

**A RISK ANALYSIS AND RISK MANAGEMENT
METHODOLOGY FOR MITIGATING
WIRELESS LOCAL AREA NETWORKS (WLANs)
INTRUSION SECURITY RISKS**

BY

HANIFA ABDULLAH

**A RISK ANALYSIS AND RISK MANAGEMENT
METHODOLOGY FOR MITIGATING
WIRELESS LOCAL AREA NETWORKS (WLANs)
INTRUSION SECURITY RISKS**

by

HANIFA ABDULLAH

Submitted in partial fulfillment of the
requirements for the degree

MASTER OF SCIENCE (Computer Science)

in the

**FACULTY OF ENGINEERING, BUILT ENVIRONMENT AND INFORMATION
TECHNOLOGY**

UNIVERSITY OF PRETORIA

APRIL 2006

TITLE: A risk analysis and risk management methodology for mitigating wireless local area networks (WLANs) intrusion security risks

CANDIDATE: Hanifa Abdullah

SUPERVISOR: Prof J.H.P. Eloff

DEPARTMENT: Department of Computer Science

DEGREE: Master of Science in Computer Science

ABSTRACT

Every environment is susceptible to risks and Wireless Local Area Networks (WLANs) based on the Institute of Electrical and Electronics Engineers (IEEE) 802.11 standard are no exception. The most apparent risk of WLANs is the ease with which itinerant intruders obtain illicit entry into these networks. These intrusion security risks must therefore be addressed which means that information security risk analysis and risk management need to be considered as integral elements of the organisation's business plan.

A well-established qualitative risk analysis and risk management methodology, the Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) is selected for conducting the WLAN intrusion security risk analysis and risk management process. However, the OCTAVE risk analysis methodology is beset with a number of problems that could hamper a successful WLAN intrusion security risk analysis. The ultimate deliverable of this qualitative risk analysis methodology is the creation of an organisation-wide protection strategy and risk mitigation plan. Achieving this end using the OCTAVE risk analysis methodology requires an inordinate amount of time, ranging from months to years. Since WLANs are persistently under attack, there is a dire need for an expeditious risk analysis methodology. Furthermore, the OCTAVE risk analysis methodology stipulates the identification of assets and corresponding threat scenarios via a brainstorming session, which may be beyond the scope of a person who is not proficient in information security issues.

This research was therefore inspired by the pivotal need for a risk analysis and risk management methodology to address WLAN intrusion attacks and the resulting risks they pose to the confidentiality, integrity and availability of information processed by these networks.

Keywords risk, risk analysis, risk assessment, risk management, OCTAVE, OODA cycle, wireless local area networks (WLANs), wireless intrusion detection system

ACKNOWLEDGEMENTS

The OODA cycle is the perfect embodiment of an effective human behavioural decision-making cycle, which I adopted for this research endeavour. I *observed* the plethora of fields in information security, I *oriented* myself by creating a mental image of the various avenues I could unearth, I *decided* precisely which areas I would explore and I finally took *action*, resulting in this dissertation.

I moved through various iterations of this cycle and during this nonlinear process, I encountered a number of exceptional people to whom I would like to express my immense gratitude:

- ▣ I owe my *parents* an enormous debt of gratitude for always believing in me and supporting me from the inception of this dissertation. I would never have been able to complete it without their continuous words of encouragement. They are without doubt the greatest *assets* in my life.
- ▣ My sister, *Munira*, was a major source of inspiration and if it were not for her personal sacrifice, I would never have succeeded.
- ▣ The rest of my family, including my *brother*, *sisters* and their respective *families* were instrumental in the accomplishment of this dissertation.
- ▣ A special word of thanks to my promoter, Professor *J.H.P. Eloff*, for his immense dedication and profound interest in my studies.
- ▣ To *Craig Rosewarne* from Concilium Technologies, Centurion, South Africa and *Russell Young* from Blue Turtle Technologies, Midrand, South Africa for demonstrating the AirMagnet and AirDefense Enterprise Wireless Intrusion Detection/Prevention systems respectively.
- ▣ My colleagues at the *University of South Africa (UNISA)* for affording me the time to work on my studies and for providing valuable insight into this dissertation.

