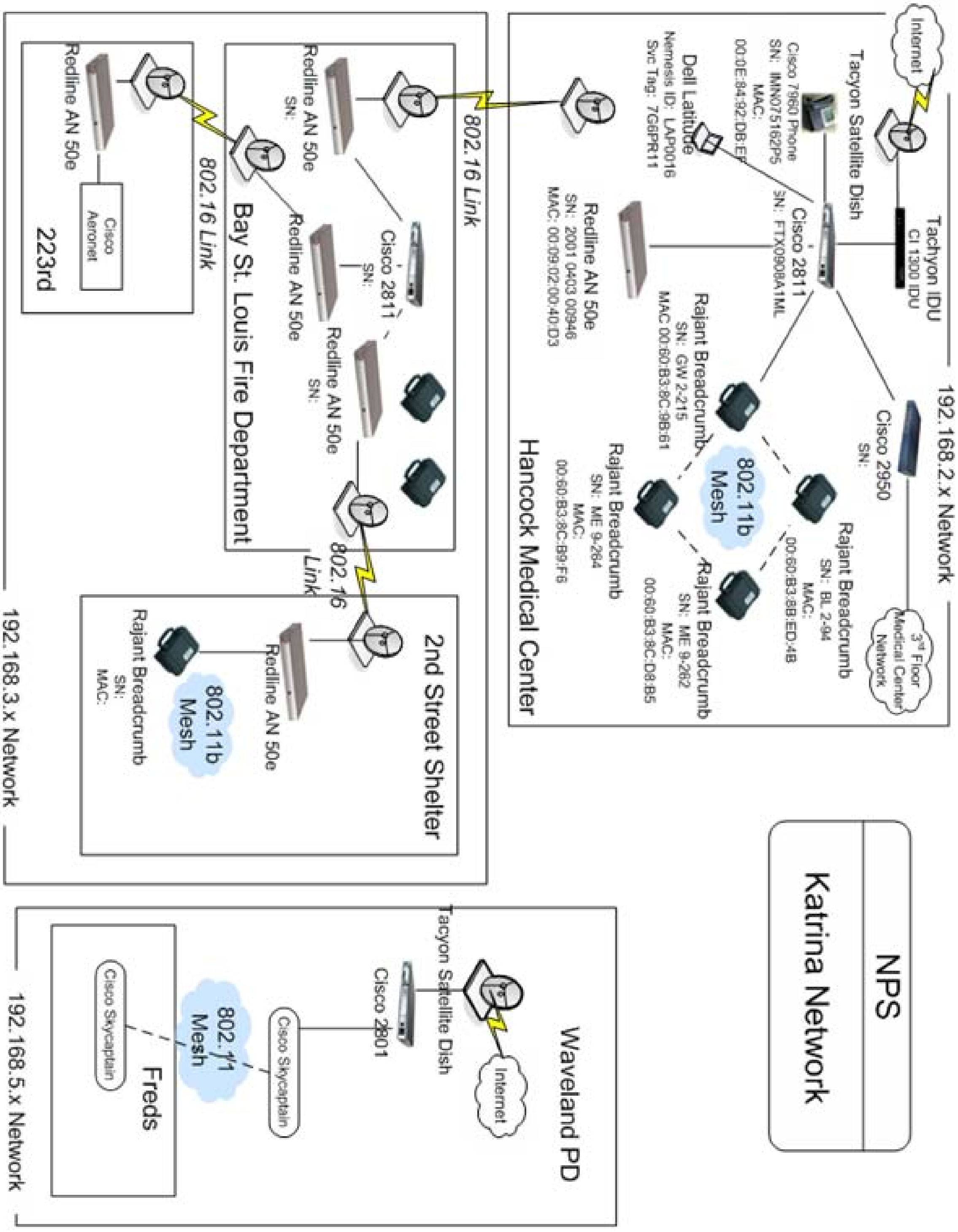


Figure 4. Hurricane Katrina HFN Architecture (From Steckler et al., 2005)

The NPS-led team operated and maintained these networks until September 30, 2006 when FEMA contracted for an outside vendor to first maintain and then replace NPS' HFN equipment. The installation, operation, and maintenance of this HFN provided a much needed service that assisted thousands of victims, first responders, volunteers, and local, state, and federal government officials. But, did these networks also allow bad people to take advantage of these victims?

B. SHOULD A DISASTER RELIEF HFN BE SECURE?

The author has no direct evidence that anyone abused or misused the network either in Thailand or Mississippi, but there was nothing in place to detect or prevent such abuse if anyone wanted to try. NPS deployed these HFNs with no wireless security measures for several reasons: 1) the HFN program at NPS is still evolving; 2) there was no existing security Concept of Operations (CONOPS) for deployment of the HFN gear; and 3) during implementation, the desire for maximum user support and minimum management complexity overrode the requirement for security. Anyone willing to put in the time could take advantage of vulnerabilities within this type of network and gain access to any information. This begs the question: should an HFN even be protected?

DoD Directive (DoDD) 8500.1, *Information Assurance (IA)*, paragraph 4.2 states

> All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets; documented threats and vulnerabilities; the trustworthiness of users and interconnecting systems; the impact of impairment or destruction to the DoD information system; and cost effectiveness.

According to paragraph 4.1 of DoDD 8100.2, *Use of Commercial Wireless Devices, Services, and Technologies in the DoD Global Information Grid*, wireless devices that connect to DoD networks are part of those networks and must conform to DoDD 8500.1 and DoD Instruction (DoDI) 8500.2, *Information Assurance Implementation*. The "catch" is the HFNs deployed in Thailand and Mississippi did not directly connect to any DoD networks. Therefore, they were not subject to DoD policies per se; so, why bother to protect the networks?

As Dodd (2005) points out, wireless network security is a serious issue users must address to maintain their privacy and protect their data. In an informal study the author conducted, the conclusions indicated an attacker will likely attack a wireless network, even if it is secured, if he/she believes there may be some profit and will absolutely attack an unprotected network (if for no other reason than just for fun). Refer to Chapter II for full details. Therefore, if network exploitation/attack is likely or imminent, what information needs to be protected?

C. WHAT INFORMATION NEEDS TO BE PROTECTED?

The reader may ask what information needs to be protected in these scenarios where the focus is all about helping the victims. In short, there are many types of information within an HFN that potentially need to be protected from both the casual observer and the potential adversary. First, the identity of victims and their private information should be protected to prevent identity theft (e.g., someone could monitor the unprotected HFN and "steal" the identity of a victim then collect the FEMA disaster checks). Second, first responder communications may need to be private (especially when talking about medical and force protection issues). Third, information about where relief supplies may be delivered or stock piled should be protected to prevent unauthorized interception or theft of supplies. In Indonesia, there were claims the Gerakan Acheh Merdeka rebels were hijacking relief supplies in early January, 2005[5]. These rebels could easily get this type of information from an unprotected network. Finally, in Mississippi, after Hurricane Katrina, the NPS team used the HFN for its only means of data communication with higher headquarters. This means that all emails sent from the deployed team to Joint Task Force Katrina, NPS staff and faculty, indeed anyone, flowed across this unsecured HFN.

In summary, unprotected networks are easy targets. Attackers may even attempt to penetrate protected networks if they think the payoff is big enough. Additionally, there is information within the HFN that warrants protection. Therefore, it behooves the information security professional to take steps to secure HFNs, even those set up for disaster relief. When properly secured, these networks will have the IA attributes of

[5] CBS News online article, http://www.cbsnews.com/stories/2005/01/12/world/main666295.shtml, Retrieved January 2006

confidentiality, integrity, authentication, non-repudiation, and availability of information as required by DoDD 8500.1. The next section provides definitions of these IA terms so the reader understands how having these attributes is beneficial.

D. DEFINITIONS OF IA TERMS[6]

1. Confidentiality

Assurance that information is not disclosed to unauthorized individuals, processes, or devices.

2. Integrity

In a formal security mode, integrity is interpreted to mean protection against unauthorized modification or destruction of information.

3. Authentication

Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information.

4. Non-repudiation

Assurance the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

5. Availability

Timely, reliable access to data and information services for authorized users.

E. SCOPE OF WORK

Some would argue that non-repudiation is a derived attribute[7] (i.e., a mix of authentication and integrity) and this author will not debate that issue here. In addition, availability, while a highly desirable attribute of any network, is beyond the scope of this thesis. Therefore, this thesis will focus on security mechanisms that address the first three of these attributes: confidentiality, integrity, and authentication. Furthermore, the security mechanisms investigated for this thesis apply primarily to the 802.11 wireless equipment within the HFN. Some products reviewed do provide security for other protocols such as 802.16 and those are noted where applicable.

[6] Committee on National Security Systems Instruction 4009, National IA Glossary, revised May 2003.

[7] NPS (2005) Course Notes for CS3690: Network Security, Instructor: J. D. Fulp, Section 3, slide 7

F. THESIS STRUCTURE

The remainder of this thesis is organized as follows:

Chapter II, To Secure or Not Secure: Is That the Question? This Chapter is an extract of a paper the author wrote in partial fulfillment of a modeling course. It models the “conflict” between an information security professional and an attacker and provides an analysis of the potential for attack in various situations. It concludes that an unprotected network is virtually guaranteed to be attacked and one that has security mechanisms in place is likely to be attacked if the value of the information within is tempting enough to the attacker.

Chapter III, Securing an HFN, presents two methods for securing an enterprise wireless network that can be applied to the HFN Scenario. The first method comes from a white paper by AirDefense and suggests a three-step approach: securing the end points, securing the communications channels, and monitoring for security and compliance. The second method, from Motorola, uses a holistic approach and recommends incorporating people, policy, process, and technology into the wireless security architecture. A sample WLAN security policy template courtesy of Planet 3 Wireless is included as Appendix A.

Chapter IV, Review of COTS Products, provides a summary of the various COTS products reviewed. The products are categorized based on the first method mentioned in Chapter III as well as which Open Systems Interconnect (OSI) layer they most closely fit in. If a product is Federal Information Processing Standard (FIPS) 140-2 validated or Common Criteria certified it is so noted. In addition, each product is assessed as to which of the IA attributes of confidentiality, integrity, and authentication it supports. The chapter also provides with a detailed description of each product or product category the author reviewed.

Chapter V, A Secure Wireless Architecture for HFNs, begins with an example of an actual implementation of some of the wireless security principles introduced in previous chapters using some of the products listed in Chapter IV. This implementation focuses primarily on securing the wireless communications path. Next, this chapter provides a target wireless architecture that could be used to include security of end devices and monitoring of the network.

Chapter VI, Conclusions, provides a summary of the key findings, some concluding remarks, and a brief discussion of areas for future work.

THIS PAGE INTENTIONALLY LEFT BLANK

II. TO SECURE OR NOT TO SECURE: IS THAT THE QUESTION?

The following is an extract from a paper focused on modeling the IA decision of whether or not to purchase security hardware and/or software or take other steps to secure an HFN being used in support of a Complex Humanitarian Disaster (CHD) (e.g., Indian Ocean Tsunami, Hurricane Katrina).[8] This paper attempted to develop theoretical payoffs for the defender and attacker and showed a two-person zero-sum game. Based on the likely outcome of the game, the defender is faced not with the decision of whether or not to provide security, but how much security to implement. This decision is based on certain variables including: the value of the information needing to be protected, the perceived threat of attack, the vulnerabilities on the network itself, the estimated cost of providing safeguards on the network, and the potential return on investment. Ultimately, the decision maker must choose a way to minimize the risk to the information subject to constraints of budget, equipment, and personnel.

A. THE MODEL: A TWO-PERSON, ZERO-SUM, NON-COOPERATIVE GAME

Assume the IA professional and an adversary are players in a two-person game. This model will refer to the IA professional as the “Good Guy” and the adversary as the “Bad Guy”. They each have opposing goals with respect to information within the target network. The Good Guy wants to ensure the confidentiality, integrity, and authenticity of certain (or all) information. The Bad Guy wants to gain easy access to that information in the hopes of exploiting it for personal gain (or maybe just for the fun of it). The Good Guy can secure or not secure the system and the Bad Guy can attack or not attack.

1. Good Guy Choices

Table 1 shows the Good Guy’s preferred outcomes from best (4) to worst (1), based on effort (Low, High) and possible outcomes (Success, Fail), where success means no information is exploited and failure means the Bad Guy got in and exploited the information.

[8] The paper was written by the author in partial fulfillment of course requirements for SO4410: Models of Conflict, December 15, 2005 and is included here with slight modification..

Table 1. Good Guy Desired Outcomes

Utility	Definition
4	Best Case: don’t secure, no attack (means no money, time or effort expended on securing the network and no attack)
3	Next Best Choice: secure, no attack (means some amount of money, time and effort expended securing the network and no attack)
2	Next Choice: secure, attack (means some amount of money, time and effort expended securing the network and information may be exploited)
1	Worst Case: don’t secure, attack (means no money, time or effort expended on securing the network and information **is** exploited)

It is difficult to assign actual utilities of these rankings due to the many variables involved. Therefore, this paper will assume the ordinal and cardinal utilities are equal.

Figure 5. Good Guy Utility Scale

2. Bad Guy Choices

Table 2 shows the utilities, in order from best (4) to worst (1) for the Bad Guy based on the effort (Low, High) and possible outcomes (Succeed, Fail), where success means information is exploited and failure means the Good Guy protected the system and no information is exploited. One will notice these are the opposite of the views of success and failure the Good Guy had.

Table 2. Bad Guy Desired Outcomes

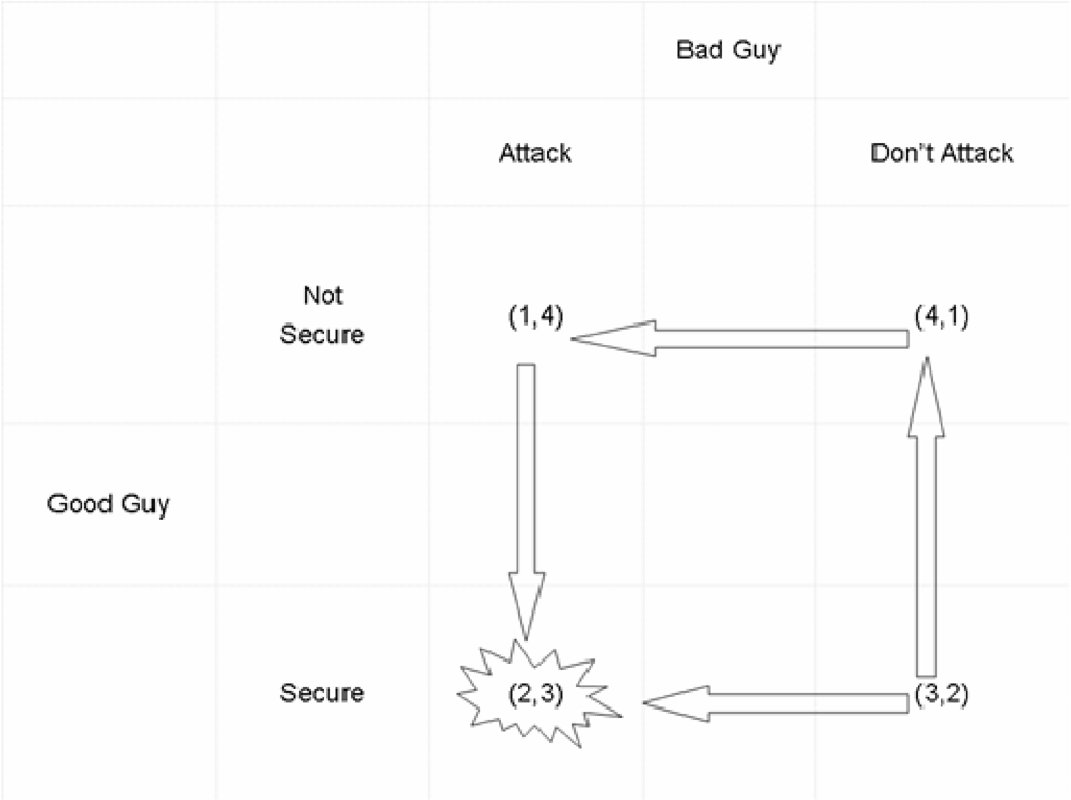
Utility	**Definition**
4	Best Case: attack, not secure (means the attacker had to expend little money, time or effort attacking the network and information is exploited since there was no security)
3	Next Best Choice: attack, secure (means the attacker expends a lot of money, time or effort on attacking the network, but is able to gain access and information is exploited)
2	Next Choice: no attack, secure (no attack = no information)
1	Worst Case: no attack, no secure (no attack = no information even though it wasn't protected)

Again, it is difficult to assign actual utilities of these rankings due to the many variables involved. Therefore, this paper will assume the ordinal and cardinal utilities are equal.

Figure 6. Bad Guy Utility Scale

3. The Game

Based on the desired outcomes above, a two-person game develops with a matrix as shown in Figure 7.



		Bad Guy	
		Attack	Don't Attack
Good Guy	Not Secure	(1,4)	(4,1)
	Secure	(2,3)	(3,2)

Figure 7. Good Guy vs. Bad Guy

Based on the assigned utilities, a Nash Equilibrium[9] appears at (2, 3) – Good Guy secure, Bad Guy attack. In fact, the Bad Guy has a dominant strategy to attack no matter what the Good Guy does. In reality, this is perfectly logical since the attacker can easily succeed if the Good Guy does not secure the network and might succeed even against a "secure" network. For the Good Guy, there is no dominant strategy as depicted in the matrix. However, the "Not secure, don't attack" outcome is not very likely and the "Not secure, attack" outcome is one the Good Guy cannot withstand. Therefore, the likely outcome is the Bad Guy will attack (his dominant strategy) and the Good Guy better secure the network. The next section provides a framework to help determine how much security is necessary to minimize the potential loss.

[9] **Definition:** Nash equilibrium are sets of strategies for players in a no cooperative game such that no single one of them would be better off switching strategies unless others did. .
Online Economics Glossary, http://economics.about.com/cs/economicsglossary/g/nashequilibrium.htm, Retrieved August 28, 2006.

B. THE DECISION

According to the Internet Storm Center the average time between attacks is 19 minutes.[10] An article on the website www.theregister.co.uk refers to a recent attack against the online security systems of a Christian charity in the United Kingdom.[11] The model shown in this paper concludes an adversary's dominant strategy is to attack no matter what the Good Guy does. Given these facts, one can easily conclude the Bad Guy will attack an HFN. Therefore, the Good Guy must determine the level of protection necessary to make the risk of attack "acceptable". In modeling this, the Good Guy wants to minimize risk subject to constraints of budget, manpower, and equipment. One method of analyzing risk is shown below.

1. Decision Variables

With respect to information assurance, the decision maker must balance the risks of having information compromised or exploited with the costs of securing the network. One way of illustrating this is reflected in the "IA Equation" shown below:[12]

$$\text{Residual Risk} = (\text{Threats} \times \text{Vulnerabilities} \times \text{Information Value}) - \text{Safeguards}$$

The product of threats X vulnerabilities X information value represents the risk to the network. The IA practitioner's job is to get the residual risk to an acceptable level. The definition of "acceptable" will be dependent on the situation. One method for performing this calculation is to assign a dollar value to each of these variables. Then, the decision point occurs when the residual risk level is equal to or below the amount the decision maker is willing to pay. However, assigning dollar amounts to these variables is non-trivial and beyond the scope of this paper. This paper will explain each of the variables and address the relative relationships among them.

a. Threats (Will Someone Want to Attack and Why?)