BRIEF CONTENTS

PART O: BACKGROUND

1.	INTRODUCTION.....	2
----	-------------------	---

PART I: TOWARDS UNDERSTANDING AND IMPROVING THE OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY FOR MITIGATING WLANs INTRUSION SECURITY RISKS

2.	AN EXPOSITORY OVERVIEW OF THE OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY	12
3.	THE OODA-OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY FOR MITIGATING WLANs INTRUSION SECURITY RISKS	32

PART II: WLAN INTRUSION SECURITY RISK ANALYSIS

4.	OBSERVATION: KNOWLEDGE ELICITATION.....	46
5.	ORIENTATION: TECHNICAL VULNERABILITY ASSESSMENT AND RISK IMPACT.....	79
6.	DECISION: PROTECTION STRATEGY AND RISK MITIGATION PLAN.....	94

PART III: WLAN INTRUSION SECURITY RISK MANAGEMENT

7.	ACTION: POST-OCTAVE ACTIVITIES.....	131
----	-------------------------------------	-----

PART IV: CONCLUSION

8.	CONCLUSION AND FUTURE RESEARCH.....	137
----	-------------------------------------	-----

CONTENTS

ABSTRACT.....	IV
ACKNOWLEDGEMENTS.....	V
BRIEF CONTENTS	VI
1. INTRODUCTION	2
1.1 INTRODUCTION	2
1.2 MOTIVATION FOR THIS STUDY	2
1.2.1 THE ESCALATING GROWTH OF WLANs.....	2
1.2.2 THE SECURITY RISKS POSED BY WLANs.....	3
1.2.3 ADDRESSING WLANs SECURITY RISKS	3
1.2.4 MITIGATING WLANs INTRUSION SECURITY RISKS	4
1.3 PROBLEM STATEMENT AND RESEARCH QUESTIONS	5
1.3.1 WHAT ARE THE POSSIBLE TYPES OF INTRUSION ATTACKS THAT CAN BE LAUNCHED ON WLANs?	5
1.3.2 HOW SHOULD A WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE BE CONDUCTED?.....	5
1.3.3 WHAT STEPS MUST AN ORGANISATION TAKE TO ENFORCE THE RESULTS OF A WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE?	5
1.4 RESEARCH LIMITATIONS	5
1.5 TERMINOLOGY USED IN THIS DISSERTATION.....	7
1.6 STRUCTURE OF THIS DISSERTATION	7
2. AN EXPOSITORY OVERVIEW OF THE OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY.....	12
2.1 INTRODUCTION	12
2.2 STRUCTURE OF THIS CHAPTER	12
2.3 DEFINING RISK.....	13
2.4 THE IMPORTANCE OF MANAGING RISK	13
2.5 TOWARDS UNDERSTANDING THE DEFINITION AND OBJECTIVE OF INFORMATION SECURITY RISK ANALYSIS, RISK ASSESSMENT AND RISK MANAGEMENT	15
2.5.1 DEFINITION OF RISK ANALYSIS AND RISK ASSESSMENT	15
2.5.2 OBJECTIVE OF RISK ANALYSIS	17
2.5.3 DEFINITION OF RISK MANAGEMENT.....	18
2.5.4 OBJECTIVE OF RISK MANAGEMENT.....	19
2.6 CONDUCTING A WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE.....	20
2.6.1 THE IMPORTANCE OF CONDUCTING A WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE.....	20

2.6.2	BACKGROUND: A SYNOPSIS OF THE OCTAVE RISK ANALYSIS METHODOLOGY	22
2.6.2.1	PHASE 1: ORGANISATIONAL VIEW	24
2.6.2.2	PHASE 2: TECHNOLOGICAL VIEW	25
2.6.2.3	PHASE 3: SECURITY STRATEGY AND PLAN DEVELOPMENT.....	25
2.6.2.4	ASSESSING THE STRENGTH OF THE OCTAVE RISK ANALYSIS METHODOLOGY.....	27
2.6.2.5	LIMITATIONS OF THE OCTAVE RISK ANALYSIS METHODOLOGY	27
2.7	CONDUCTING A WLAN INTRUSION SECURITY RISK MANAGEMENT EXERCISE.....	28
2.7.1	AUSTRALIAN/NEW ZEALAND STANDARD FOR RISK MANAGEMENT.....	29
2.8	CRITICAL EVALUATION OF THE OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY	30
2.9	CONCLUSION	30
3.	THE OODA-OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY FOR MITIGATING WLANs INTRUSION SECURITY RISKS	32
3.1	INTRODUCTION	32
3.2	STRUCTURE OF THIS CHAPTER	33
3.3	THE OODA DECISION-MAKING CYCLE.....	33
3.3.1	BACKGROUND: A SYNOPSIS OF THE OODA CYCLE.....	33
3.4	ADDRESSING THE WEAKNESSES OF THE OCTAVE RISK ANALYSIS METHODOLOGY	35
3.5	THE OODA-OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY FOR MITIGATING WLANs INTRUSION SECURITY RISKS.....	38
3.5.1	WLAN INTRUSION SECURITY RISK ANALYSIS	38
3.5.1.1	OBSERVATION – KNOWLEDGE ELICITATION	38
3.5.1.2	ORIENTATION: TECHNICAL VULNERABILITY ASSESSMENT AND RISK IMPACT.....	39
3.5.1.3	DECISION: PROTECTION STRATEGY AND RISK MITIGATION PLAN.....	40
3.5.2	WLAN INTRUSION SECURITY RISK MANAGEMENT.....	40
3.5.2.1	ACTION: POST-OCTAVE ACTIVITIES	40
3.6	CONCLUSION	44
4.	OBSERVATION: KNOWLEDGE ELICITATION.....	46
4.1	INTRODUCTION	46
4.2	STRUCTURE OF THIS CHAPTER	46
4.3	TERMINOLOGY USED IN THIS CHAPTER	49
4.4	PREPARATION FOR THE WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE	49
4.5	OBSERVING THE ENVIRONMENT - BACKGROUND: A SYNOPSIS OF WLANs	50
4.5.1	BENEFITS OF DEPLOYING WLANs.....	50
4.5.2	DRAWBACKS OF DEPLOYING WLANs	51
4.5.3	IEEE STANDARDS	52

4.5.3.1	802.11b	52
4.5.3.2	802.11a.....	53
4.5.3.3	802.11g	53
4.5.4	ARCHITECTURE OF WLANs	55
4.5.4.1	INDEPENDENT BSS (IBSS)	55
4.5.4.2	INFRASTRUCTURE BSS	56
4.6	OBSERVING THE INTRUDER: OODA CYCLE OF THE WLAN INTRUDER.....	59
4.6.1	OBSERVATION	59
4.6.2	ORIENTATION.....	59
4.6.2.1	CULTURAL TRADITIONS.....	60
4.6.2.2	PREVIOUS EXPERIENCE.....	62
4.6.2.2.1	WEP.....	62
4.6.2.3	GENETIC HERITAGE.....	63
4.6.2.3.1	WEP.....	64
4.6.2.3.2	Service Set Identifier (SSID)	64
4.6.2.3.3	Mac address filtering.....	65
4.6.2.3.4	AP passwords.....	66
4.6.2.3.5	Simple network management protocol (SNMP) parameters	66
4.6.2.3.6	DHCP setup on wireless routers.....	66
4.6.2.3.7	Default subnet.....	66
4.6.2.4	NEW INFORMATION	66
4.6.2.4.1	802.1x: Port-based network access control.....	67
4.6.2.4.2	802.11 and WPA	68
4.6.2.4.3	Social environment of WLAN intruders.....	70
4.7	DECISION	71
4.7.1	DENIAL-OF-SERVICE (DOS) ATTACKS	71
4.7.2	MASQUERADE ATTACKS	73
4.7.3	PENETRATION OF THE SECURITY CONTROL SYSTEM	74
4.7.4	LEAKAGE.....	75
4.7.5	MONITORING COMMUNICATIONS (EAVESDROPPING)	75
4.7.6	MALICIOUS USE.....	76
4.7.7	REPLAY ATTACKS	76
4.7.8	SOCIAL ENGINEERING.....	77
4.7.9	BRUTE FORCE ATTACKS.....	77
4.8	ACTION.....	77
4.9	OBSERVING ONESELF	78
4.10	CONCLUSION	78