This is the least controllable variable in the equation. Threats can be categorized in various ways. One method is to classify them based on the attribute of IA that is being attacked: confidentiality, integrity, authenticity, or availability. A second

[10] SANS Internet Storm Center, http://isc.sans.org/ Last accessed December 10, 2005.

[11] The Register Web Site, http://www.theregister.co.uk/2005/12/12/charity_hack/, Last accessed November 20, 2005.

[12] NPS (2005) Course Notes for CS3690: Network Security, Instructor: J. D. Fulp, Section 3, slide 8

method provides categories such as human error, abuse of authority, direct probing, probing with malicious software, direct penetration, or subversion of security mechanism. These various threats are perpetrated by two main types of attackers (professionals and amateurs) who can perform their attacks from inside or outside your network. For an extensive discussion of Wireless Local Area Network (WLAN) threats and vulnerabilities as well as basic WLAN security principles see Kessel and Goodwin (2005).[13]

As the previous modeling points out, there is a high likelihood of some sort of attack. In the context of HFN for CHD, the type of attack is difficult to classify. The various types of attacks mentioned each present a different level of severity (or potential damage) and each have a different probability of happening. This probability is dependent on the situation and requires further study.

b. Vulnerabilities (What are the Known Weaknesses?)

Vulnerabilities represent the attributes of a system's design that result in the potential for intentional or accidental problems.[14] Once identified, there are well known ways to reduce various vulnerabilities. The vulnerabilities of the HFN in the context of a CHD have not been extensively studied and require further research.

c. Information Value (What are We Protecting?)

Information in the context of a CHD has different value to different users. As previously mentioned, there is information within the network that should only be visible to certain individuals. Exactly what information is this? How does one determine the value of this information? The answers to these questions are dependent on the exact situation. The information owner must determine the value and whether or not the information should be protected.

d. Costs of Safeguards (Hardware, Software, Time)

Safeguards are the countermeasures applied to a system "after the fact" that attempt to mitigate the risk (threat X vulnerabilities X information value). Protecting a network's information from unauthorized access and unwanted tampering can be done in many ways. These methods can be relatively inexpensive or very expensive and may involve hardware, software, and additional personnel. How much of each to use will be

[13] Kessel and Goodwin, (2005), Chapters II & III.

[14] NPS (2005) Course Notes for CS3690: Network Security, Instructor: J. D. Fulp, Section 3, slide 10

constrained by the budget. The IA professional must factor in the costs associated with each chosen security measure and weigh this as a decision variable. One method for performing this analysis is looking at the return on investment (ROI) of each proposed solution as indicated in the equation below.

$$\text{ROI} = \frac{(\$\text{Expected loss without safeguard} - \$\text{Expected loss with safeguard} - \$\text{Cost of safeguard})}{\$\text{Expected loss without safeguard}}$$

This will yield an ROI value between 0 and 1. The closer a solution is to 1, the better it is. The IA professional can then compute the ROI for each security measure.

2. Putting It All Together

The IA professional now has a methodology to follow to determine which threats to protect against, vulnerabilities to close, value of the information to be protected, and the cost of implementing various security measures. While this may sound simple, it requires significant work to "crunch the numbers" and is highly dependent on the specific implementation of the network being secured. The key is to get the optimal level of security at the minimal cost. Motorola (2006, p. 4) states "an effective risk-management approach to security balances the costs of security measures against the potential costs of the breaches they are designed to prevent." Figure 8 illustrates this tradeoff.

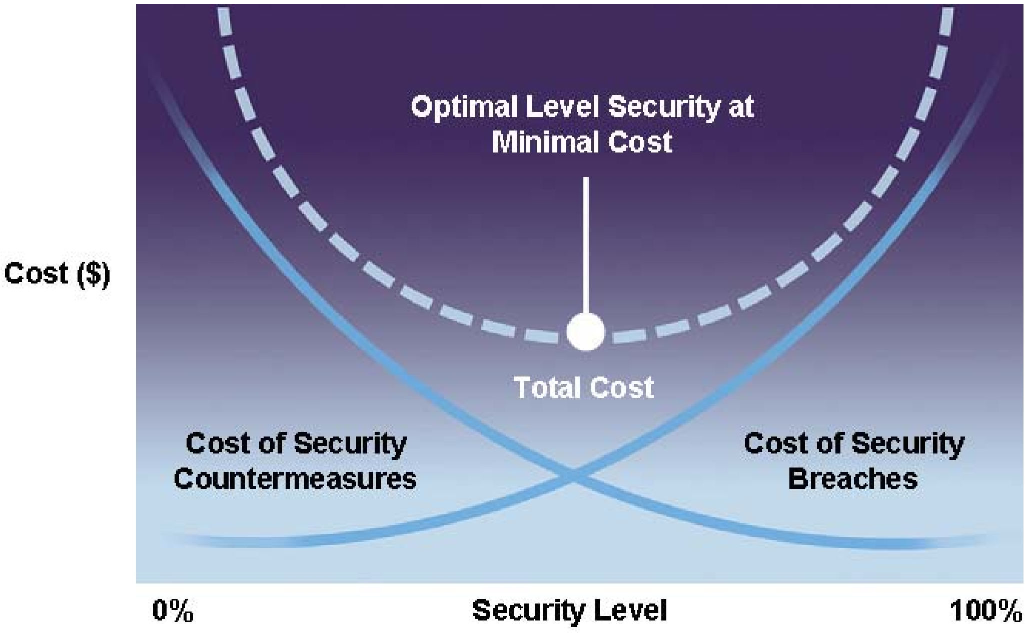


Figure 8. Optimal Security and Cost (From Motorola, 2006).

C. CONCLUSIONS OF THE MODELING

1. This Model

Each disaster is unique and will present its own set of challenges. Deploying an HFN to support the disaster will have to be flexible to meet those challenges. However, providing an HFN with no security will only complicate the already hectic situation for those it is intended to help.

Based on the modeling done in this case study, it is advisable for the security professional to provide at least some security apparatus to the HFN. When considering which security measures to employ, one must consider the risks (threats, vulnerabilities, and information value) and the costs (hardware, software, and personnel) to determine how much security to implement. One technique is to compare the expected cost of the attack with the expected cost of the security as shown in the ROI equation above.

One must use caution, however, when implementing the various security measures to ensure all user access requirements can still be met. There are security measures available that will allow for the protection of information without blocking access to those users, like the recent victims of Hurricane Katrina, desperately needing unhindered access to the Internet. See Chapter V for details of a possible solution for this type of scenario.

2. Applicability to Other Scenarios

This modeling should be general enough to apply not only to HFNs, but also to other situations where the IA professional must decide how much security to implement on a particular network.

III. SECURING AN HFN

As the previous chapters have shown, an HFN should have at least some measure of security implemented. The amount of wireless security required may be situation and resource dependent, but there are some constants that can be designed into the HFN architecture.

Many experts agree the best defense is one of layers or "Defense in Depth." Like an enterprise WLAN, an HFN must consider wireless security from the edges of the network (e.g., the client devices) to the wired portions of the network (e.g., the servers, whether local or remote). The following sections present two approaches to providing wireless security within an HFN using this layered approach. While some specific vendors and products may be mentioned, this chapter will be limited to non-technical, general steps for security.

A. AIRDEFENSE THREE STEP METHOD

In an AirDefense white paper titled *Three Steps for Bullet-proof Wireless LAN Security & Management*, the authors suggest a layered approach to security that will address all network components. They recommend 1) securing WLAN devices, 2) securing communications, and 3) monitoring for security and compliance.[15] Each of the three steps will be explored in more depth below. All three of these should be addressed in a well-written wireless security policy for the HFN. See Appendix A for a sample policy.

1. Securing WLAN Devices

There are two categories of WLAN devices typically deployed in an HFN to support disasters like those discussed in Chapter I. First, there were a limited number of WLAN devices provided by NPS (e.g., Wireless Access Points [WAP], laptops and VoIP phones). It is these devices that must be secured to ensure this level of wireless protection is properly implemented. There are a number of ways to secure these devices including:

- Windows update: ensure all patches and updates are applied to your operating system and major applications

[15] AirDefense (2006), p. 1. For more information on their products, see Chapter IV of this thesis.

- Use National Security Agency Security Configuration Guides[16] to secure the operating system, applications, and wireless features
- Use Defense Information Systems Agency Security Technical Implementation Guides[17] and checklists
- Ensure only guest access to laptops with no administrator privileges
- Antivirus update: ensure the latest virus signatures and antivirus software are installed on applicable devices
- Firmware update: ensure latest firmware and operating system software are installed on WAPs and VoIP phones.
- Personal firewall (AirDefense recommends AirDefense Personal for this task[18])

The second category of WLAN devices in use in an HFN are those provided by anyone else (e.g., First responders, local government agencies, survivors). While there should be provisions for these users to connect their own equipment (e.g., Guest access which will be discussed later), these devices must be treated as untrusted. Procedurally, it would be counter productive for the HFN administrators to have to verify configurations on every end-user device that would connect. Therefore, to enable the most users to join the network, these devices should only be allowed to access the untrusted path (see Chapter V for an implementation using Virtual LANs [VLAN] to segment trusted and untrusted traffic).

2. Securing Communications

This step focuses on the authentication of user devices with the network and encryption of the data flowing across the airwaves. There are many forms of authentication including Extensible Authentication Protocol (EAP) and all its variants. The reader is referred to the plethora of readily available literature for technical details on these various protocols. The authentication step is one of the most important in establishing a secure WLAN. It is here that the wireless client device is authenticated as being allowed to join the network. There is, however, another equally important aspect that is often overlooked: authentication of the network to the client device.

[16] National Security Agency, http://www.nsa.gov/snac/, Last accessed August 27, 2006.

[17] Defense Information Systems Agency, http://iase.disa.mil/stigs/stig/, Last accessed August 27, 2006.

[18] AirDefense (2006), p. 2. AirDefense Personal protects mobile users of hotspots and other public Wi-Fi networks from wireless-specific risks that could expose private data and transactions.

Having the authentication done in both directions is called mutual authentication and is the best case for a truly secure authentication scheme. Edney and Arbaugh (2004) assert,

> In the wireless world, you usually need mutual authentication. The network wants proof about the user, but the user also wants proof that the network really is the expected one. This is important for Wi-Fi LANs because it is so inexpensive to set up decoy access points.[19]

They go on to say that authentication must be performed initially when a client joins the network, but should also be done every time the client communicates with the network. Once the mutual authentication has taken place, the next step is to set up the encrypted communications channel to ensure the confidentiality and integrity of the information flowing across the airwaves.

For wireless path encryption, IEEE 802.11 provides three cryptographic algorithms to protect data traffic: Wired Equivalent Privacy (WEP), Temporal Key Integrity Protocol (TKIP), and Counter Mode with Cipher-Block Chaining with Message Authentication Code Protocol (CCMP) using the Advanced Encryption Standard (AES).[20] The reader is again referred the available literature for technical details. IEEE 802.11i (Amendment 6: Medium Access Control (MAC) Security Enhancements), ratified July 29, 2004, provides for more robust security mechanisms. In the book *WiFoo: The Secrets of Wireless Hacking*, the authors argue the improved data confidentiality and integrity may improve wireless security for those choosing to implement the new standard and may force attackers to search for pre-802.11i networks.[21] Due to the known problems with WEP, Wi-Fi Protected Access (WPA), which uses TKIP, and WPA2, which uses TKIP or CCMP, are now the wireless security protocols of choice. According to the Wi-Fi Alliance, there are at least 1488 devices that are WPA certified and over 575 devices available that are WPA2 certified.[22]

In the absence of one of the algorithms above, a wireless user could instead use a trusted "wired" security solution, Virtual Private Networks (VPN), to provide the

[19] Edney & Arbaugh, (2004), p. 91.

[20] IEEE 802.11i, (2004), p. 12.

[21] Vladimirov, Gavrilenko, & Mikhailovsky (2004), p. 251.

[22] Wi-Fi Alliance, http://certifications.wi-fi.org/wbcs_certified_products.php, Last accessed August 5, 2006.

confidentiality needed. In a white paper from Blue Ridge Networks titled Wireless Security is Broken and it Doesn't Matter, the authors maintain that VPN technology has stood the test of time and can be a viable solution to protect both wireless and wired communications regardless of whether or not other encryption mechanisms are used on the WLAN link.[23] While this solution is indeed proven, it does come at a price. Most VPN implementations require both server and client-side application software which increases the management overhead. Furthermore, the type of VPN implementation must be considered. Korelc and Tittel (2006) say the two most popular VPN implementations, IPSec (IP Security) and SSL (Secure Sockets Layer), each have their own strengths and weaknesses. This is another factor that administrators must consider when designing the security mechanisms for their WLAN links.

3. Monitoring for Security and Compliance

Once the end-user devices and communications paths have been protected, the WLAN must be monitored for security and compliance with policies. To do this effectively requires round-the-clock monitoring of the airwaves to detect intruders and ensure that authorized users remain properly configured and authenticated while connected. AirDefense advocates a monitoring solution that provides the following:[24]

- Ears and Eyes of the airspace
- Rogue Detection & Mitigation
- Intrusion Detection
- Active Defenses
- Policy Enforcement
- Forensic & Incident Analysis
- Fault Diagnostics & Health Monitoring

They recommend their AirDefense Enterprise solution to handle these varied tasks. Other vendors provide similar products (see Chapter IV for details).

[23] Blue Ridge Networks (2005), p. 3.

[24] AirDefense (2006), p. 4.

B. MOTOROLA'S HOLISTIC SECURITY APPROACH

Like AirDefense, Motorola recommends a layered or holistic approach to wireless security. They reason that people, process, policy, and technology must all be addressed to have truly comprehensive wireless security.[25] These four aspects of holistic security are further detailed below.

1. People

The authors of Motorola (2006) state "Once a company can leverage its most valuable resource, people, the ability to mitigate risks becomes more efficient and less cost-intensive."[26] Bruce Schneier, in his book titled *Secrets and Lies*, argues the fact that people have to use the computer introduces "the biggest security risk of them all."[27] Schneier goes on to suggest that "people often represent the weakest link in the security chain and are chronically responsible for the failure of security systems."[28] Having an employee training and awareness program and implementing a good audit program are just part of the key to closing this weak link.

Applying this aspect of security to HFNs, however, is somewhat difficult since you never know ahead of time who the people using the network are going to be. Furthermore, during disasters such as those discussed in Chapter I, there is little time and no mechanism for formal or informal training of users. Some of this difficulty can be mitigated with proper security policies such as Acceptable Use Statements (see the WLAN Security Policy in Appendix A for further detail). The remaining pieces of securing the HFN through addressing people issues are beyond the scope of this thesis.

2. Process

Motorola (2006) claims processes that are measurable can streamline operational costs and enhance security thereby helping to ensure system availability, confidentiality, and integrity.[29] In an HFN implementation, the processes for installing, operating, and maintaining the wireless network should be defined ahead of time. A detailed CONOPS

[25] Motorola (2006). p. 9.

[26] Ibíd.

[27] Schneier (2000), p. 255.

[28] Ibíd.

[29] Motorola (2006), p. 9.

and Standard Operating Procedure (SOP) documents would go a long way toward making this a reality for future HFN deployments. This is included in Chapter VI as future work recommended for others.

3. Policy

Wireless LAN security policies are a key to ensuring your network is protected. Moerschel, Dreger, and Carpenter (2006) state,

> When strictly followed and combined with effective technical solutions, wireless LAN security policies can reduce intrusions, risks, and costs associated with intrusion response and legal action. Where security policies are not strictly followed, gaping security holes exist that no technical solution can repair.[30]

The authors of Motorola (2006) suggest that policy goes further than just risk reduction. They state "a prudent and dynamic policy is critical to informed decision-making."[31]

The contents of the wireless security policy are dependent on the environment in which the wireless LAN is deployed as well as the importance of the information flowing across the airwaves. Moerschel et al. (2006) provide great detail on what should go into a WLAN security policy.[32] Planet 3 Wireless, creators of the Certified Wireless Network Professional program, teamed with Cisco Systems to create a WLAN Security Policy Template. A copy of this template has been included as Appendix A.[33]

In the context of an HFN, the environment is likely to be unpredictable. There will be many unknowns to deal with, but having a well-written, thorough WLAN security policy will help deal with those uncertainties. This is an area that could benefit from further research and is included in Chapter VI as future work recommended for others.

4. Technology

Technology is the primary focus of this thesis. The authors of Motorola (2006) argue

[30] Moerschel et al. (2006), p. 134.

[31] Motorola (2006), p. 9.

[32] Moerschel et al. (2006), Ch 6-9 provide detailed explanations of what should go into the policy.

[33] Also available at Planet 3 Wireless' Certified Wireless Network Professionals (CWNP) web site, https://www.cwnp.com/templates/WLAN_Security_Policy_Template_v1.05.pdf To download a copy of the template, a user account is required (no purchase necessary). Go to www.cwnp.com for details.

> The technology component of an effective enterprise security strategy encompasses traditional security measures, such as firewalls, authentication and [Intrusion Detection] systems. It must also account for ever-changing vulnerabilities, the interconnectedness of wired and wireless systems, and the need to identify and address emerging threats before they cause damage.[34]

The commercial marketplace is full of products that offer various mechanisms for providing wireless LAN security. Chapter IV provides a summary of these various products and which of the IA attributes (confidentiality, integrity, and authentication) they provide.

C. CONCLUSION

Regardless of the specific approach one takes, wireless security is necessary and achievable within an HFN. Chapter V shows a simple implementation of some of these security measures that the author tested in a laboratory environment and installed in the NPS Nemesis MRF. In addition, there is a target architecture that incorporates a layered approach to wireless security with additional measures that would make future HFN deployments even more secure.

Providing a guest access Service Set Identifier (SSID) is also paramount in situations like the HA/DR scenarios discussed in Chapter I to ensure the maximum number of affected personnel, rescue workers, first responders, volunteers, local government agency personnel, and others have access to the WLAN.

The next chapter looks at COTS products that claim to provide security for WLANs. Some of the products are unique to WLANs (e.g., Wireless Intrusion Detection Systems [WIDS], Wireless Intrusion Prevention Systems [WIPS], and WAPs). Others are tried and true solutions (e.g., VLANs, VPNs, Remote Authentication Dial-In User Service [RADIUS]) for wired security problems that can be extended to the wireless domain.

[34] Motorola (2006), p. 10.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. REVIEW OF COTS PRODUCTS

A. METHODOLOGY FOR CLASSIFYING PRODUCTS

The previous chapter discussed various strategies for applying layers of security or Defense in Depth for a WLAN. A robust security implementation should provide multiple layers of defense using products from the various layers. The products listed in this chapter represent only a small subset of those available on the market today. As this thesis research progressed, additional products were being announced on a regular basis.[35] The products are grouped according to the method described below and are listed in alphabetical order within each section.

1. AirDefense Three-Step Model

As discussed in the previous chapter, AirDefense (2006) recommends a three-step approach to WLAN security: securing WLAN devices, securing communications, and monitoring for security and compliance on the network. This method also provides a convenient way to categorize the various wireless security products to better understand where and how they provide security.