5.	ORIENTATION: TECHNICAL VULNERABILITY ASSESSMENT AND RISK IMPACT	79
5.1	INTRODUCTION	79
5.2	STRUCTURE OF THIS CHAPTER	79
5.3	THREAT ASSESSMENT	81
5.3.1	IDENTIFYING THREATS TO CRITICAL ASSETS.....	81
5.4	TECHNOLOGICAL VULNERABILITY ASSESSMENT	82
5.4.1	IDENTIFY KEY CLASSES OF COMPONENTS.....	82
5.4.2	IDENTIFY INFRASTRUCTURE COMPONENTS TO EXAMINE.....	84
5.4.3	RUN VULNERABILITY EVALUATION TOOLS ON SELECTED INFRASTRUCTURE COMPONENTS.....	86
5.4.4	REVIEW TECHNOLOGICAL VULNERABILITIES AND SUMMARISE THE RESULTS	87
5.5	RISK IMPACT ASSESSMENT.....	89
5.5.1	CREATE NARRATIVE IMPACT DESCRIPTION	89
5.5.2	CREATE RISK EVALUATION CRITERIA	90
5.5.3	EVALUATE THE IMPACT OF THREATS TO CRITICAL ASSETS	91
5.5.4	CREATE RISK PROFILE.....	92
5.6	CONCLUSION	93
6.	DECISION: PROTECTION STRATEGY AND RISK MITIGATION PLAN	94
6.1	INTRODUCTION	94
6.2	STRUCTURE OF THIS CHAPTER	94
6.3	WLAN ENTERPRISE-WIDE PROTECTION STRATEGY AND RISK MITIGATION PLAN	96
6.3.1	CREATION OF A WLAN ENTERPRISE-WIDE PROTECTION STRATEGY.....	96
6.3.2	CREATION OF A WLAN RISK MITIGATION PLAN	96
6.4	JUSTIFICATION OF A WIRELESS IDS FOR MITIGATING WLANs INTRUSION SECURITY RISKS	96
6.4.1	BACKGROUND: A SYNOPSIS OF INTRUSION DETECTION SYSTEMS (IDSS)	97
6.4.2	FUNCTIONS OF A WIRELESS IDS SYSTEM.....	98
6.5	OPERATIONAL DESIGN OF A WIRELESS IDS	99
6.5.1	OBSERVATION	100
6.5.2	ORIENTATION.....	106
6.5.2.1	AIRMAGNET SMARTEDGE SENSORS DETECTION OF WLAN INTRUSION ATTACKS AND POLICY VIOLATION.....	107
6.5.2.2	AIRMAGNET CENTRALISED ENTERPRISE DETECTION OF WLAN INTRUSION ATTACKS AND POLICY VIOLATIONS	113
6.5.3	DECISION.....	123
6.5.4	ACTION.....	123
6.6	WLAN INTRUSION SECURITY RISK ANALYSIS CONCLUDING ACTIVITIES.....	128

6.6.1	PREPARATION TO MEET WITH SENIOR MANAGEMENT.....	128
6.6.2	PRESENTATION OF RISK INFORMATION.....	128
6.6.3	REVIEW AND REFINEMENT OF WLAN ENTERPRISE-WIDE PROTECTION STRATEGY AND WLAN INTRUSION SECURITY MITIGATION PLAN.....	128
6.6.4	CREATION OF SUBSEQUENT STEPS.....	129
6.7	CONCLUSION	129
7.	ACTION: POST-OCTAVE ACTIVITIES	131
7.1	INTRODUCTION	131
7.2	STRUCTURE OF THIS CHAPTER	131
7.3	PLANNING HOW TO IMPLEMENT THE WLAN ENTERPRISE-WIDE PROTECTION STRATEGY AND WLAN INTRUSION SECURITY RISK MITIGATION PLAN	133
7.4	IMPLEMENTING THE PLANS	133
7.5	PROMOTING AWARENESS OF THE PLANS.....	134
7.6	MONITORING THE PLANS FOR EFFECTIVENESS AND PROGRESS.....	134
7.7	CONTROLLING BY TAKING APPROPRIATE CORRECTIVE ACTION FOR ANY VARIATIONS IN THE EXECUTION OF THE PLAN.....	134
7.8	CONCLUSION	135
8.	CONCLUSION AND FUTURE RESEARCH.....	137
8.1	INTRODUCTION	137
8.2	ASSESSING THE DEGREE TO WHICH RESEARCH QUESTIONS HAVE BEEN ADDRESSED	137
8.2.1	WHAT ARE THE POSSIBLE TYPES OF INTRUSION ATTACKS THAT CAN BE LAUNCHED ON WLANs?.....	137
8.2.2	HOW SHOULD A WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE BE CONDUCTED?.....	137
8.2.3	WHAT STEPS MUST AN ORGANISATION TAKE TO ENFORCE THE RESULTS OF A WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE?	140
8.3	EXTENSIBILITY OF RESEARCH	140
8.4	FUTURE RESEARCH.....	141
8.5	CONCLUSION	141
9.	APPENDIX A: ASSESSING THE STRENGTH OF THE OCTAVE RISK ANALYSIS METHODOLOGY.....	143

10. APPENDIX B: ACTIVE AND PASSIVE WLAN DISCOVERY FOR SELECTED AREAS IN SOUTH AFRICA	149
10.1 ACTIVE WLAN DISCOVERY IN V & A WATERFRONT (CAPE TOWN) USING NETSTUMBLER	149
10.2 ACTIVE WLAN DISCOVERY IN MIDRAND USING NETSTUMBLER.....	153
10.3 PASSIVE WLAN DISCOVERY IN EASTERN PRETORIA USING KISMET	154
10.4 ACTIVE AND PASSIVE WLAN DISCOVERY IN SUNNYSIDE, PRETORIA USING AIRMAGNET	157
11. APPENDIX C: WLAN INTRUSION SECURITY ORGANISATIONAL KNOWLEDGE.....	159
11.1 KNOWLEDGE ELICITATION.....	159
11.1.1 IDENTIFY THE MOST IMPORTANT ASSETS.....	159
11.1.2 IDENTIFY AREAS OF CONCERN	160
11.1.3 IDENTIFY SECURITY REQUIREMENTS FOR THE MOST IMPORTANT ASSETS.....	165
11.1.4 CAPTURE KNOWLEDGE OF CURRENT SECURITY PRACTICES AND ORGANISATIONAL VULNERABILITIES	167
12. APPENDIX D: WLAN ENTERPRISE-WIDE PROTECTION STRATEGY	169
12.1 STRATEGIC PRACTICES	170
12.2 OPERATIONAL PRACTICES	174
13. APPENDIX E: DEVELOPMENT OF THE OODA-OCTAVE RISK ANALYSIS AND RISK MANAGEMENT DATABASE	182
14. REFERENCES.....	183