2. OSI Model

Moerschel et al. (2006) claim an OSI-based model is also useful to categorize the various products.[36] Knowing where the various products fit in the OSI model helps one understand how the security is implemented. Figure 9 provides a depiction of the OSI model. Most of the WLAN security products on the market that provide encryption do so at either Layer 2 or Layer 3.

[35] A list of references, including web sites, is provided As Appendix B. Additional information on specific products can be found by visiting the vendor’s web site. Further information on products meeting FIPS 140-2 validation can be found at http://csrc.nist.gov/cryptval/140-1/1401vend.htm and information on products meeting common criteria certification can be found by visiting http://www.commoncriteriaportal.org/public/consumer/index.php.

[36] Moerschel et al. (2006), p 212.

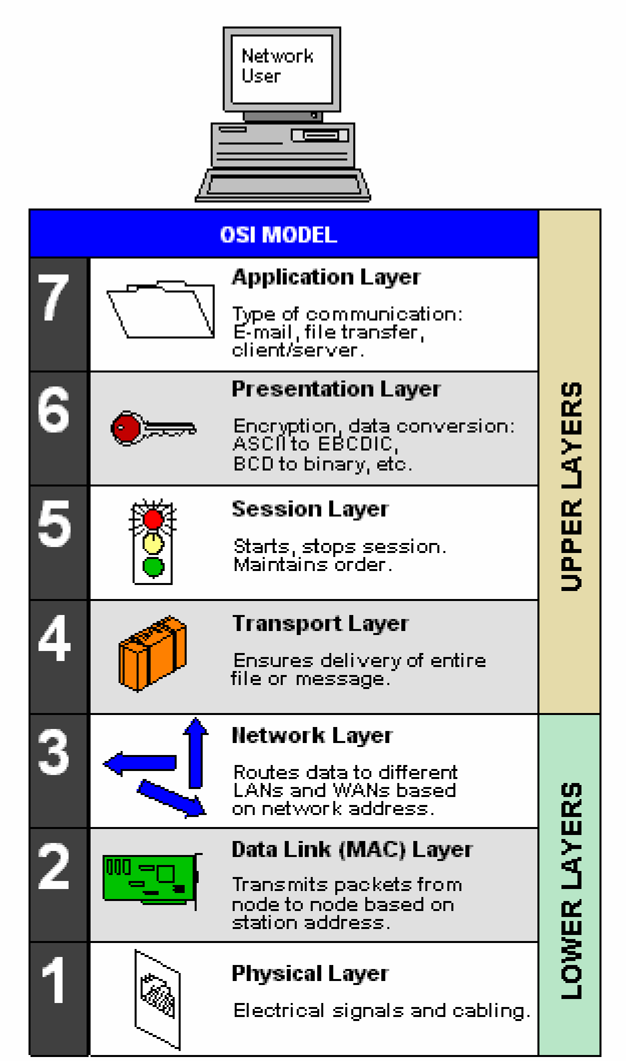

Network User
OSI MODEL
7
Application Layer
Type of communication: E-mail, file transfer, client/server.
6
Presentation Layer
Encryption, data conversion: ASCII to EBCDIC, BCD to binary, etc.
5
Session Layer
Starts, stops session. Maintains order.
4
Transport Layer
Ensures delivery of entire file or message.
3
Network Layer
Routes data to different LANs and WANs based on network address.
2
Data Link (MAC) Layer
Transmits packets from node to node based on station address.
1
Physical Layer
Electrical signals and cabling.
UPPER LAYERS
LOWER LAYERS

Figure 9. OSI Model (After The Free Dictionary online)[37]

[37] OSI Model Picture, http://computing-dictionary.thefreedictionary.com/OSI+model, Last accessed August 27, 2006.

Table 3 provides examples of various security solutions and where they fit in this model.

Table 3. Example Security Solutions by OSI Layer (From CWSP Study Guide)[38]

Layer 2 (Data-Link Layer) • WEP (and all variations such as TKIP) • 802.1x/EAP (and all variations) • Enterprise Encryption Gateways • Layer 2 Tunneling Protocol (L2TP)
Layer 3 (Network Layer) • Point-to-Point Tunneling Protocol (PPTP) • IP Security (IPSec)
Layer 7 (Applications Layer) • Secure Shell (SSH) • Secure Shell Version 2 (SSH2) • Novell Directory Services (NDS or eDirectory) • Microsoft Active Directory (AD)

The following sections provide a summary table and details of the various COTS products the author reviewed. The table includes vendor, product, type, step, FIPS Validation level, Common Criteria certification level, OSI layer, and which of the IA attributes listed in Chapter I they provide. Following the table is a detailed listing of these COTS products. They are organized according to which of the three steps mentioned in the AirDefense (2006) white paper the product best fits. In addition, the OSI layer into which they most closely fall is noted. The author focused primarily on products that specifically provide wireless security in the context of HFNs. Some of the products, however, originated to fulfill a need in the "wired" environment and are included in this analysis because they do provide at least one of the desired security capabilities necessary

[38] Moerschel et al. (2006), p 212.

in a WLAN. Some products classes such as VPN software were not individually reviewed, but are noted generically in the appropriate category.

B. PRODUCT SUMMARY

As previously mentioned, an IA professional should strive to provide Defense in Depth. In doing so, one must draw products from several of the categories described above. Table 4 shows a summary of the various products reviewed and includes the step (corresponding to AirDefense (2006) step 1, 2, or 3), FIPS 140-2[39] and Common Criteria[40] level if applicable, OSI layer, and which of the IA attributes each product meets. The products appear in the table in alphabetical order by vendor. The order of appearance does not imply that any particular product is better than any other.

Key to table:

Type: HW = Hardware; SW = Software

Step: 1. Securing WLAN Devices;
2. Securing Communications;
3. Monitoring for Security & Compliance

FIPS 140-2: FIPS validated at indicated level (1-4); N = not FIPS validated

CC: Common Criteria Evaluation Assurance Level (EAL) level (1-7)
N = not certified

Attributes: C = Confidentiality
I = Integrity
A = Authentication
✓ indicates product has that attribute.

X indicates product does not have that attribute.

N/A = not applicable for any column in the table.

[39] The reader is reminded that FIPS 140-2 is a validation for cryptographic modules and is therefore not applicable to some of the products in the table. See http://csrc.nist.gov/cryptval/140-1/1401vend.htm for additional information on products that have received FIPS 140-2 validation.

[40] Common Criteria Evaluation Assurance Levels (1-7) provide a uniformly increasing scale which balances the level of assurance obtained with the cost and feasibility of acquiring that degree of assurance. Additional information is available at http://www.commoncriteriaportal.org/public/files/ccintroduction.pdf, Retrieved September 6, 2006. See http://www.commoncriteriaportal.org/public/consumer/index.php for a search capability to access certification reports. Last accessed September 1, 2006.

Table 4. WLAN Security Product Summary

Vendor	Product	Type	Step	FIPS 140-2	CC	OSI	C	I	A
3e	527 Mesh WAP	HW+SW	1, 2	2	N	3	✓	✓	✓
3e	AirGuard 110 WLAN PC Card w/ Crypto Client SW	HW+SW	1, 2	1	N	3	✓	✓	✓
AirDefense	Personal (Firewall)	SW	1	N/A	N	N/A	**X**	**X**	**X**
AirDefense	Enterprise WIPS (Guard, version 3.5)	HW+SW	3	N/A	2	N/A	**X**	**X**	**X**
AirMagnet	SmartEdge Sensors AM-5010 & 5012	HW+SW	3	2	N	N/A	**X**	**X**	**X**
Aruba	Access Points	HW+SW	1, 2	N	N	3	✓	✓	✓
Aruba	Mobility Controllers	HW+SW	3	2	N	3	✓	✓	✓
Blue Ridge Networks	BorderGuard Series VPN Appliances	HW+SW		2	N	3	✓	✓	✓
BlueSocket	BlueSecure 2100 & 5000 Controllers	HW+SW	3	2	N	3	✓	✓	✓
CipherOptics	Data Protection Gateway SG1002	HW+SW	2	2	2	3	✓	✓	✓
Cisco	WAPs	HW+SW	2	2	N	3	✓	✓	✓
Cisco	Network Admission Control (NAC)	HW+SW	3	N/A	N	N/A	**X**	**X**	✓
Cisco	WLAN Controllers	HW+SW	3	2	N	3	✓	✓	✓
Cranite Systems	Wireless Wall & Access Controller	SW	2, 3	1	N	2	✓	✓	✓
Fortress Technologies	AF2100 & AF7500 Secure Gateways	HW+SW	2	2	N	2	✓	✓	✓
Fortress Technologies	MaPS	SW	3	N/A	N	N/A	**X**	**X**	✓
Fortress Technologies	Secure Client	SW	2	3	N	2	✓	✓	✓
Juniper Networks	Odyssey Access Client w/ Security Component, ver 1.2	SW	2	1	N	2	✓	✓	✓
Juniper Networks	Odyssey Access Server; Steel Belted RADIUS Server	SW	2, 3	N/A	N	2	✓	✓	✓
Juniper Networks	Steel Belted RADIUS Appliance	HW+SW	2, 3	N/A	N	2	✓	✓	✓
Newbury Networks	WiFi Watchdog	HW+SW	1, 3	N	N	N/A	**X**	**X**	✓
Phoenix Technologies	TrustConnector 2	SW	1	N	N	N/A	**X**	**X**	✓

C. PRODUCTS FOR SECURING WLAN DEVICES (STEP ONE)

This category of products includes the WLAN devices themselves as well as products that help to "lock down" the WLAN devices. When purchasing WLAN devices (e.g., WAPs, laptops, and handheld computers/PDAs) one must ensure the product has built in features to prevent unauthorized access both remotely and locally.

The COTS products in this category are, for the most part, not unique to the wireless domain (WAPs are discussed in Section D later in this chapter as products that secure the communications links). Therefore, only a high level of information is provided. Section E below provides another group of products that ensure the WLAN devices are "secure" before being allowed to join the network.

1. Personal Firewalls

Personal firewalls are necessary for wireless devices as well as desktop computers. Many vendors offer personal firewall software including McAfee, Norton, Microsoft, and AirDefense. The authors of AirDefense (2006) contend the protection they offer is a must to ensure the WLAN edge devices on your network are properly protected.

According to www.airdefense.net, AirDefense Personal™, a Windows-based software agent, is the industry's most advanced, wireless end-point security and policy enforcement solution for mobile workers. Residing on mobile users' computers, AirDefense Personal quietly monitors for malicious or accidental wireless activities and wireless misconfigurations that may cause security exposures or policy violations.[41]

2. Anti-Virus

Anti-virus software is another "must have" to ensure the overall protection of wireless client devices. There are many vendors providing software in this category including McAfee, Symantec, Panda Software, Trend Micro, and Computer Associates to name a few.

3. Disk Encryption

Physical security of WLAN devices, especially in an environment like those described in Chapter I may not be a high concern. There is likely to be little or no data on

[41] This solution complements personal firewalls and host-based IDS systems that don't protect the client against wireless attacks. See AirDefense's web site for additional information on this product at http://www.airdefense.net/products/adpersonal/index.php, Last accessed August 30, 2006.

the computer that is sensitive enough to worry about. In the case where there is sensitive data, however, one needs to have a mechanism for protecting that information. Disk encryption software is one method to ensure the data is not compromised even if the WLAN device is. Various open source (e.g., www.truecrypt.org) and commercial products (e.g., PGP, Dekart) are available to provide partial or whole disk encryption.

4. WLAN Endpoint Protection

Phoenix Technologies provides a software product called TrustConnector 2 that is a cryptographically-based solution for existing Windows machines. Once loaded, it ensures any x86-based device connecting to an IP network is absolutely trusted by using an industry-unique combination of user/device authentication.[42]

D. PRODUCTS FOR SECURING COMMUNICATIONS (STEP TWO)

The products in this category provide security of the communications link between wireless clients and WAPs or between WAPs themselves (bridge links). This involves both authentication and encryption. Authentication is provided using an implementation of the authentication, authorization, and accounting (AAA) protocol. The most common methods for encryption are provided at either Layer 2 (e.g., encryption gateways) or Layer 3 (e.g., VPNs) of the OSI model. This section is divided into products that provide for authentication and products that provide for encryption of the link.

1. Authentication

This class of products is a carryover from wired networks. RADIUS is an implementation of the AAA protocol and is a common authentication protocol used in IP networks. It typically provides for authentication of clients on the network using some form of EAP and is of equal utility on wireless LANs. As of this writing, there are at least nine implementations of EAP.[43]

[42] Phoenix Technologies, http://www.phoenix.com/en/Products/Trusted+Applications/TrustConnector/default.htm, Last accessed August 30, 2006.

[43] For additional information on authentication and the various implementations of EAP, see the white paper entitled Demystifying Wireless Network Access and 802.1X Security by Fluke Networks available at http://www.flukenetworks.com/FNet/en-us/findit?Document=2647086, Last accessed August 30, 2006.

There both open source and commercial sources for RADIUS server and client software and appliances.[44] One product was found to be FIPS 140-2 validated and is discussed below.

In addition to client and server software, many vendors have RADIUS authentication capabilities built into their WAPs (e.g., 3Com, Cisco, Intel, and Linksys). Some of these WAPs use IEEE 802.1X implementations while others offer proprietary solutions. Therefore, one must choose carefully when engineering a solution using WAPs that offer authentication.

a. Juniper Networks (formerly Funk Software)

Juniper Networks offers RADIUS servers called Odyssey Access Server (OAS) and Steel Belted RADIUS (SBR) to handle remote authentication and the Odyssey Access Client (OAC) for WLAN devices to securely connect to the network.[45] One version of the OAC using Juniper's Odyssey Security Component includes a cryptographic module that is FIPS 140-2 Level 1 Validated.[46] In addition, they offer an SBR appliance that is rack mountable and supports the Enterprise and Global Editions of their SBR server software. The servers, in all forms, also provide security policy management functions which fits under Section E of this chapter.

2. Encryption

In a white paper by Northrop Grumman (Knuth, 2004), the author argues that network security is most appropriate when implemented at the lowest layer possible and OSI Layer 2 solutions are superior for mobile WLAN encryption since more information is protected.[47] Figure 10 illustrates Knuth's point. The portion of the data not include in the protected payload is the only data at risk if the transmission is intercepted by an unauthorized recipient.

The remainder of Section D will look at products that offer encryption at either Layer 2 or Layer 3 of the OSI model. This includes encryption gateways, WAPs, and

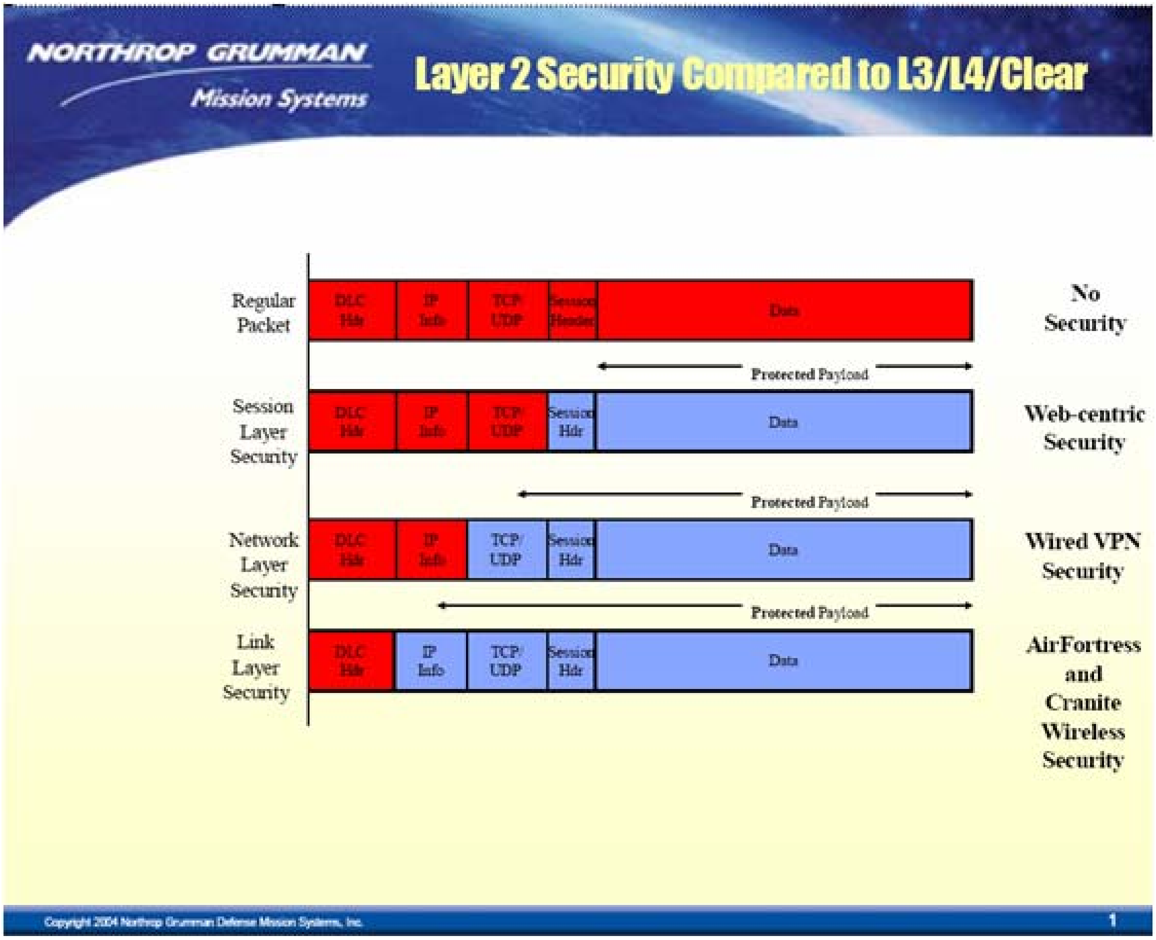
[44] Wikipedia, http://en.wikipedia.org/wiki/List_of_RADIUS_Servers, Last accessed August 27, 2006..

[45] Juniper Networks, http://www.juniper.net/solutions/literature/white_papers/200171.pdf, Last accessed August 29, 2006.

[46] Juniper Networks, http://www.juniper.net/products/aaa/odyssey/oac_fe.html, Last accessed August 29, 2006.

[47] Knuth (2004), p. 5.

wireless client products. While there are thousands of products fitting this category, the following discussion focuses on those that are either FIPS 140-2 validated or have very specific applicability to HFNs.


NORTHROP GRUMMAN
Mission Systems

Layer 2 Security Compared to L3/L4/Clear

Regular Packet: DLC Hdr | IP Info | TCP/ UDP | Session Header | Data — No Security

Protected Payload

Session Layer Security: DLC Hdr | IP Info | TCP/ UDP | Session Hdr | Data — Web-centric Security

Protected Payload

Network Layer Security: DLC Hdr | IP Info | TCP/ UDP | Session Hdr | Data — Wired VPN Security

Protected Payload

Link Layer Security: DLC Hdr | IP Info | TCP/ UDP | Session Hdr | Data — AirFortress and Cranite Wireless Security

Copyright 2004 Northrop Grumman Defense Mission Systems, Inc.