LIST OF FIGURES

Figure 1-1: Graphical depiction of dissertation layout	10
Figure 2-1: OCTAVE phases and processes.....	24
Figure 2-2: OCTAVE risk analysis activities.....	26
Figure 3-1: The OODA cycle	34
Figure 3-2: Reproduction of Colonel John R. Boyd's sketch of the OODA cycle as espoused in his summation, "A Discourse on Winning and Losing" on 28 June 1995	37
Figure 3-3: High-level diagram depicting the OODA-OCTAVE risk analysis and risk management methodology for mitigating WLANs intrusion security risks	38
Figure 3-4: Database for storing WLAN intrusion security risk analysis information	42
Figure 3-5: Database for storing WLAN intrusion security risk management information	42
Figure 3-6: The OODA-OCTAVE risk analysis and risk management methodology for mitigating WLANs intrusion security risks.....	43
Figure 4-1: The role of chapter four within the overall context of the dissertation	48
Figure 4-2: WLAN intrusion security risk analysis preparatory activities	50
Figure 4-3: Addition of Physical and Data Link layers to the OSI model.....	53
Figure 4-4: Format of an IEEE 802.11 frame	54
Figure 4-5: Independent BSS.....	56
Figure 4-6: Infrastructure BSS.....	56
Figure 4-7: An ESS and DSS infrastructure network.....	57
Figure 4-8: Successfully associating with an AP in the sample UNISA WLAN operating environment	58
Figure 4-9: WEP encryption	62
Figure 4-10: MAC address spoofing	65
Figure 4-11: EAP-FAST Authentication at the sample UNISA WLAN operating environment.....	68
Figure 4-12: A Denial-of-service attack using jamming.....	72
Figure 4-13: Rogue access point	73

Figure 4-14: NMap scanning at the sample UNISA WLAN operating environment	74
Figure 4-15: Ethereal scan at the sample UNISA WLAN operating environment	76
Figure 4-16: Obtaining the MAC address of a WNIC.....	78
Figure 5-1: The role of chapter five within the overall context of the dissertation	80
Figure 5-2: Asset-based threat profile for human actors using wireless network access.....	82
Figure 5-3: Topology diagram of the sample UNISA WLAN operating environment	83
Figure 5-4: Identifying key classes of components	84
Figure 5-5: Identifying wireless clients as an infrastructure component.....	85
Figure 5-6: Identifying APs as an infrastructure component	85
Figure 5-7: APs that were detected on the sample UNISA WLAN operating environment.....	86
Figure 5-8: Vulnerability detected on the sample UNISA WLAN operating environment.....	87
Figure 5-9: Report on policy violations	88
Figure 5-10: Impact description for the outcome disclosure.....	89
Figure 5-11: Impact description for the outcome modification.....	89
Figure 5-12: Impact description for the outcome modification.....	89
Figure 5-13: Impact description for the outcome loss/destruction.....	90
Figure 5-14: Impact description for the outcome interruption	90
Figure 5-15: Risk Evaluation Criteria.....	91
Figure 5-16: Impact value for disclosure.....	91
Figure 5-17: Impact value for modification.....	91
Figure 5-18: Impact value for modification.....	92
Figure 5-19: Impact value for loss/destruction.....	92
Figure 5-20: Impact value for interruption	92
Figure 5-21: Asset-based risk profile.....	93
Figure 6-1: The role of chapter six within the overall context of the dissertation.....	95
Figure 6-2: SmartEdge sensor monitoring the sample UNISA WLAN operating environment.....	102
Figure 6-3: AirDefense personal on the sample UNISA WLAN operating environment.....	104