1

Figure 10. Comparison of Security (From Knuth, 2004, p. 1.)

VPN servers and software are another of the carry over technologies from the wired network environment.[48] They are typically implemented at Layer 3 of the OSI model and are quite useful for securing the communications paths in wireless implementations as well. Blue Ridge Networks offers a line of Border Guard Security Appliances and Client Software that provide security for both wired and wireless clients.[49] VPN products will not be discussed further in this thesis.

[48] Some would argue that VPNs are all that are needed to properly secure a wireless link. For further information supporting this argument, see Blue Ridge Networks (2005).

[49] Blue Ridge Networks, http://www.blueridgenetworks.com/solutions/solutions_wireless.htm, Last accessed September 2, 2006.

a. Encryption Gateways

Most encryption gateways secure information at Layer 2 of the OSI model. This method leaves only the link header in the clear and provides better confidentiality of data. Some, however, provide encryption at Layer 3.

CipherOptics

CipherOptics data protection gateways provide full duplex, wire-speed AES or 3DES (Triple Data Encryption Standard) IPSec encryption (100 Mbps and Gigabit) to broadband wireless paths as shown in Figure 11.

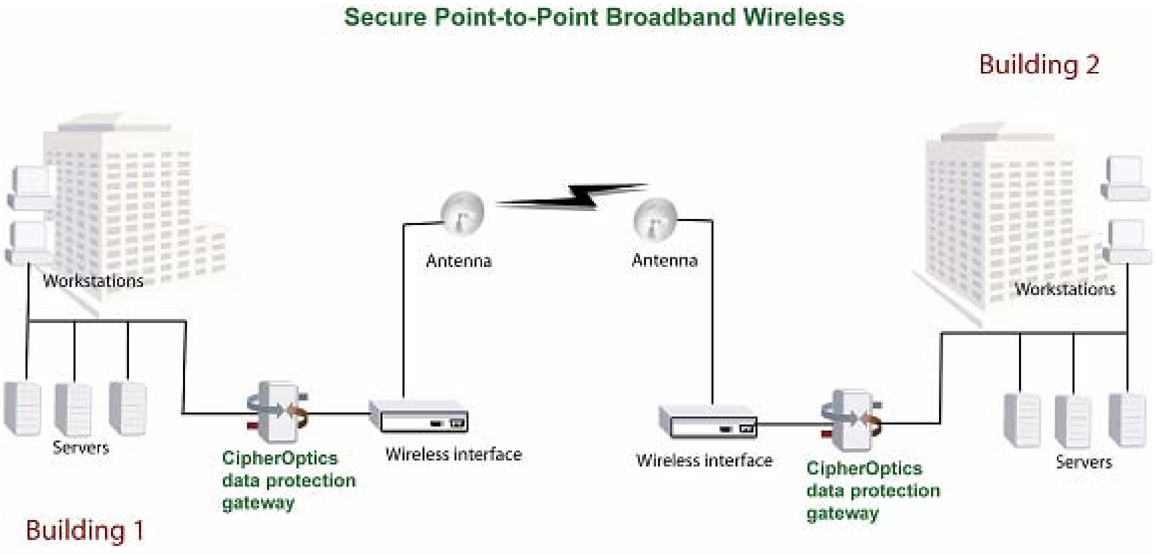

Secure Point-to-Point Broadband Wireless
Building 2
Antenna
Antenna
Workstations
Workstations
Servers
CipherOptics data protection gateway
Wireless interface
Wireless interface
CipherOptics data protection gateway
Servers
Building 1

Figure 11. Secure Broadband Wireless (From CipherOptics Solution Note, 2005)[50]

The CipherOptics solution, which operates at OSI Layer 3, creates an IPSec tunnel, much like a VPN, to protect the wireless point to point link as shown above independent of the wireless implementation (e.g., 802.11 or 802.16). In addition, CipherOptics data protection gateways are FIPS 140-2 Level 2 validated and provide the authentication and encryption as specified in DoDI 8100.2.[51] The CipherOptics SG1002

[50] CipherOptics Solution Note (2005), p. 2., http://www.cipheroptics.com/pdf/sn-wireless.pdf, Last accessed August 26, 2006.

[51] Ibid., p. 1.

is Common Criteria EAL2 Certified and winner of the Info Security Products Guide's Product Excellence Award 2006 for Excellence in Wireless Security.[52]

Fortress Technologies

Fortress Technologies offers end-to-end security for wireless networks. Figure 12 shows a typical implementation using the AF7500 Security Gateway, AF Secure Client software, and the Management and Policy Server (MaPS).

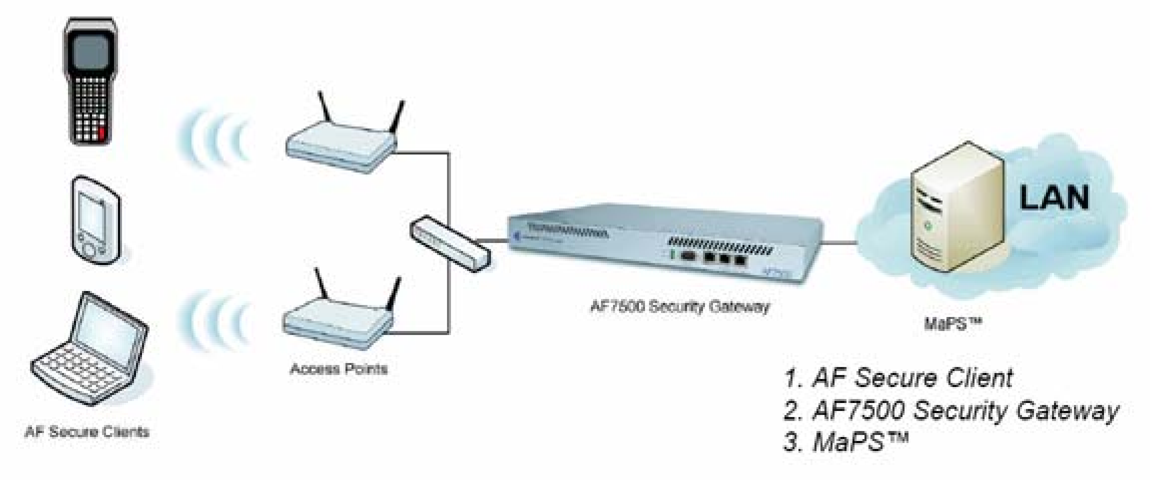


Figure 12. Fortress Security System (From www.fortresstech.com)

This implementation ensures that each device is authenticated before being allowed to access the network and all communications from end user devices (e.g., laptop, PDA, barcode scanner) is encrypted before passing over the wireless airwaves. This solution provides OSI Layer 2 protection and is FIPS 140-2 Level 2 validated. It provides security across multiple access points simultaneously and optimizes critical security operations (e.g., encryption, authentication, key exchange) to minimize management.

Furthermore, the Fortress Technologies family of products is protocol and vendor independent allowing for protection of multiple wireless technologies (e.g., 802.11, 802.16, SATCOM, and Free Space Optical) as shown in Figure 13.

[52] InfoSecurity Products Guide, http://www.infosecurityproductsguide.com/wireless/SG1002.html, Last accessed August 26, 2006.

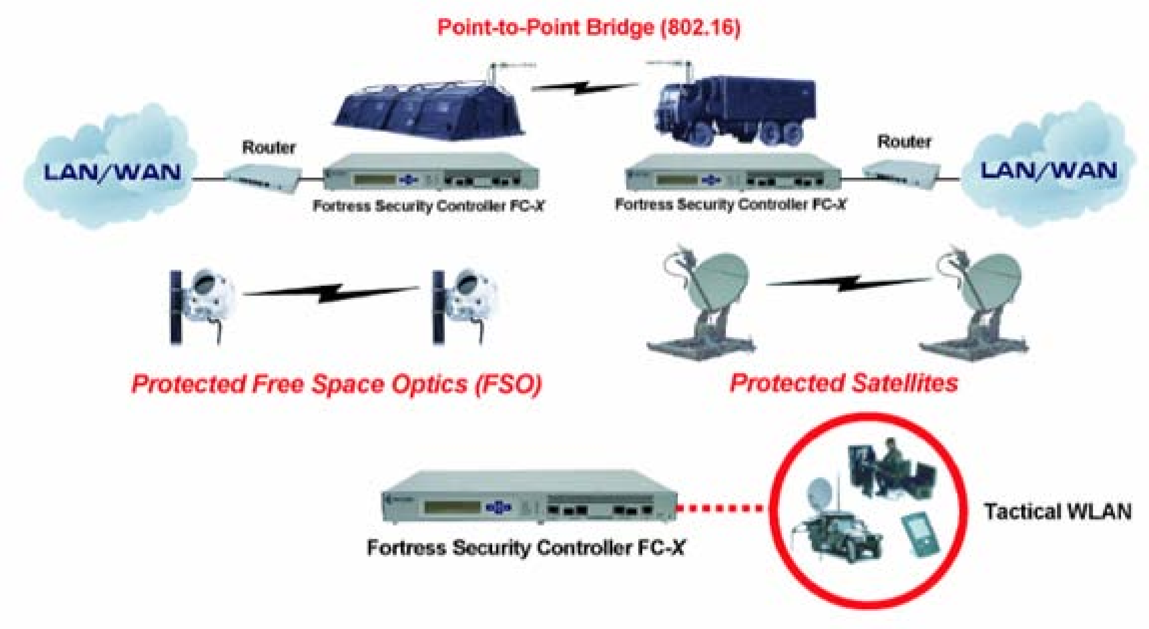

Point-to-Point Bridge (802.16)
LAN/WAN
Router
Fortress Security Controller FC-X
Fortress Security Controller FC-X
Router
LAN/WAN
Protected Free Space Optics (FSO)
Protected Satellites
Fortress Security Controller FC-X
Tactical WLAN

Figure 13. Fortress Secured Point-to-Point Technology
(From http://www.fortresstech.com/solutions_applications/pdfs/federal.pdf)

Finally, Fortress' MaPS provides a centralized management and administration platform for security services and policy management. This product is discussed further in Section E later in this chapter.

Cranite Systems

Cranite Systems has two product lines that support securing the communications between WLAN devices and the network and also provide some management functionality.[53] Cranite's WirelessWall® solution provides an OSI Layer 2 encryption path using FIPS 140-2 Level 1 validated technology inside the enterprise WLAN. It protects sensitive payload and IP address information from any unauthorized listeners. It is comprised of three components: the manager, access controller, and client as shown in Figure 14 and supports VLAN tagging, directory caching, and third party RADIUS servers.

[53] See Cranite Web Site, http://www.cranite.com/ for details on both product lines. Last accessed August 26, 2006.

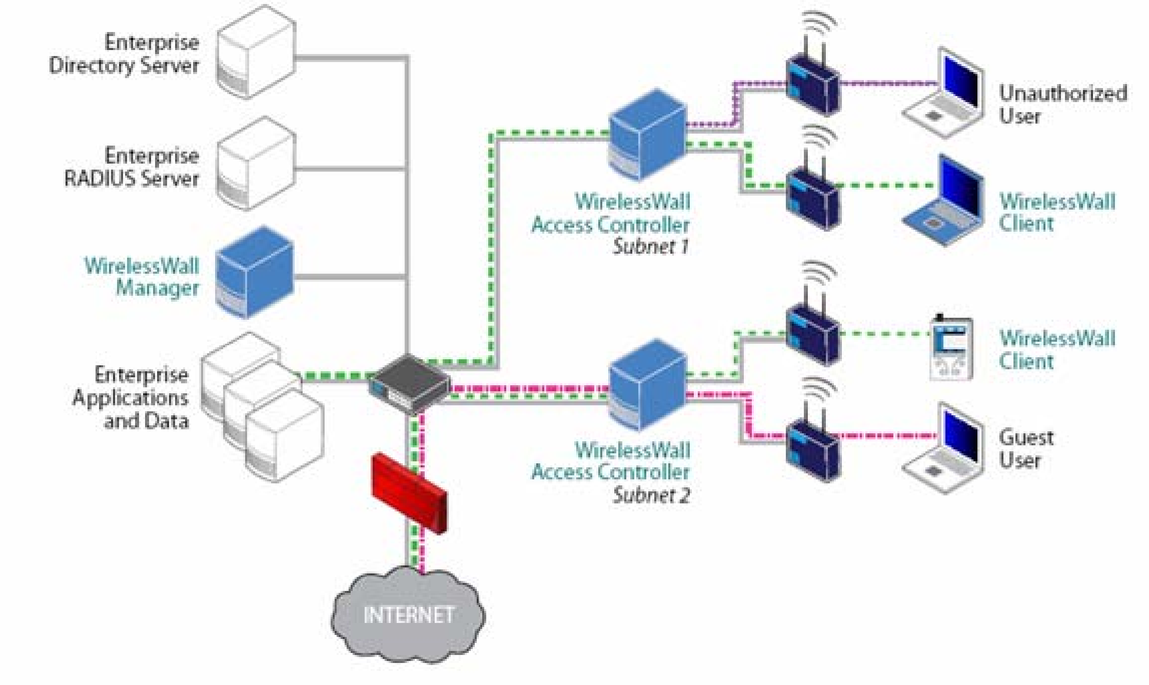

Enterprise Directory Server
Enterprise RADIUS Server
WirelessWall Manager
Enterprise Applications and Data
INTERNET
WirelessWall Access Controller Subnet 1
WirelessWall Access Controller Subnet 2
Unauthorized User
WirelessWall Client
WirelessWall Client
Guest User

Figure 14. Cranite WirelessWall® Architecture (From www.cranite.com)

Cranite's other software-based solution, SafeConnect® is specifically designed to provide mobile users secure connectivity to the enterprise from hotspots, homes, and other remote locations. It again uses an OSI Layer 2 solution along with a unique, patent-pending protective layer designed to abstract users from attack.[54] This solution also has three components: client, access controller, and management system. While it may sound like a VPN solution, Cranite's SafeConnect® goes beyond either IPSec or SSL VPN implementations by providing client-side integrity and attack protection from untrusted locations regardless of wireless transport (e.g., 802.11, 802.16).

[54] See Cranite web site, http://www.cranite.com/safeconnect/safeconnect-datasheet.pdf or www.cranite.com for details. Last accessed August 28, 2006. source

b. Wireless Access Points (WAP)

When deploying WAPs and bridges for an HFN, there are several key features that must be included: encryption, authentication, and ease of management. There are currently at least 1,053 WAPs that carry Wi-Fi certified product status issued by the Wi-Fi Alliance.[55] Many of these WAPs provide the three desired features. In addition, some enterprise class WAPs support multiple SSIDs and VLANs which enable traffic segmentation and further enhance security (e.g., Cisco 1200 series). This section presents details on three vendors who provide the desired security features listed above.

3e Technologies International (3eTI)

3eTI provides WLAN products including security and management server, mesh networking, supplicant and WLAN client devices. 3eTI's AirGuard™ infrastructure solutions are FIPS 140-2 Level 2 validated and DoD-proven for security and use in the most hostile and adverse environments.[56] Their offerings include indoor, outdoor, and video surveillance equipment (see Figure 15) and provide for encryption, authentication, and remote management.

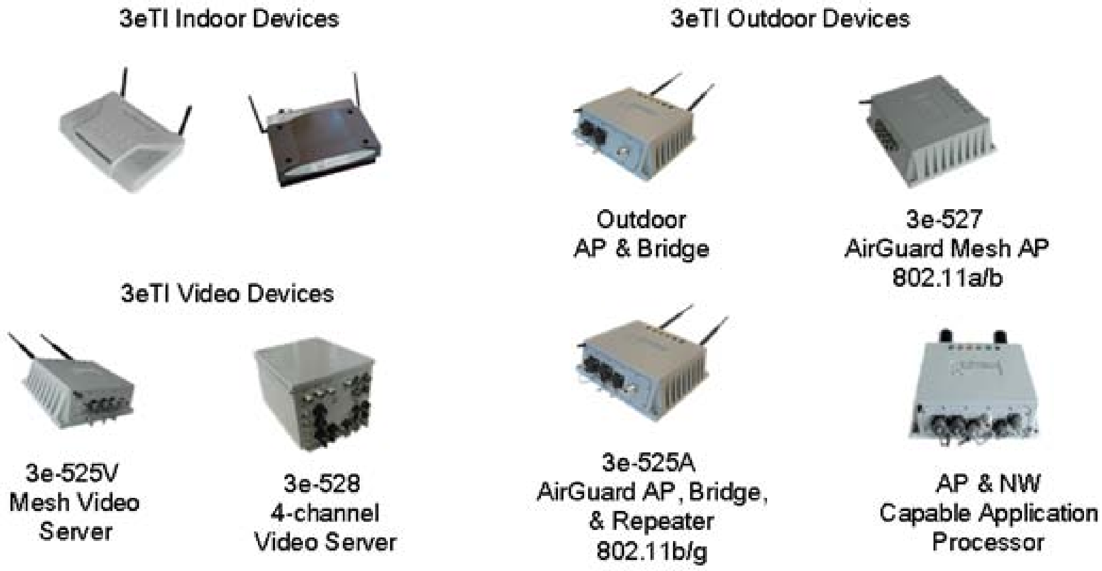


Figure 15. 3eTI AirGuard™ Access Points

[55] Wi-Fi Alliance, http://certifications.wi-fi.org/wbcs_certified_products.php, Last accessed August 26, 2006.

[56] 3e Technologies, http://www.3eti.com/, Last accessed August 28, 2006.

Aruba Networks

Aruba provides a line of products that include an operating system (OS), mobility controllers, and controlled access points. The OS and mobility controllers will be discussed in Section E of this chapter. The Aruba controlled access point line includes both indoor and outdoor rated WAPs that provide for encryption, authentication, and easy management (using ArubaOS and Aruba Mobility Controllers). The WAPs (see Figure 16) are available with single (802.11a or b/g configurable) or dual radio (802.11a + b/g simultaneous) and some can act as both an access point and RF monitor concurrently.[57]

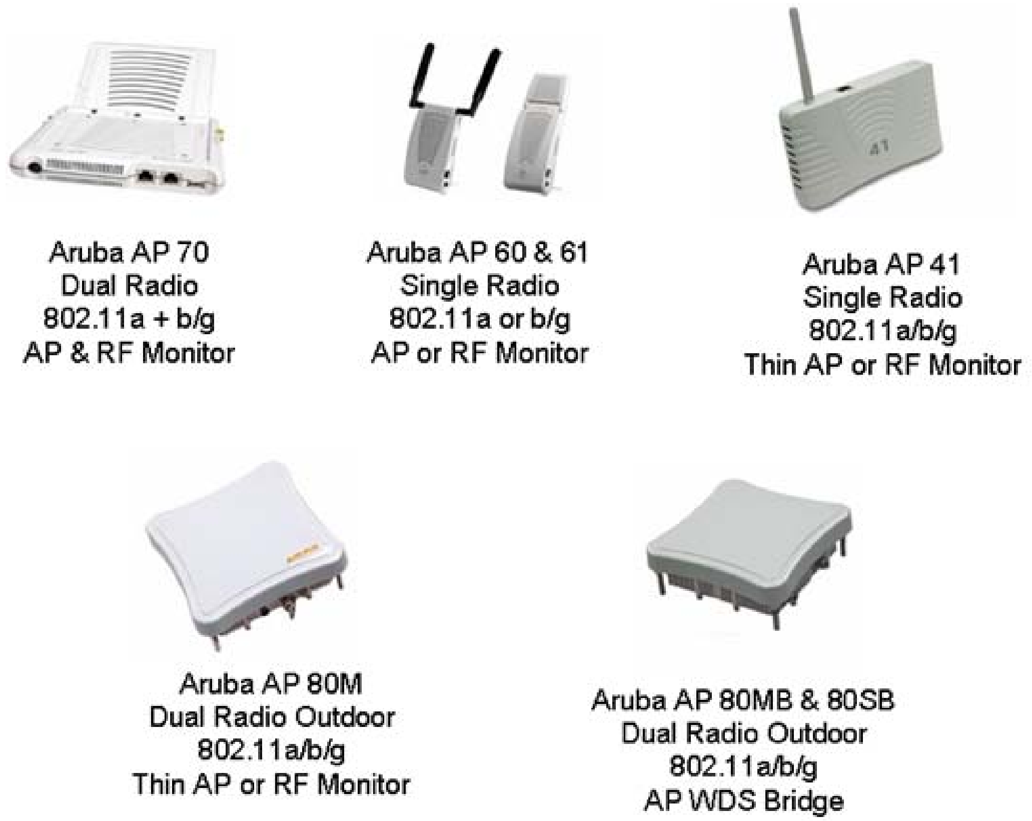


Figure 16. Aruba Networks Access Points

[57] See Aruba Networks, http://www.arubanetworks.com/products/ for additional information. Last accessed August 29, 2006.