Figure 6-4: Using AirDefense personal to enforce a policy.....	104
Figure 6-5: Managing multiple AirDefense personal agents using the personal manager.....	105
Figure 6-6: Unauthorised AP detected	107
Figure 6-7: DOS (flood association request) attack detected.....	108
Figure 6-8: MAC address masquerading detected	108
Figure 6-9: Unconfigured AP detected	109
Figure 6-10: SmartEdge sensors policy management.....	110
Figure 6-11: Configuration vulnerabilities detected	111
Figure 6-12: Explanation of one of the configuration vulnerabilities.....	111
Figure 6-13: AirMagnet find tool locating an intruding device	112
Figure 6-14: AirDefense multidimensional correlation engine	113
Figure 6-15: AirMagnet Enterprise Console	114
Figure 6-16: AirDefense manager dashboard	115
Figure 6-17: Rogue IDS screen	116
Figure 6-18: Rogue triangulation	117
Figure 6-19: Spectrum analyser identifying RF jamming devices	120
Figure 6-20: AirDefense forensic engine	122
Figure 6-21: Wired port lookup feature of AirDefense Enterprise 7.0	123
Figure 6-22: Operational design of a wireless IDS/IPS using AirMagnet	127
Figure 7-1: The role of chapter seven within the overall context of the dissertation	132
Figure 7-2: Post-OCTAVE activities	135
Figure 9-1: OCTAVE Automated Tool.....	148
Figure 10-1: NetStumbler 0.4.0	149
Figure 10-2: Active WLAN discovery at the V & A Waterfront, Cape Town using NetStumbler	150
Figure 10-3: Signal-to-noise ratio.....	151
Figure 10-4: APs that do not have encryption enabled	152
Figure 10-5: Statistical analysis of War driving at V & A Waterfront, Cape Town	152
Figure 10-6: Active WLAN discovery in Midrand, South Africa using NetStumbler	153
Figure 10-7: Example of APs that have retained their default SSIDs.....	154

Figure 10-8: Using NetStumbler to detect the type of network	154
Figure 10-9: Passive WLAN Discovery in Eastern Pretoria using Kismet.....	156
Figure 10-10: Graphical depiction of APs in Eastern Pretoria.....	156
Figure 10-11: Active WLAN discovery in Sunnyside, Pretoria using NetStumbler	157
Figure 10-12: Passive WLAN discovery in Sunnyside, Pretoria using AirMagnet	157
Figure 11-1: Identify the most important assets	160
Figure 11-2: First area of concern	161
Figure 11-3: Second area of concern	161
Figure 11-4: Third area of concern	162
Figure 11-5: Fourth area of concern.....	162
Figure 11-6: Fifth area of concern	163
Figure 11-7: Sixth area of concern.....	163
Figure 11-8: Seventh area of concern	164
Figure 11-9: Eight area of concern	164
Figure 11-10: Ninth area of concern.....	165
Figure 11-11: Security requirement in respect of integrity.....	166
Figure 11-12: Security requirement in respect of confidentiality.....	166
Figure 11-13: Security requirement in respect of availability.....	167
Figure 11-14: Current protection strategy.....	168
Figure 11-15: Current organisational vulnerabilities.....	168
Figure 13-1: The Entity-Relationship diagram as shown in Microsoft Access 2003	182

LIST OF TABLES

Table 1-1:	Tabular representation of dissertation layout	9
Table 4-1:	Differences between 802.11i and WPA	70
Table 9-1:	Assessing the strength of the OCTAVE risk analysis methodology	148
Table 12-1:	WLAN security awareness and training	170
Table 12-2:	WLAN security strategy	170
Table 12-3:	WLAN security management	171
Table 12-4:	WLAN security policies and regulations	172
Table 12-5:	Collaborative security management	172
Table 12-6:	Contingency planning/disaster recovery	173
Table 12-7:	Information technology security system and WLAN management	174
Table 12-8:	WLAN security system administration and tools	175
Table 12-9:	WLAN security monitoring and auditing	175
Table 12-10:	WLAN authentication and authorisation	176
Table 12-11:	WLAN security: Encryption	177
Table 12-12:	WLAN security architecture and design	177
Table 12-13:	WLAN security: Incident management	178
Table 12-14:	General staff practices	178
Table 12-15:	Technical and operational recommendations	181

CORROBORATING MATERIAL

A CD-ROM has been included at the end of this dissertation. The contents of this CD-ROM include a Microsoft Access 2003 database that includes forms and reports for the retrieval and printing of WLAN intrusion security risk analysis and risk management information.