Cisco Systems

Cisco Systems Unified Wireless Network offers secure, scalable, cost-effective WLAN solutions.[58] The product line includes client devices, access points, network infrastructure, network management, and delivery of mobility services to maintain network security and simplify network management. Figure 17 shows their line of access points and bridges.

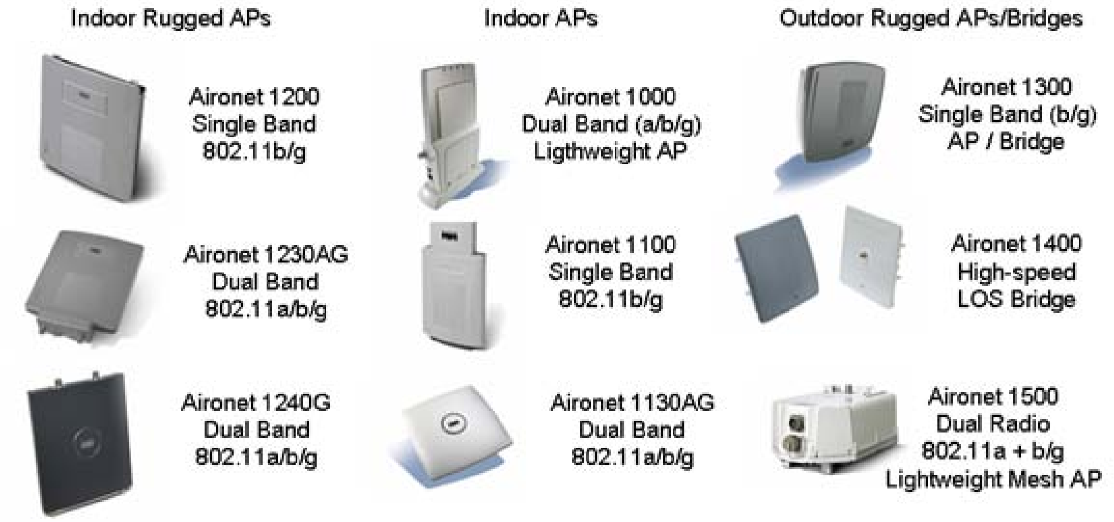


Figure 17. Cisco Aironet Access Points

Cisco's Unified Wireless LAN Controllers and numerous Access Points are FIPS 140-2 Level 2 validated.[59] Many of these WAPs allow for the configuration of multiple SSIDs and VLANs, within a single WAP, allowing for segmentation of traffic to further enhance protection of sensitive data. In addition, most of the product lines can be run in autonomous or lightweight mode. Autonomous mode is like any traditional WAP; lightweight mode requires the use of one of Cisco's Wireless LAN controllers.[60]

[58] Cisco Systems web site provides additional information about the Unified Wireless Network, http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html, Last accessed August 29, 2006.

[59] From Cisco web site, http://newsroom.cisco.com/dlls/2006/prod_081406.html, Last accessed August 28, 2006. See also FIPS 140-2 Vendor List, http://csrc.nist.gov/cryptval/140-1/1401vend.htm for list of specific models.

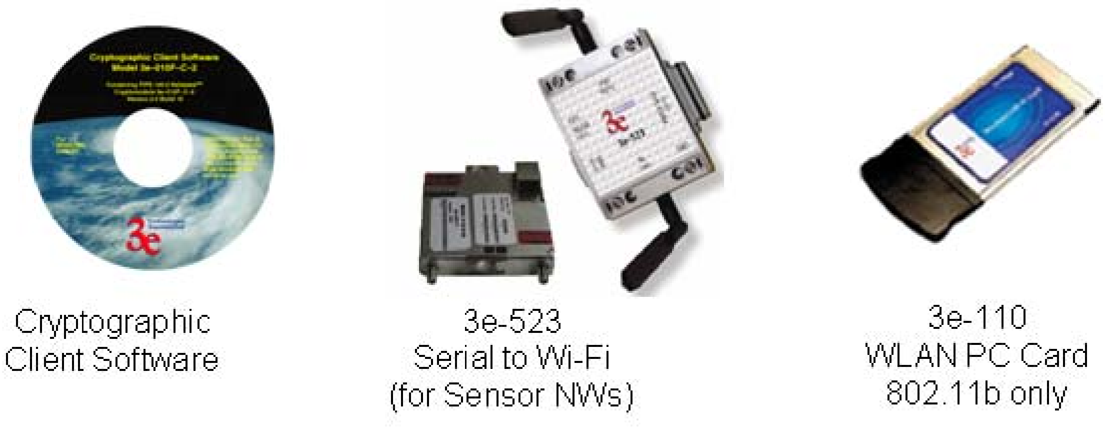
[60] See Cisco's web site for a discussion of Lightweight WAPs and a comparison with autonomous WAPs. http://www.cisco.com/en/US/products/ps6306/products_qanda_item09186a00806a4da3.shtml, Last accessed August 29, 2006.

c. WLAN Client Products

This group of products is used in concert with the WAPs in the previous section to provide security of the communications link between wireless clients and WAPs. This category includes embedded wireless access devices within laptops or PDAs, expansion cards (internal PC cards, laptop cards, Compact Flash, and external USB devices), and client software. There are currently over 1,485 WLAN client products certified by the Wi-Fi Alliance that provide at least some form of encryption.[61] Due to known weaknesses in the WEP protocol, however, one should only consider devices that support 802.11i security features such as WPA or WPA-2. Of note, 3eTI and Fortress Technologies offer products that are FIPS 140-2 validated.

3e Technologies International (3eTI)

3eTI's entries in this category include cryptographic client software, a serial to Wi-Fi unit for sensor networks, and the AirGuard 110 WLAN PC Card (see Figure 18). When used in conjunction with 3eTI's Crypto Client software, the 3e-110 provides advanced wireless RF data security with AES and 3DES encryption that meets FIPS 140-2 Level 1 requirements.[62] It uses only 802.11b, however, which limits it to a maximum of 11 Mbps data transfer rate.



Cryptographic
Client Software

3e-523
Serial to Wi-Fi
(for Sensor NWs)

3e-110
WLAN PC Card
802.11b only

Figure 18. 3eTI's Client Hardware and Software

[61] Wi-Fi Alliance, http://certifications.wi-fi.org/wbcs_certified_products.php, Last accessed August 26, 2006.

[62] Also requires 3e's Security Server software (3e-030) running on an application server within the wired portion of the network. See 3eTI's Product Brochure for Security Server, http://en1.endiva.net/3eti/files/literature/3467.2447_3e-030_SecServ.pdf, Last accessed August 30, 2006.

Fortress Technologies

Fortress Technologies offers a software based product, the Fortress Secure Client (see Figure 19), that is FIPS 140-2 validated (up to Level 3 depending on operating system). Fortress' web site states

> Fortress Secure Clients are security agents that provide the same level of high assurance security across all client devices. All critical security functions - encryption, authentication, data integrity checking, key exchange, and data compression - are optimized to ensure transparent operation. [It] enables devices to securely communicate with the network and peer-to-peer. When installed, the Fortress Secure Client creates a unique device identifier so that only authorized devices are allowed access to the network. This lightweight software agent supports the widest range of devices and operating systems. The Fortress Secure Client runs on PCs, tablets, PDAs, and industrial devices running Windows, Windows CE, Windows Mobile, Linux, Palm (Tungsten C), DOS, or Mac OS X (Tiger and Panther).[63]

Figure 19. Fortress Technologies Secure Client (From www.fortresstech.com)

This software agent protects the authentication and connection of users and devices with AES, DES (Data Encryption Standard), or 3DES encryption, preventing unauthorized access while protecting login credentials and sensitive data across the wireless link. It also has a bridge version that allows for secure extension of applications, devices, and data throughout the enterprise.

[63] See Fortress Technologies, http://www.fortresstech.com/products_services/products_secure_client.asp, Last accessed August 29, 2006.

E. PRODUCTS FOR MONITORING FOR SECURITY AND COMPLIANCE (STEP THREE)

This category of products is the final layer of protection and security that one might apply to HFNs. It includes products such as Wireless Intrusion Detection Systems (WIDS) and Wireless Intrusion Prevention Systems (WIPS), as well as wireless management and control products. Some of these products could greatly simplify network management and control in the HFN. If the threat or the value of the data to be protected is high enough, these products would be essential in an HFN deployment.

1. WIDS & WIPS

A WIDS is typically composed of a central computer and various sensors that continuously scan for network anomalies, misconfiguration, and attack signatures to warn network administrators an attack is under way. A WIPS is similar in operation to a WIDS with the added function of having the ability to also take action to prevent an identified attacker from making unauthorized connection to victim systems.[64]

a. AirDefense Enterprise

AirDefense provides an enterprise class WIPS (see Figure 20) that was the first solution to receive Common Criteria certification and is widely used by U.S. government agencies.[65] AirDefense's product brochure states,

> As a key layer of security, AirDefense Enterprise 7.0 complements wireless VPNs, encryption & authentication. AirDefense Enterprise detects & responds to wireless threats and unauthorized devices on the wireless network using distributed smart sensors (monitoring 802.11 a/b/g) and a secure server appliance. With Common Criteria certification and FIPS compliant cryptography, AirDefense's enterprise-class products scale to support single offices as well as organizations with hundreds of locations around the globe…AirDefense uses collaborative intelligence with secure sensors that work in tandem with a hardened purpose-built

[64] Moerschel et al (2006), p. 600.

[65] Common Criteria certification information pertains to the AirDefense Guard version 3.5 and is available at http://www.commoncriteriaportal.org/public/files/epfiles/ST_VID1025-VR.pdf. A press release from AirDefense at http://www.airdefense.net/newsandpress/08_23_05.php states "AirDefense Enterprise is used by many government agencies… and many other civilian agencies, to protect network data, detect unauthorized devices, mitigate threats and to monitor all wireless activity. [and] as a key component in WLAN architectures which have received DoD DITSCAP accreditation." DITSCAP is the DoD Information Technology Security Certification & Accreditation Process. For additional information about DITSCAP, see http://www.dtic.mil/whs/directives/corres/html/520040.htm.

> server appliance to monitor all 802.11 (a/b/g) wireless traffic in real time for the highest level of security, rogue mitigation and policy enforcement.[66]

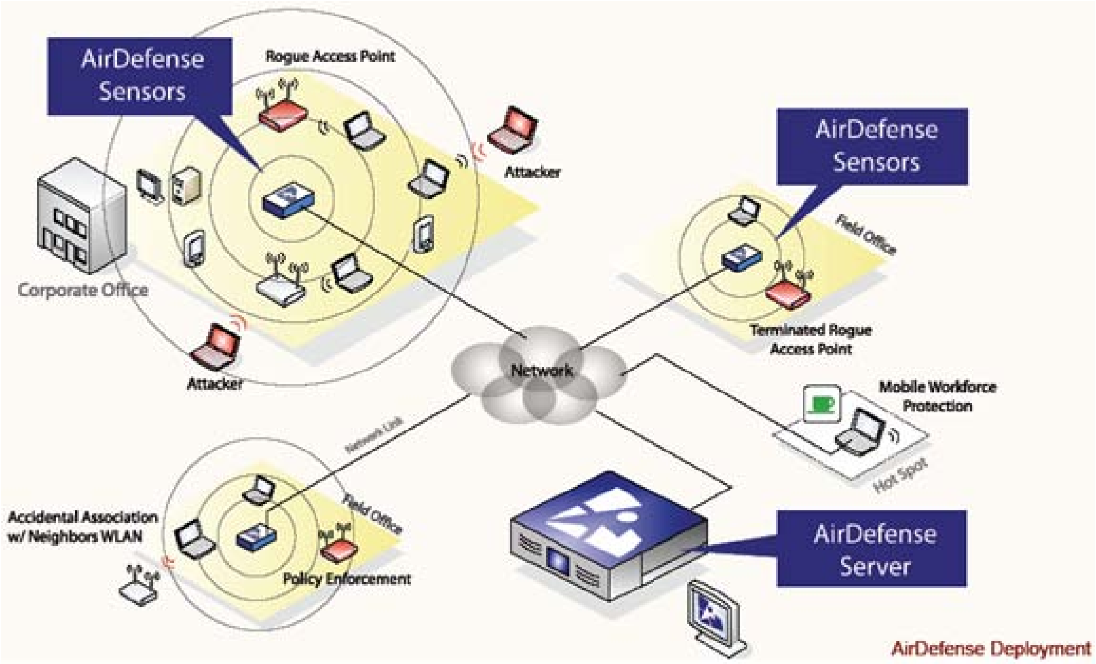


Figure 20. AirDefense Enterprise Deployment (From www.airdefense.net)

b. AirMagnet Enterprise

AirMagnet's product line includes tools for WLAN planning, management, and troubleshooting. These products combine to provide security, improve performance, and ensure compliance with industry-specific regulations. According to AirMagnet's web site, with these solutions

> you always know who has access to your network, what the state of security is, how devices are performing, and more. Most importantly, if something goes wrong you have an expert system that automatically alerts you, identifies and explains each event, and physically locates issues, helping you to immediately solve problems anywhere in the network.[67]

AirMagnet Enterprise 7.5 is more than just a WIPS; it provides management and policy enforcement functions as well. Figure 21 shows the AirMagnet Enterprise architecture which uses their FIPS 140-2 Level 2 validated SmartEdge

[66] AirDefense Enterprise product brochure is available for download from www.airdefense.net after completing a brief information request form.

[67] AirMagnet, https://airmagnet.com/products/, Last accessed August 30, 2006.

Sensors. According to a September 2005 press release, “as the only vendor-independent wireless security solution to achieve FIPS 140-2 certification, AirMagnet Enterprise is the leading choice for government agencies and other organizations and enterprises tasked with guaranteeing the integrity of highly sensitive data.”[68]

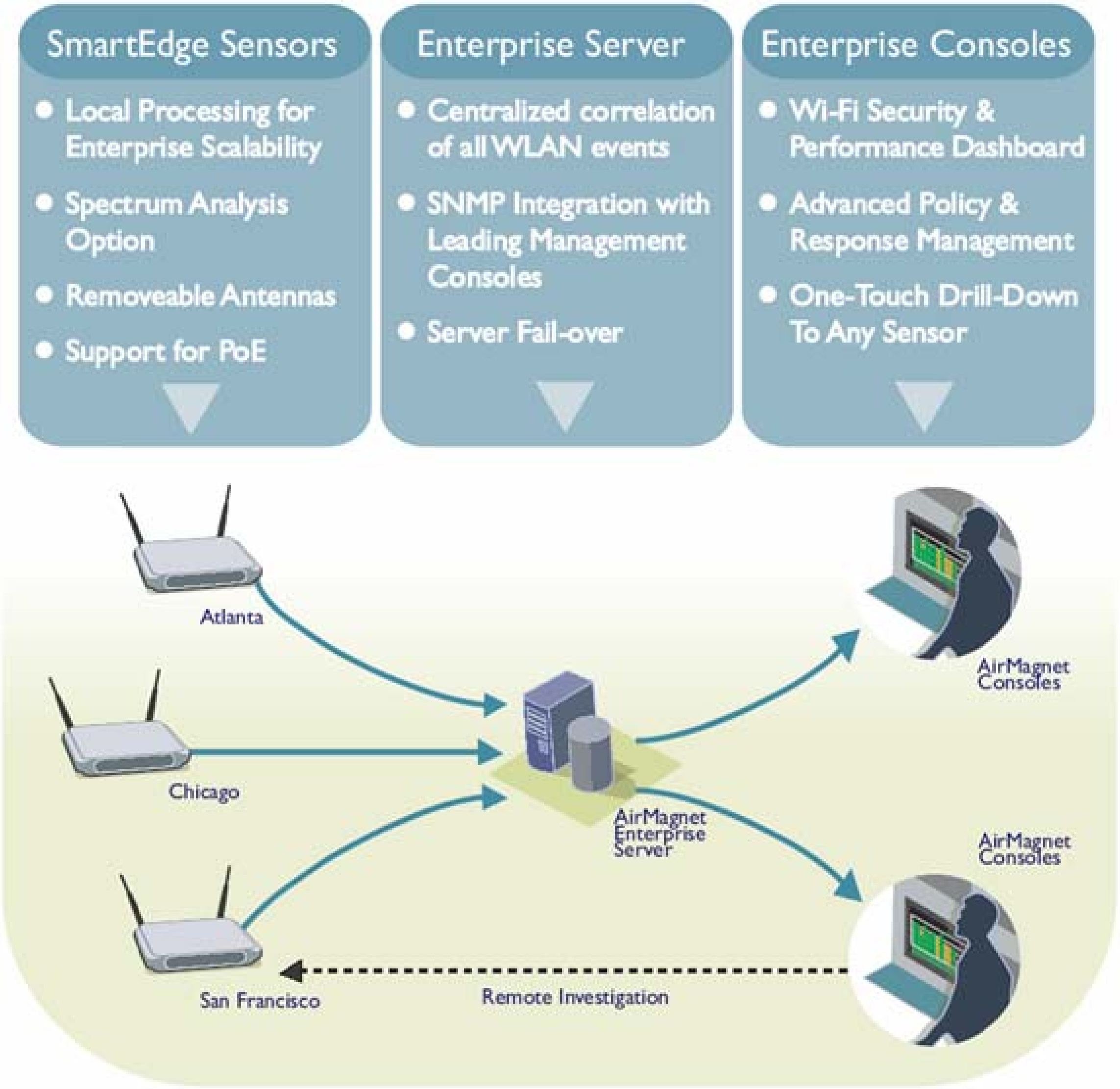

SmartEdge Sensors
● Local Processing for Enterprise Scalability
● Spectrum Analysis Option
● Removeable Antennas
● Support for PoE
Enterprise Server
● Centralized correlation of all WLAN events
● SNMP Integration with Leading Management Consoles
● Server Fail-over
Enterprise Consoles
● Wi-Fi Security & Performance Dashboard
● Advanced Policy & Response Management
● One-Touch Drill-Down To Any Sensor
Atlanta
Chicago
San Francisco
AirMagnet Enterprise Server
AirMagnet Consoles
AirMagnet Consoles
Remote Investigation

Figure 21. AirMagnet Enterprise Solution
(From http://www.airmagnet.com/assets/datasheets/Enterprise_7.5_Datasheet.pdf)

[68] AirMagnet, http://www.airmagnet.com/news/press/news.20050926.htm, Last accessed August 30, 2006.

2. Wireless Management & Control Products

This category of products includes those that specialize in controlling and managing other wireless devices. Major functions include WLAN security policy enforcement and compliance checking as well as control of access points and end user device configuration monitoring.

a. Aruba Mobility Controllers and Management System

Aruba uses their mobility controllers to control their line of wireless APs and to provide encryption, authentication, and other security and management functions. Aruba's Mobile Edge product brochure claims,

> Mobility controllers are high-performance networking platforms built specifically to run centralized ArubaOS functions such as controlled access point management, 802.11 station management, 802.11x [sic] authentication and encryption, site-to-site and client VPNs using IPsec/3DES encryption, stateful policy enforcement firewalls, L1-L7 intrusion protection, endpoint integrity checking, and seamless user roaming between access points and across mobility controllers.[69]

They offer three different models including the Aruba 800, 2400, and 6000 which offer varying levels of scalability and functionality. The Aruba 800 and 6000 are FIPS 140-2 Level 2 validated when running the ArubaOS version 2.4.1.0-FIPS Software.[70]

Aruba's other offering in this category is their Mobility Management System (MMS) which is available as an integrated appliance and as a software application. In conjunction with its Mobility Controllers and Controlled Access Points, the MMS provides a comprehensive suite of applications for planning, monitoring, fault management, reporting, RF coverage and location visualization.[71] Figure 22 shows the Aruba MMS architecture.

[69] Aruba Networks, http://www.arubanetworks.com/pdf/me_prodbrochure.pdf, Last accessed August 30, 2006.

[70] See FIPS 140-2 Vendor List, http://csrc.nist.gov/cryptval/140-1/1401val2006.htm#649 for details. Last accessed August 30, 2006.

[71] Aruba Networks Mobility Management System Product Brochure is available at http://www.arubanetworks.com/pdf/mms.pdf, Last accessed August 30, 2006.

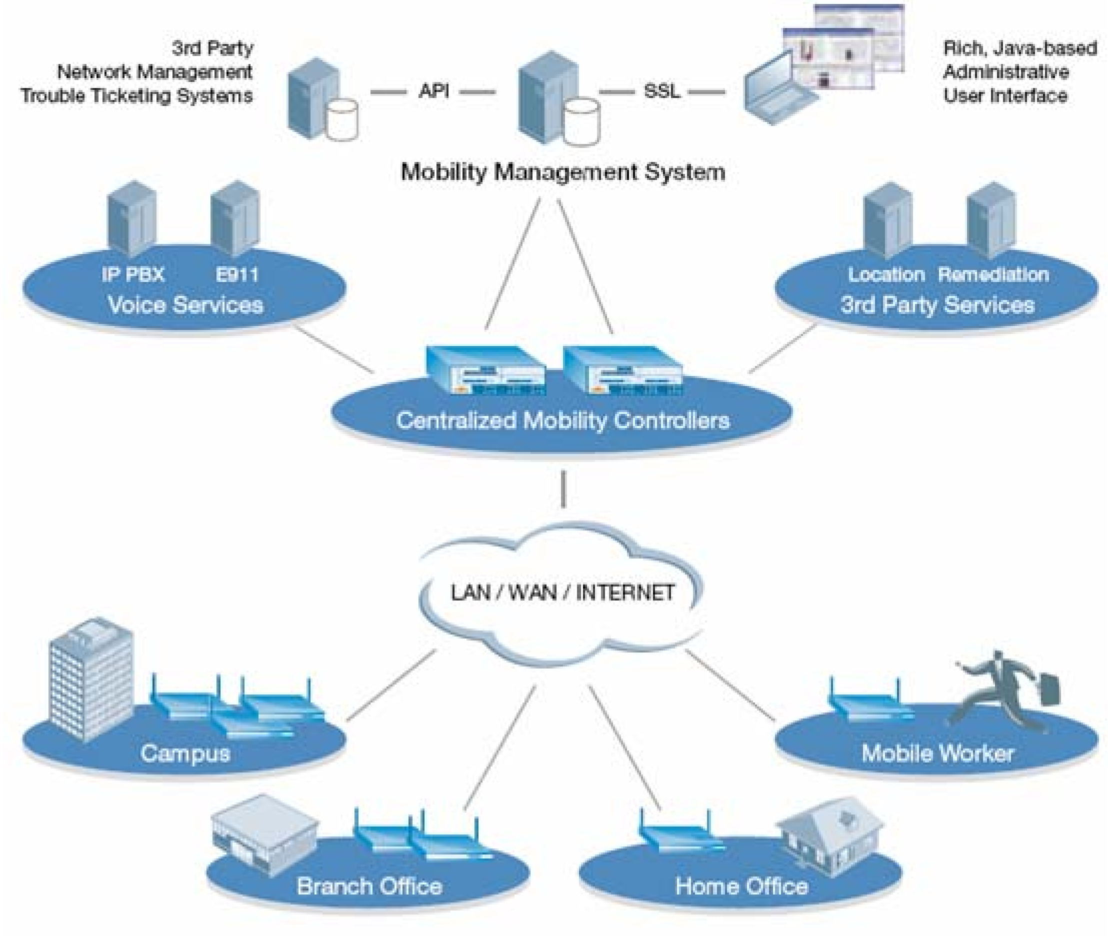


Figure 22. Aruba Networks MMS Architecture (From Ref 59).

b. BlueSocket BlueSecure Controllers

BlueSocket provides a family of WLAN controllers that provide flexible role-based access control and policy enforcement; universal WLAN authentication; strong data encryption; intrusion detection, worm protection and clientless scanning for trusted endpoint security; and security and Quality of Service for VoIP.[72] The BSC 2100 and 5000 controllers are FIPS 140-2 Level 2 validated.[73]

[72] BlueSocket web site, http://www.bluesocket.com/products/controllerfamily.html, Last accessed August 30, 2006.

[73] See FIPS 140-2 alphabetical list of vendors at http://csrc.nist.gov/cryptval/140-1/1401vend.htm, Last accessed August 30, 2006.

c. Cisco Systems

Cisco Systems provides several products that fit into the management and control category. First, Cisco's Network Admission Control (NAC), which is part of Cisco's Self-Defending Network, helps ensure that all wired and wireless endpoint devices (such as PCs, laptops, servers, and PDAs) accessing network resources are adequately protected from security threats.[74] Cisco offers NAC as an appliance and a framework. The appliance provides an end-to-end solution that allows network administrators to authenticate, authorize, evaluate, and remediate wired and wireless users and their machines prior to allowing access to the network. The NAC framework solution is an architecture-based approach that uses the network infrastructure and third-party software to enforce security policy compliance on all endpoints.

Second, Cisco's Wireless LAN Controllers come in stand-alone and modular form. They provide security, mobility, and ease of use to manage from 6 (2000 series and WLAN Controller Module) to 100 (4400 Series) Lightweight Wireless Access Points (LWAP).[75] They each provide centralized security policy management, WIPS capabilities, RF management, Quality of Service, and OSI Layer 3 fast secure roaming for WLANs.

d. Fortress Management and Policy Server (MaPS)

Fortress' MaPS runs as a server on Windows 2000 (Service Pack 4) or Windows Server 2003 and provides centralized management for their Security Gateways and Controllers. Their product brochure lists the following features and benefits:[76]

- Policy Based Management
- Identity Based Access Control
- Centralized monitoring
- User & Device Authentication
- Enterprise Scalability

[74] See Cisco web site, http://www.cisco.com/en/US/netsol/ns466/networking_solutions_package.html for full details on NAC. Last accessed September 2, 2006.

[75] See Cisco web site, http://www.cisco.com/en/US/products/ps6366/index.html for information on the 4400 series; http://www.cisco.com/en/US/products/ps6308/index.html for information on the 2000 series and http://www.cisco.com/en/US/products/ps6730/index.html for information on the WLAN controller module for Integrated Services Routers. Last accessed September 2, 2006.

[76] See Fortress Technologies, http://www.fortresstech.com/products_services/pdfs/maps.pdf for additional details. Last accessed September 2, 2006.

e. Newbury Networks WiFi Watchdog

Newbury Networks WiFi Watchdog™ detects, monitors and secures 802.11-based WLANs. Key features include physical perimeter security and containment; rogue AP and WLAN detection; actionable alerts; client protection and unapproved connection prevention; intrusion detection with precise location; and seamless integration with existing infrastructure (e.g., Cisco, Aruba, Symbol, Trapeze).[77] Using patented location tracking and location based authentication, WiFi Watchdog is able to provide security and authentication for any authorized device joining the network while denying access to unauthorized devices.

F. SUMMARY

This chapter presented a snap shot of some of the COTS wireless security products available on the market as of this writing and is far from exhaustive. In fact, new products are coming on the market almost daily. The reader needs only do a Google search on wireless security to get hundreds of "hits".

The next chapter provides a simple implementation of some of the security practices described in Chapter III (primarily securing the communication path) using some of the products from this chapter. It then concludes with a target architecture for an HFN deployment that uses all three aspects of the AirDefense (2006) three-step method.

[77] Newbury Networks, http://www.newburynetworks.com/products-watchdog.htm, Last accessed August 30, 2006.

THIS PAGE INTENTIONALLY LEFT BLANK

V. A SECURE WIRELESS ARCHITECTURE FOR HFNS

As previously discussed, there are seemingly conflicting requirements for an HFN. The primary concern is rapidly installing a communications network with at least voice and data services that will support the maximum number of users. This implies a requirement for openness which seems to contradict the need for security as discussed in Chapter II. Additionally, an HFN must be easy to install, operate, and maintain with a limited number of onsite personnel. This, too, may seem to fly in the face of security.

One possible solution is to treat the HFN like an enterprise WLAN requiring guest access. While there are some aspects of an enterprise WLAN that are unique (e.g., fixed location, RF over-radiation concerns), it nevertheless serves as a good model for applying wireless security measures to an HFN. The key in an HFN is ensuring that guest access is available to maximize user access, but does not allow guest users to access data or services requiring protection. This ensures that users who provide their own devices (e.g., laptops) are able to join the network, but are properly segmented from other areas of the network requiring protection. One method for ensuring this segmentation is the use of multiple SSIDs and VLANs.

The following sections provide one example of such an implementation. This is an actual implementation that allows for a limited number of users. It incorporates portions of the three step method introduced in Chapter III (primarily step two) and uses some of the COTS equipment detailed in Chapter IV to provide a security solution while still meeting the requirement for openness to allow as many users as possible to join the network. This is the actual architecture currently implemented in the NPS Nemesis MRF. This implementation does not, however, provide for the management component discussed as step three in the AirDefense model shown in Chapter III, but could easily scale to include that capability at a later time.

Finally, this chapter concludes with a target architecture modeled using the Cisco Unified Wireless Network approach. This is a much more robust design for a medium to large scale implementation and would include protection of end points, communication paths, and appropriate monitoring and control.

A. WIRELESS WARFARE LAB & NEMESIS IMPLEMENTATION

Following the AirDefense three-step method introduced in Chapter III, the author designed a small prototype network to meet a set of requirements addressing an HA/DR scenario similar to those introduced in Chapter I. The scope of the implementation is limited to the 802.11 wireless paths in a single node. Due to limited equipment availability, this implementation focuses primarily on the second step or securing the communications channels. Additional hardware and software necessary to fully implement steps one and three are discussed later in the target architecture.

Specifically, this implementation meets the following requirements:

- Secure wireless access to a “protected” set of clients and servers
- Secure wireless access for VoIP phones
- Non-secure guest wireless access with no access to “protected” assets

The solution was implemented using the following equipment:

- Cisco 2811 router with internal HWIC 4ESW & HWIC AP cards running Internetwork Operating System (IOS) version 12.4(2)T[78]
- Cisco 2950 switch running IOS version 12.1(22)EA4 standard image
- Fujitsu P-Series Lifebook laptop running Windows XP Home
- Panasonic CF-48 laptop running Windows 2000
- HP Pavilion DV1000 series laptop running Windows XP Professional
- Cisco AIR-CB21AG-A-K9 PCM/CIA wireless card
- Cisco 7920 Wireless VoIP handset

Figure 23 shows the architecture of this implementation.

[78] HWIC-4ESW is Cisco’s High-Speed WAN Interface Card 4-port Ethernet Switch and HWIC-AP is the internal WAP card with 802.11a + b/g dual radio capability.

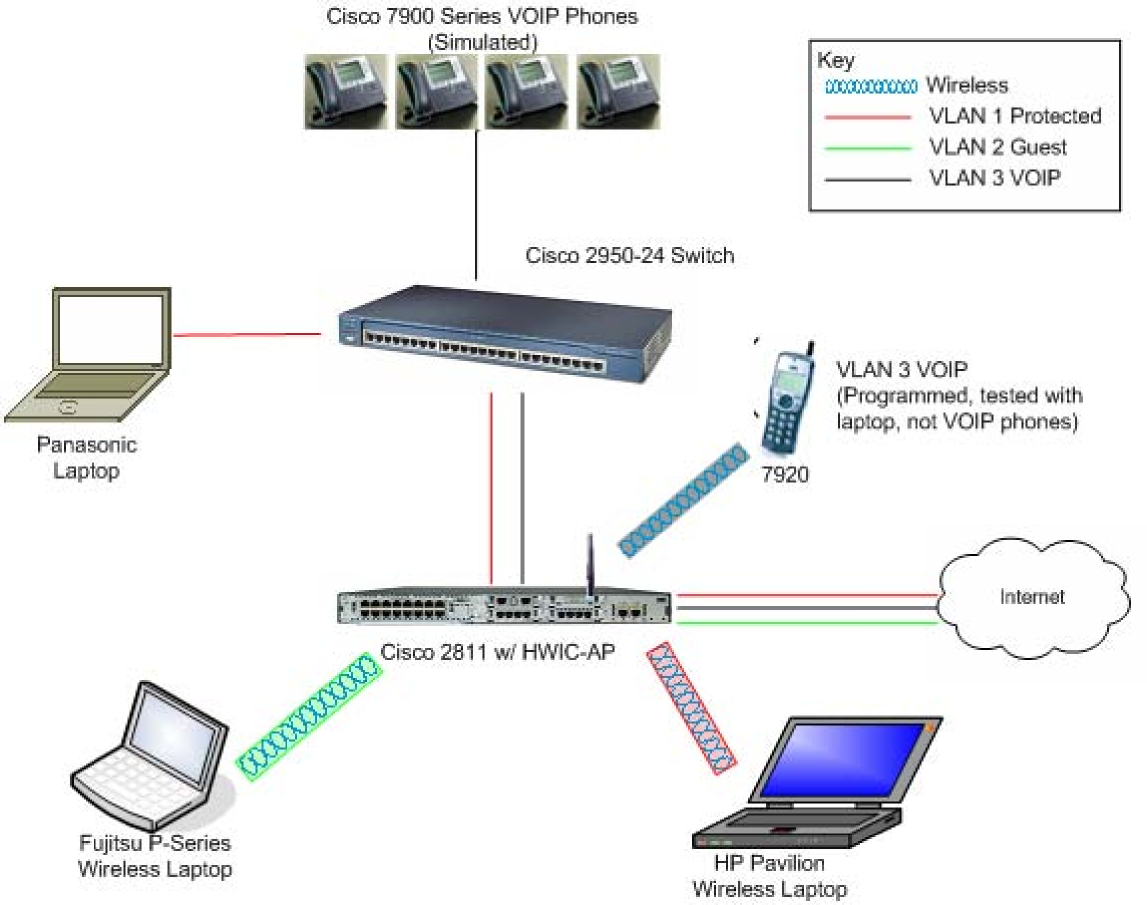


Figure 23. Wireless Warfare Lab Implementation

This solution included programming the Cisco 2811 internal access point with three SSIDs: *data*, *guest*, and *voip*. The *data* SSID was protected with WPA-PSK (pre-shared key); the *guest* SSID had no encryption applied; the *voip* SSID will have WEP applied in a future implementation. Each of these SSIDs were mapped to a separate VLAN programmed within the router: 1 = *data* (protected data); 2 = *guest* (no protection); 3 = *voip* (will have WEP on wireless segment).

The Catalyst 2950-24 switch was programmed with ports 1-16 mapped to VLAN 1; ports 17-20 mapped to VLAN 3; and ports 21-24 as trunk ports for communication with the router and other switches. For this implementation, none of the switch's Ethernet ports were programmed for *guest* VLAN access. Guest access was restricted to only wireless clients.

Next, the router had to be programmed with several access control lists to manage how and where the traffic flowed from the internal access point to the wired ports within the router and on the switch.

This implementation allowed for properly configured wireless clients to join the protected *data* SSID and gain access to the wired workstations. The same approach was used to verify the access for the *voip* SSID and VLAN programming. Due to a lack of availability of the Call Manager Express for the VoIP phones, wireless laptops and a wired workstation were used to verify this step. Finally, wireless clients without the proper security configuration were only able to join the *guest* SSID which was the only SSID being broadcast from the WAP. The author verified this configuration does prevent traffic from the unprotected *guest* SSID/VLAN from being able to access either of the other VLANs.

A similar configuration was then implemented in the NPS Nemesis MRF to facilitate network segmentation and protection of data while providing for wireless guest access. Figure 24 shows the Nemesis implementation. A Cisco Catalyst 3560 switch with power over Ethernet was added to the equipment string to facilitate power to the VoIP phones. This configuration was successfully used to support Exercise Strong Angel III in San Diego, CA from 20-26 August 2006.[79]

[79] Strong Angel III is a disaster-response exercise that simulates a worldwide viral pandemic that stretches emergency response efforts toward the breaking point. At the same time, a terrorist network launches a wave of cyber-attacks that disable communications throughout the United States when they’re needed most. The Nemesis MRF was used to facilitate emergency communications during the exercise. See Strong Angel III web site, http://www.strongangel3.net/, for additional information. Last accessed September 1, 2006.

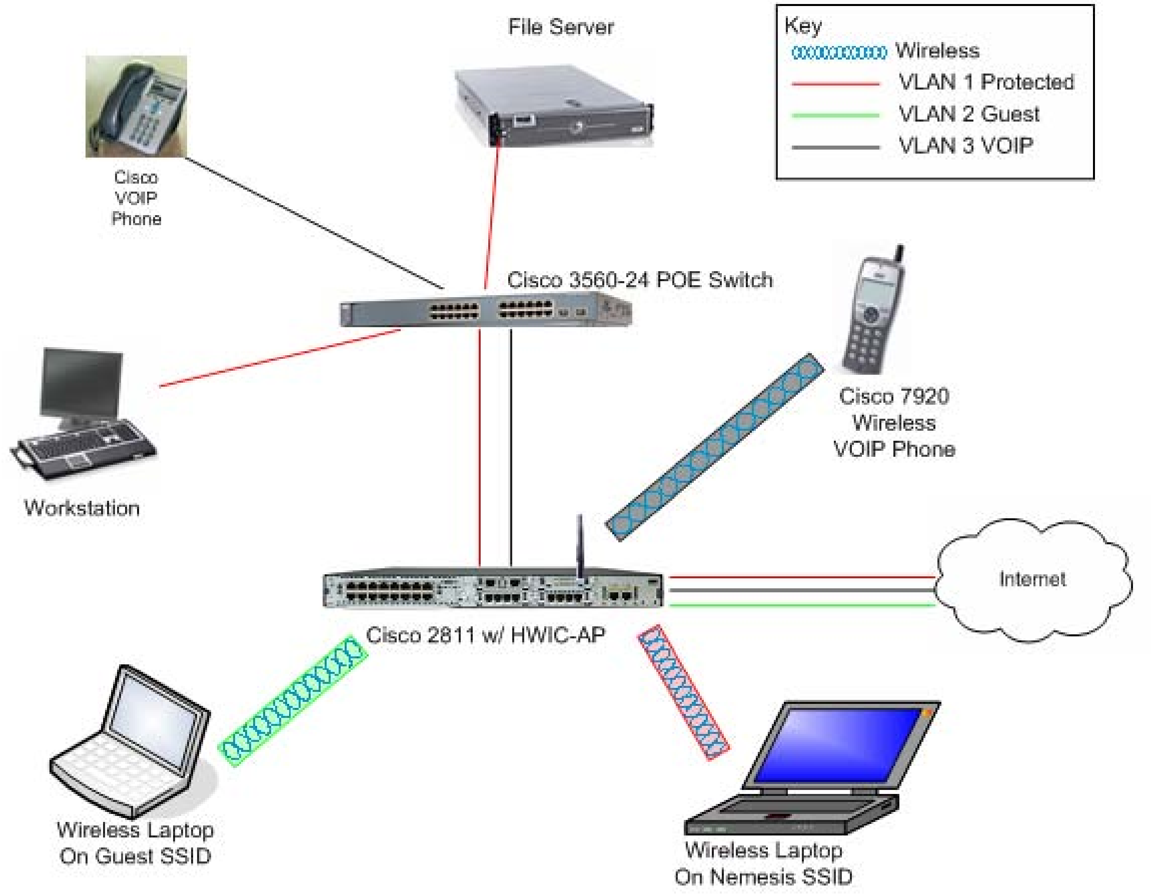


Figure 24. Nemesis VLAN Implementation

These two implementations were quite simplistic and met a limited goal. The next section provides a target architecture for future HFN deployments. It includes suggested additions to the Nemesis MRF and a starting point for the design of Fly Away Kits (FLAK).

B. TARGET HFN ARCHITECTURE

For this target architecture, the author recommends treating the HFN like an enterprise wireless network that has appropriate security measures applied and provides for guest wireless access. Using the Cisco Unified Wireless Network model, with its various security mechanisms, a properly equipped and configured HFN could provide all the desired security attributes introduced in earlier chapters.[80] Figure 25 shows the layered approach used in this model.

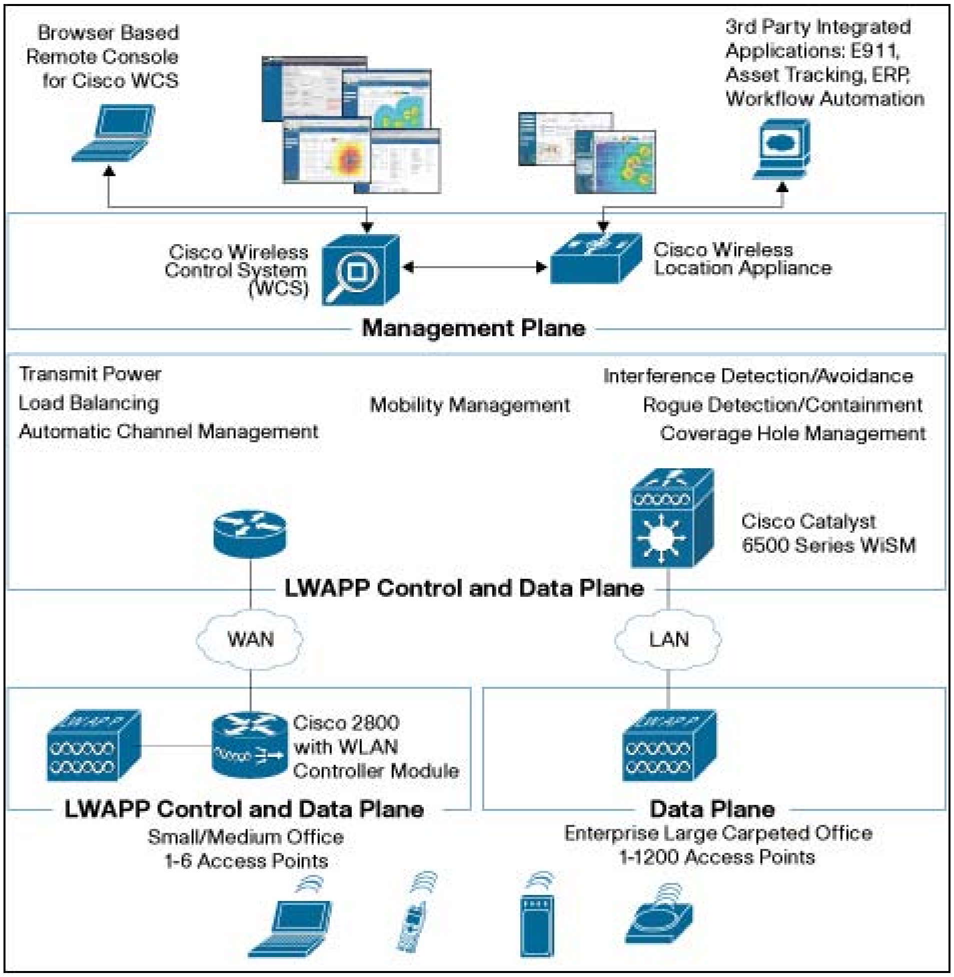

Browser Based Remote Console for Cisco WCS
3rd Party Integrated Applications: E911, Asset Tracking, ERP, Workflow Automation
Cisco Wireless Control System (WCS)
Cisco Wireless Location Appliance
Management Plane
Transmit Power
Load Balancing
Automatic Channel Management
Mobility Management
Interference Detection/Avoidance
Rogue Detection/Containment
Coverage Hole Management
Cisco Catalyst 6500 Series WiSM
LWAPP Control and Data Plane
WAN
LAN
Cisco 2800 with WLAN Controller Module
LWAPP Control and Data Plane
Small/Medium Office
1-6 Access Points
Data Plane
Enterprise Large Carpeted Office
1-1200 Access Points

Figure 25. Cisco Unified Wireless Networks (From www.cisco.com)[81]

[80] See also Cisco's White Paper Titled Best Practices For Outdoor Wireless Security. http://www.cisco.com/application/pdf/en/us/guest/netsol/ns621/c654/cdccont_0900aecd8044059b.pdf, Last accessed September 2, 2006.

[81] See Cisco Systems web site http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/networking_solutions_package.html, Last accessed September 2, 2006.

This implementation fits well for the HFN because of its scalability and centralized management capabilities. Continuing the work this author did with the Nemesis MRF, the next step would involve adding a wireless LAN controller to the Cisco 2811 Integrated Services Router (ISR) (shown earlier in Figure 24). Then, the Nemesis MRF would be able to control up to six LWAPs and would have the ability to deliver centralized security policies, WIPS capabilities, RF management, quality of service, and OSI Layer 3 fast secure roaming for its WLANs.

The next equipment to add to Nemesis would be the six LWAPs (e.g., Cisco Aironet 1500 series mesh LWAPs), a Cisco Wireless Location Appliance, and the Cisco Wireless Control System (WCS). The Wireless Location Appliance uses advanced RF fingerprinting technology to simultaneously track thousands of 802.11 wireless devices from directly within the WLAN infrastructure. This allows not only asset tracking, but also provides location-based alerts for policy enforcement and RF capacity management.[82] Only one of these devices is necessary for any HFN and could, in fact, be deployed forward or kept in the rear at the network operations center (NOC).

According to Cisco's web site, the WCS is the leading platform for wireless LAN planning, configuration, and management.[83] The WCS is an optional component that works in conjunction with LWAPs, WLAN controllers, and the Wireless Location Appliance. With the WCS, administrators have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and WLAN systems management. Cisco WCS runs on a server platform with an embedded database. This provides the scalability necessary to manage hundreds of Cisco wireless LAN controllers, which in turn can manage thousands of Cisco Aironet LWAPs. This allows for the WCS to also be located outside the affected area where the HFN is deployed. Cisco wireless LAN controllers can be located on the same LAN as Cisco WCS, on separate routed subnets, or across a wide-area connection. All Cisco wireless LAN controller models can be managed by Cisco WCS.

[82] See Cisco web site, http://www.cisco.com/en/US/products/ps6386/prod_literature.html for details on the Wireless Location Appliance. Last accessed September 2, 2006.

[83] See Cisco web site, http://www.cisco.com/en/US/products/ps6305/index.html for information about the Wireless Control System. Last accessed September 2, 2006.

Similar configurations could be built into FLAKs. One FLAK should be designed as the network hub or NOC kit. The others should be designed to provide one node with up to six LWAPs and one ISR with Wireless LAN Control Module (WLCM). Figures 26 and 27 show notional equipment stacks for the NOC and node FLAKs. Both notional kits show only the 802.11 wireless and control equipment. One would also need the SATCOM and 802.16 WiMAX equipment to complete the HFN downlink and node-to-node links.

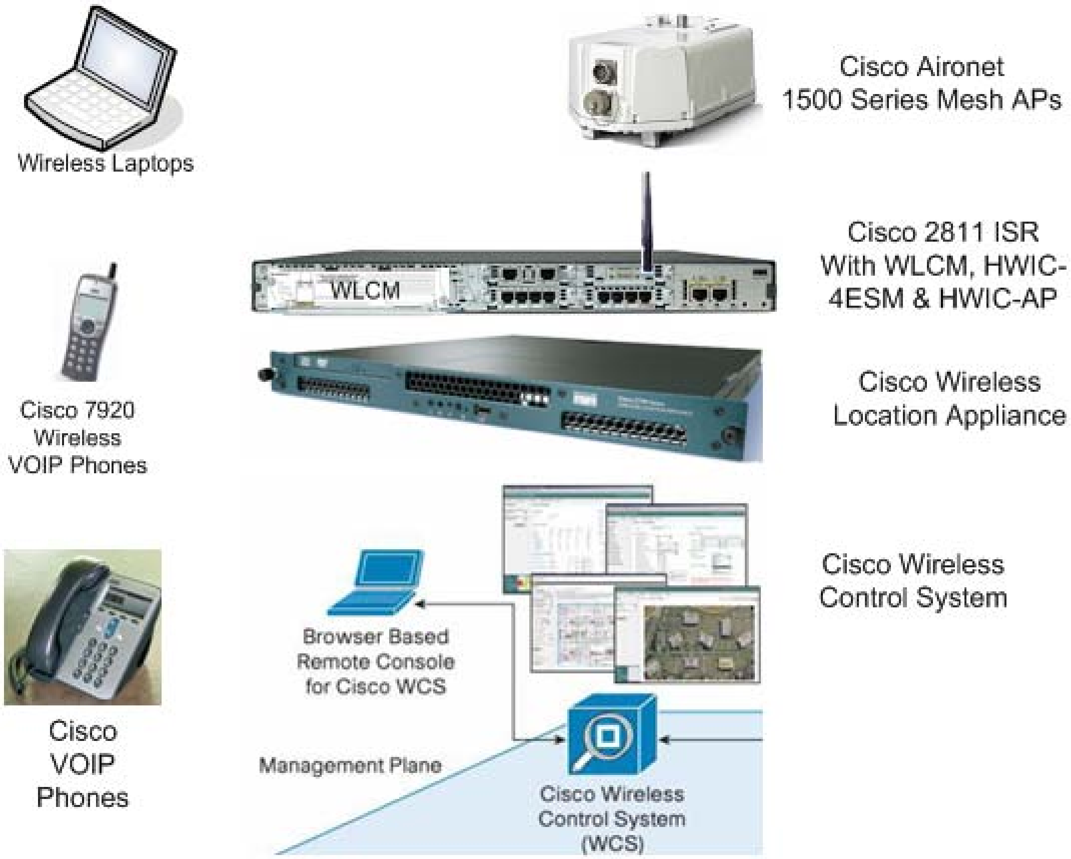


Figure 26. Notional FLAK for Network Operations Center

This NOC kit contains the necessary gear to operate and manage all wireless equipment in the HFN. In addition, it would include local user equipment (e.g., VoIP phones and laptops) for administrators and users at the NOC location.

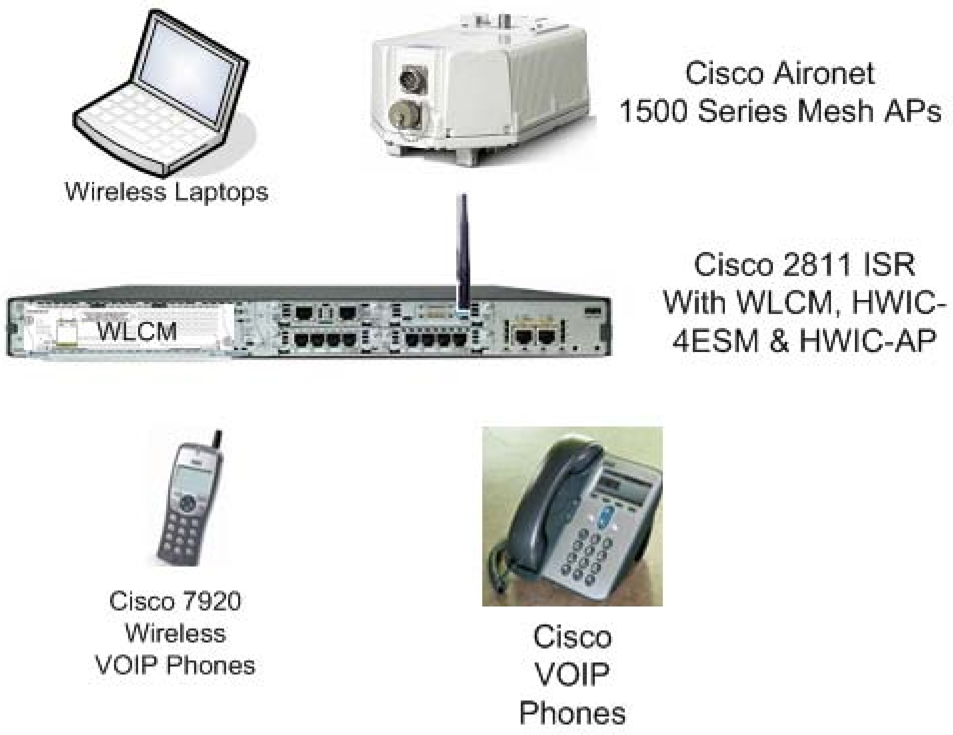


Figure 27. Notional FLAK for HFN Node

The Node Kit would include only a properly equipped ISR and the wireless equipment necessary for establishing the 802.11 cloud. In addition, it should contain at least a couple of VoIP phones and laptops for end users.

This target architecture and notional FLAKs are intended to provide a starting point for additional research and development for future HFN implementations.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSIONS

A. KEY FINDINGS

1. HFNs Have Seemingly Conflicting Requirements

Openness vs. Security! HFNs must be rapidly deployable and must serve the maximum number of users with a minimum amount of labor for installation, operation, and maintenance. Conversely, they do contain information that needs protecting and, therefore, must have at least some level of security implemented. This implementation must be simple and easy to manage either remotely (by experts not in the affected area) or on scene by personnel who are properly trained.

2. HFNs Can Be Treated Like Enterprise WLANs

There are numerous ways to apply security mechanisms to HFNs. Chapter III showed two models for layering security onto wireless networks. Treating an HFN like an enterprise wireless network allows one to use recognized best practices for applying either of those models. To meet the requirement for openness, one can implement a guest access SSID and VLAN to allow open access while segmenting the "untrusted" users from the data you wish to protect.

3. No Single Security Product or Process Can Ensure Total Protection

As the authors of Motorola (2006) point out, wireless security is a combination of people, process, policy, and technology. This thesis focused primarily on the technology aspect of security. There are thousands of existing COTS products that claim to provide wireless network security. As many security experts have previously stated, the best way to implement security is through the concept of Defense in Depth. Therefore, choosing one or more security mechanism from the various categories discussed will improve the overall security on your wireless network.

4. Implementing a WLAN Security Solution for HFNs is a Must

The last thing an HFN should do is complicate the situation it is trying to help. Implementing an HFN without security would almost certainly do just that. This thesis provided an example of an implementation of hardware and software that will provide a measure of wireless security for a future deployment of HFNs. Further work and funding are required, but implementing a rapidly deployable, easily configurable HFN with robust, multi-layer security is definitely achievable.

B. CONCLUDING REMARKS

An HFN, like an enterprise WLAN, should have at least some measure of security implemented. The amount of security provided will be situation dependent; however, not implementing any security could further harm those you are trying to help. At a minimum, any HFN deployed should consider the following to ensure the maximum protection for “private” information within the HFN:

- having protection at the edges by controlling at least some of the end-user devices
- protecting the communications paths by using commercially available encryption mechanisms like WPA, WPA2, or VPNs
- authenticating users or devices via RADIUS or some other authentication mechanism
- monitoring the security and compliance on the network

Providing a guest access SSID is also paramount in situations like the HA/DR scenarios introduced earlier to ensure the maximum number of affected personnel, rescue workers, first responders, volunteers, local government agency personnel, and others have immediate access to voice and data services on the WLAN.

C. AREAS FOR FUTURE WORK

1. Fly Away Kits (FLAKs)

Build and test FLAKs that have the aforementioned security mechanisms implemented. Include wireless mesh technology to allow for rapid expansion of coverage area.

2. Nemesis MRF

Complete the configuration of the Nemesis Mobile Research Facility (MRF) and expand the security mechanisms to include mutual authentication and centralized management. Add Lightweight Wireless Access Points and WLAN controllers to improve scalability for larger implementations.

3. Develop HFN Documentation

A detailed CONOPS, Standard Operating Procedure (SOP) documents, and a WLAN security policy for future HFN deployments would go a long way toward defining measurable processes and thereby enhancing wireless security even more.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

AirDefense, (2006), White Paper: Three Steps for Bullet-proof Wireless LAN Security & Management, http://www.airdefense.net/whitepapers/index.php, Last accessed August 4, 2006.

Blue Ridge Networks, (2005), White Paper: Wireless Security Is Broken And It Doesn't Matter, http://www.blueridgenetworks.com/docs/Wireless_Security_Paper.pdf, Last accessed August 4, 2006.

CipherOptics Solution Note (2005), http://www.cipheroptics.com/pdf/sn-wireless.pdf, Last accessed August 26, 2006.

Committee on National Security Systems Instruction 4009, (2003) *National IA Glossary*

Dodd, J. (2005). Wireless network security. *Smart Computing in Plain English, 16*(11), 72.

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

Department of Defense Directive 8500.1, (2002), *Information Assurance*.

Department of Defense Instruction 8500.2, (2003), *Information Assurance Implementation*.

Edney, J. & Arbaugh, W. A. (2004). *Real 802.11 Security : Wi-Fi Protected Access and 802.11i*. Boston: Addison-Wesley

IEEE 802.11i, (2004), *Amendment 6: Medium Access Control (MAC) Security Enhancements*

Kessel, A. K. & Goodwin, M. S. (2005). *Wireless local area network (WLAN) vulnerability assessment and security.* (M.S. in Information Technology Management, Naval Postgraduate School). , 151. (Springfield, Va. : Available from National Technical Information Service)

Korelc, J. & Tittel, E. (2006). VPNs for Disaster Recovery: IPsec vs SSL. http://searchnetworking.techtarget.com/tip/0,289483,sid7_gci1205030,00.html, Last accessed August 15, 2006.

Knuth, D. (2004). White Paper: A Vendor Neutral Evaluation of Wireless LAN Secure Mobile Solutions. http://www.cwnp.com/pdf/call_wireless_security.pdf, Last accessed August 7, 2006.

Moerschel, G., Dreger, R., & Carpenter, T. (2006). *Certified Wireless Security Professional (CWSP) Study Guide*, (2nd ed.). New York: McGraw-Hill.

Motorola, (2006). White Paper: Building a Secure Foundation for Enterprise Mobility. http://www.motorola.com/Enterprise/contentdir/en_US/Enterprise/Files/White%20Papers/WS_Building_a_Secure_Foundation_White_Paper.pdf, Last accessed August 3, 2006.

Naval Postgraduate School, (2005), *Course Notes for CS3690: Network Security*.

Schneier, B. (2000). *Secrets and Lies: Digital Security in a Networked World*, Indianapolis: Wiley.

Steckler, B., Bradford, B., & Urrea, S., (2005). Hastily Formed Networks for Complex Humanitarian Disasters: After Action Report and Lessons Learned. From http://www.nps.navy.mil/disasterrelief/docs/NPS-Katrina_AAR_LL.pdf, Last accessed August 4, 2006.

Vladimirov, A., Gavrilenko, K., & Mikhailovsky, A. (2004). *Wi-Foo: The Secrets of Wireless Hacking*, Boston: Addison-Wesley.

APPENDIX A SAMPLE WLAN SECURITY POLICY TEMPLATE

This Wireless LAN Security Policy Template © Copyright 2003 Planet3 Wireless, Inc. is included by permission from Devin Akin, Chief Technical Officer.[84]

The template below is included in its entirety, but has been reformatted for inclusion as an appendix in this thesis.

ABOUT THIS TEMPLATE:

Joel Barrett, a Systems Engineer and member of the Enterprise Wireless LAN Technology Leadership Program (TLP) at Cisco Systems, developed this Wireless LAN Security Policy Template.

The purpose of this template is to provide enterprises with a starting point for developing a security policy to apply to the implementation of a wireless network, whether that implementation is yet to be completed, or has been installed already. The point being that any organization that uses wireless LAN technology needs to have a security policy to address the security issues inherent to any wireless LAN installation.

This template is fully printable, can be used on a PDA, allows extraction of contents, but does not allow for editing of the document.

[84] D. Akin, personal communication, August 6, 2006.

INTRODUCTION

Use the following template to build a comprehensive corporate wireless LAN security policy. Each section and subsection contains a heading and then brief instructions or suggestions for what that section should contain. The final result should be integrated with the existing corporate security policy. Organizations may not need all of the sections listed in this template, but we have included a comprehensive list to choose from. The policy may need revision when new wireless network vulnerabilities and/or solutions arrive in the market place. An electronic version (Adobe PDF) of this template is available when you subscribe to the CWNP e-mail newsletter.

GENERAL POLICY

This first section, General Policy, is used as an introduction to why the organization is adding a wireless section to their corporate security policy (its purpose) and what role this policy will play in keeping the network safe from intrusion. Even if the organization has no wireless capabilities, a wireless security policy should be in place to address a minimum of rogue equipment discovery.

Introduction

An introductory section on what the General Policy section covers and how it applies to the organization.

Statement of Authority

Define the authority that put this policy in place.

Executive Sponsorship

List the executive sponsors who back this policy and their contact information.

Emergency Response Team

Large organizations usually have an Emergency Response Team to handle corporate security issues for both facility and network emergencies. List ERT network representatives and the team’s contact information.

Applicable audience

Define the audience to whom this policy applies, including employees, visitors, and contractors.

Scaled down versions of the Wireless LAN Security Policy may be needed for IT staff, end users, visitors, and contractors as an easy-to-read type of “To Do” and “Not To Do” list.

Violation reporting procedures and enforcement

Part of the security policy must address policy enforcement. When policy is violated, there must be a procedure in place to address what actions the organization will take against the individual that violates policy directives. Define and describe what will be done to reinforce policy directives after a violation and what reports will be written by whom and whom they will be given to.

Risk Assessment

Asset Protection

Sensitive Data

List and discuss the organization’s intellectual property, trade secrets, identity information, credit card information, health information, customer databases, and any other information stores that could be jeopardized by wireless network compromise.

Network Services

List and describe email, file, database, directory, custom application services, Internet connectivity, web-based applications, and virus and intrusion detection services that could be compromised by network infiltration.

Threat Prevention

Explain the steps necessary to reduce or prevent wireless network threats, such as:

- Denial of Service (DoS)
- Equipment Damage or Theft
- Unauthorized Network Access
- Credit Card Fraud
- Identity Theft
- Corporate Secret Theft
- Personal Information Exposure
- Malicious Data Insertion

Legal Liabilities

Document legal liabilities that could be incurred in the event of a wireless network compromise and how to react to each type of situation appropriately. These liabilities should also include third party attacks and illegal data insertion.

Note that if exposure to legal liabilities presents a problem that could cost significant amounts of time and money due to an intrusion, then adequate resources should be proactively applied to the security weaknesses.

Costs

Management must consider costs involving people, training, and equipment when implementing wireless LAN security solutions. Keeping quality employees who fully understand the network and its vulnerabilities is especially important. Training is continually required for installation and configuration tasks. Training is imperative to maintaining network operations, end-user capabilities, and security solution upgrades.

This section should give way to Finance & Budget documentation for extensive details, but should outline the importance of appropriate spending to assure security levels are appropriate. List the various expenses that are expected in implementing and maintaining proper wireless network security.

Impact Analysis

An Impact Analysis should be performed so that administrators understand the degree of potential loss involved in a network compromise. The following items, as a minimum, must be considered during the Impact Analysis:

- Financial Loss
- Data Loss
- Loss of Customer Confidence
- Reputation Damage
- Regulatory Effects

Policy should address accessing the network from outside the organization, especially from public access locations (i.e., wireless hot spots).

Security Auditing

Independent Testing

This section is about hiring external consultants to perform independent security testing of wireless network systems. This step is often taken after internal resources and knowledge have been exhausted or to get a fresh perspective on security design and solution selection. The tests allowed to be performed by the consultant should be documented and cleared through internal legal channels. Any anticipated vulnerabilities or limitations of the security solutions chosen should be documented before the auditor begins any testing.

Sources of Information

There are many tools hackers can employ to infiltrate wireless networks. Audits should employ as many of these tools as possible:

- Wireless LAN Discovery
- Password Capture & Decrypt
- Share Enumerators
- Network Management & Control
- Wireless Protocol Analyzers
- Manufacturer Defaults
- Antennas & WLAN Equipment
- OS Fingerprinting & Port Scanning
- Application Layer Analyzers
- Networking Utilities
- Network Discovery Tools
- RF Jamming Tools
- Hijacking Tools
- WEP Decryption Tools
- Operating System Exploit Tools

List and describe the tools that are, have been, or will be used in auditing the wireless segment of the network.

FUNCTIONAL POLICY – GUIDELINES AND BASELINES

Policy Essentials

Policy Change Control and Review

Contacts and Responsibilities

Include the specific contacts and their responsibilities for policy change control management.

Change Management Procedures

List the specific procedures for making changes to organizational policy.

Change Control Enforcement

Describe the procedures when enforcing organizational policy change control.

Password Policy

Guidelines

Create guidelines that help users implement strong passwords and help administrators enforce password policy.

Password Implementation

If passwords are used as a security mechanism, set password policies for the following network devices as a minimum.

- Access points
- Wireless client software
- Other wireless infrastructure devices
- Windows platforms
- Linux/Unix platforms
- VPN solutions
- Applications

Networking Staff and End User Employee Training Requirements

Networking Staff

Explain training requirements for the networking staff.

End Users

Explain training requirements for end users.

Non-Employee Wireless Access

Visitors

Explain access restrictions for visitors.

Consultants

Explain access restrictions for consultants.

Acceptable Use Policy

Acceptable Use

Explain acceptable uses of the wireless network.

Unacceptable Use

Explain unacceptable uses of the wireless network.

Violation Enforcement

Define the methods used to enforce the Acceptable Use Policy.

Staging, Implementation, and Management Procedures

Describe the procedures that will be used to maintain consistency when staging, implementing, and managing wireless network devices. These procedures must be readily available and up-to-date when used by support staff to manage the devices. This section may include checklists, interface types used for management, and how the wireless infrastructure will be installed.

Auditing and Compliance

Internal recurring process by support staff

Support staff must perform penetration testing and reporting, vulnerability scanning, and risk assessments on an ongoing basis. Audits should follow the policies established in the Risk Assessment section of the Wireless LAN Security Policy. Define established timelines and processes for recurring internal audits.

External periodic process by independent professionals

Independent professionals should be considered as a valid periodic method of performing penetration testing and reporting, vulnerability scanning, and risk assessments. Define established timelines and processes for recurring external audits.

General Guidelines

Security Checklist

Create a security checklist that addresses the expectations of the security policy. This checklist will be used during product staging, implementation, and management to verify configuration parameters are set correctly. This checklist should comply with the Baseline Practices section below.

Available Network Resources

Define the restrictions that wireless users have compared to wired network users regarding use of existing network resources. It is not always necessary to give wireless users the same level of access to network resources as wired users.

Asset Management

Describe the asset management practices in place and how they affect the wireless network. This may include an intrusion detection and management software package or similar asset management tool.

Periodic Inventory

Show the organization's inventory schedule and the team responsible for the schedule.

Change Management

Make appropriate annotations about how existing change management procedures should include wireless LAN infrastructure devices. This should list the steps to be followed in order to properly implement a change on the wireless network so as to assure adherence with all sections of this policy.

Spot-checks & Accountability

Perform regular spot checks to prevent rogue access points and similar devices and to verify policy compliance. End users and network staff should be held accountable to the corporate policy. Establish timelines and processes for conducting spot checks.

Baseline Practices

Establish baseline practices to help create operating procedures and implementation checklists for wireless LAN equipment and security. These areas need to be considered:

- Access point default SSID modification
- MAC filtering
- Use of static WEP
- Default access point configuration modification
- Firmware upgrades for wireless network equipment
- Rogue equipment
- Outdoor bridge security
- RF cell sizing and AP placement
- SNMP configuration
- Discovery protocol configuration
- Remote access configuration
- Client configuration
- IP services configuration
- AP network connectivity
- Pre-deployment staging and testing
- Equipment installation

FUNCTIONAL POLICY – DESIGN AND IMPLEMENTATION

Interoperability

Consider solutions that interoperate and document how interoperability affects purchasing decisions. For example, if 128-bit WEP is chosen as a security solution and multiple wireless LAN infrastructure equipment providers are used, then interoperability testing should be performed before an enterprise rollout is attempted and before a large amount of equipment is purchased.

Layering

If solutions that use different layers of the OSI model are used, it is important to document which solution types will be used and to assure that they have been tested together. An example of this is using 802.1x/EAP (Layer 2) solutions with IPSec (Layer 3). Define policy for implementing layered security solutions.

Segmentation & VLANs

Wireless LANs should be segmented from the wired network backbone by an appropriate security solution. Wired and wireless VLANs offer a method of segmenting users and networks. The importance of segmentation should be explained here, and the type(s) of segmentation solution required to properly secure the network should be listed. Any necessary security and mobility features should be documented here.

Authentication & Encryption

Choose and document authentication and encryption types based on existing implementations, data sensitivity, scalability, availability, and access control.

Existing Implementations

Authentication system integration with existing user databases and authentication systems and support for the latest standards, security features, and protocols is paramount. Existing equipment may not be able to support the latest available encryption, so an evaluation of the level of security provided by these more legacy devices is warranted. Describe and document the current level of encryption on existing systems and devices.

Data Sensitivity

Define and document authentication and encryption solutions that support the required level of security. Keep in mind that authentication systems do not typically provide data payload encryption. In most cases, authentication and data encryption must be handled by separate mechanisms.

Scalability & Availability

Security solutions should be scalable and provide a high degree of availability for users. Wireless networks allow employees to be mobile which means that new ways of using the network will be found. This will translate into increased network usage and dependency on the network. The network's design should lend itself to ease of growth at a reasonable cost. Define and describe the levels of scalability and availability that are required for the wireless network to grow with the organization.

Access Control

Having a wide range of devices types may dictate a degree of flexibility in choosing security solutions. Create corporate security solutions that can handle access control for a variety of wireless network device types, manufacturers, and operating systems. Solutions may include client and server software applications that run on various operating systems, authentication and encryption appliances, and a plethora of infrastructure devices such as access points, workgroup bridges, and wireless bridges. Access may be controlled based on roles, groups, device types, etc. Define and document the different levels of access control to be implemented on the wireless network segment.

FUNCTIONAL POLICY – MONITORING AND RESPONSE

Physical Security

Address unauthorized visitors in the facility's physical security policy. Physical access and security of wireless infrastructure devices is extremely important in preventing hackers from entering the facility to place their own wireless devices onto the network and to keep thieves from stealing equipment or accessing console ports of infrastructure devices. Define and describe the facility's physical security required as a result of implementing the wireless network.

Rogue Access Points & Ad Hoc Networks

Prevent rogue access points and Ad Hoc networks inside the corporate work area. A well-defined wireless security policy can help prevent most rogue access points – whether placed by employees or intruders. Make periodic manual scans or have a wireless IDS in place to detect unauthorized equipment. Define and describe the regularity and processes for preventing and detecting rogue wireless devices.

RF Jamming

RF jamming should be addressed so that network administrators understand how to recognize and appropriately react to unintentional and intentional jamming of any kind – to include spread spectrum and narrowband. Explain how RF jamming is accomplished and explain appropriate preventative or responsive steps.

Data Flooding

Give end users a clear definition of what it means to be a good wireless network user. End users may inadvertently flood the wireless network when downloading large files. Help end users understand what should and should not occur over the wireless LAN. Explain baselining as a task to be performed by the network administrator, and reinforce the importance of maintaining baselines over time and changes to the network. Explain how baselines are to be used as a comparative tool to help identify network attacks. Explain how data flooding is accomplished, and list any preventative steps.

Social Engineering

Ensure employees are aware of the data they are making available to others and what hackers might do with the knowledge they gain from that data. Train end users in the proper handling of social engineering tactics, such as:

- Dumpster diving
- Phone calls
- Email
- Instant messaging
- Onsite Visits

Prevention

Teach employees how to prevent intrusion attempts by verifying identification, using secure communication methods, reporting suspicious activity, establishing procedures, and shredding corporate documents. Define established procedures for employees to report or respond to various types of attacks.

Audits

Employ external consultants to perform periodic audits and social engineering attempts to test employees and the network security. Define regularity of audits by external consultants.

Reporting

Develop clear procedures for who is responsible for generating reports and who reviews the reports. Timely, accurate, and comprehensible reports are essential in future attack prevention and pinpointing hacker activity. Define and describe the types of reports, details within the reports, and proper archival of all reports for historical reference.

Response Procedures

Define the steps to take after an intrusion has been recognized. Recommended steps should include a minimum of the following:

- Positive identification
- Confirmed attack
- Immediate action
- Documentation
- Reporting

WLAN SECURITY POLICY APPENDICES (AS NEEDED)

Glossary

Include a glossary to define words readers may not understand or those that require further clarification.

Whitepapers

Include any applicable industry whitepapers that may help during implementation, analysis, prevention, or recovery.

Education / Certification

List any classes, self-study materials, and certifications that would be beneficial to employees (end users and IT staff) toward the goal of securing the wireless network.

APPENDIX B RESOURCES FOR FUTURE RESEARCH

The following is a list of references and other resources the author found useful during the research phase of this thesis. It includes various publications and web sites that were not necessarily cited in the body of the thesis, but are very useful for further research in the area of wireless security.

Department of Defense Directives, Instructions, and Guides:

All available at http://www.dtic.mil/whs/directives/.

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

Department of Defense Directive 8500.1, (2002), *Information Assurance*.

Department of Defense Instruction 8500.2, (2003), *Information Assurance Implementation*.

Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIG) including those specifically targeted at wireless implementations. Available at http://iase.disa.mil/stigs/stig/.

Other Federal Government Publications and Guides:

National Institute of Standards and Technology Special Publication 800-48, *Wireless Network Security, 802.11, Bluetooth, and Handheld Devices.* Available at http://csrc.nist.gov/publications/nistpubs/index.html.

National Security Agency Security Configuration Guides. Available at http://www.nsa.gov/snac/downloads_wireless.cfm?MenuID=scg10.3.1.

IEEE Standards

IEEE 802.11 LAN/MAN Wireless LANS series. Available at http://standards.ieee.org/getieee802/portfolio.html.

IEEE 802.1X IEEE Standards for LAN and MAN--Port-Based Network Access Control. Available at http://standards.ieee.org/getieee802/802.1.html.

Wireless Security Vendor Web Sites

Vendor Name	Web Site
3e Technologies International	www.3eti.com
AirDefense	www.airdefense.net
Airespace	www.airespace.com
AirMagnet	www.airmagnet.com
Aruba Networks	www.arubanetworks.com
Blue Ridge Networks	www.blueridgenetworks.com
BlueSocket	www.bluesocket.com
CipherOptics	www.cipheroptics.com
Cisco Systems	www.cisco.com
Cranite Systems	www.cranite.com
EFJ, Inc: (new parent company of 3eTI)	www.efji.com
Fortress Technologies	www.fortresstech.com
Juniper Networks	www.juniper.net
Newbury Networks	www.newburynetworks.com
Phoenix Technologies	www.phoenix.com

Other Wi-Fi Related Web Sites

Common Criteria Certified Products

http://www.commoncriteriaportal.org/public/consumer/index.php

FIPS 140-2 Validated Products

http://csrc.nist.gov/cryptval/140-1/1401vend.htm

Info Security Products Guide (Wireless)

http://www.infosecurityproductsguide.com/products/wireless.html

Network World Wireless Security

http://www.networkworld.com/topics/wireless-security.html

Wi-Fi Alliance

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

Wi-Fi Planet Wi-Fi Products

http://products.wi-fiplanet.com/wifi/recent1.html

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. Chairman, Department of Information Sciences
   Naval Postgraduate School
   Monterey, California