PART

BACKGROUND

CHAPTER ONE

INTRODUCTION

Wireless is a huge whale floating just beneath the surface. All people are seeing is the tail fluke. But one day it's going to breach, and everyone is going to be surprised at the size of it.

-David Hughes, 1970s Computer Maven

A square graphic with a grey background and a white border. Inside, the number '1' is prominently displayed in a large, white, serif font. The word 'CHAPTER' is written in a bold, black, sans-serif font across the middle of the square, partially overlapping the number '1'. The background of the square is filled with a repeating pattern of small, light grey icons, including arrows and the letter 'c'.

1. INTRODUCTION

1.1 INTRODUCTION

The liberty of being able to gain access to the corporate network without being constrained by a fixed-wired cabling infrastructure has certainly made WLANs an enticing technology. This, in turn, has led to mobile freedom and greater flexibility (McCullough, 2004:8). Large business corporations, government organisations and home users all desire this type of technology but the very nature of WLANs, which is the transmission of signals through the open-air has unleashed an entire spectrum of security concerns (Ciampa, 2001:20) and associated risks ("Best Practices", 2003:1).

The inspiration for this research therefore emanated from the pivotal need for a risk analysis and risk management methodology to address WLAN intrusion attacks and the resulting risks they pose to the confidentiality, integrity and availability of information processed by these networks.

1.2 MOTIVATION FOR THIS STUDY

A number of factors stimulated the research undertaken for this study. The ensuing section discusses these factors.

1.2.1 THE ESCALATING GROWTH OF WLANs

The proliferation and adoption of WLANs in the near future is inevitable as illustrated by the following:

- ▣ Anticipated growth of business wireless data users from "6.6 million at the end of 2001, to more than 39 million in 2006" ("Corporate Use", 2002).
- ▣ Estimated revenue of U.S. \$3 billion from WLAN services offered to an estimated 21 million Americans who will be using this technology in 2007 ("Public Wireless", 2002).
- ▣ 50 million wireless devices projected to be installed on LANs by 2006 (Palmer, 2004:359).

- ▣ WLAN spending by healthcare providers is expected to grow from \$47.8 million in 2002 to \$75.8 million in 2007 (Cruz & Klein, 2004:1).
- ▣ Manufacturers of portable devices already are incorporating 802.11 wireless cards as built-in networking devices (Adelstein, Alla, Joyce & Richard III, 2004:482).

The above statistics and particulars all attest to the fact that WLANs are destined to be a promising technology. It is therefore crucial to address the security issues of these networks. This led to the next motivating factor for this dissertation.

1.2.2 THE SECURITY RISKS POSED BY WLANs

Every environment is susceptible to risks, and WLANs are no exception. According to the CSI/FBI Computer Crime and Security Survey, the only category to indicate an increase in types of attacks or misuse detected in 2005 from 70 respondents is the "abuse of wireless networks" ("Tenth Annual", 2005:14). The broadcasting nature of WLANs, which is the transmission of signals through the open-air rather than in protected cables, has made WLANs more prone to hacker attacks (Miller, 2003:5). This, in turn, has brought about an array of unique security risks not encountered with traditional fixed-wired networks (Lewis & Davis, 2004:10).

This problem is also compounded by the multitude of freely available WLAN hacking tools on the Internet ("Information", 2002:14), as well as the inherent vulnerabilities of WLANs themselves, the most sensationalised being that of the Wired Equivalent Privacy (WEP) protocol, a problem so grave that many companies have decided to abandon wireless networking altogether (Stewart, 2004:367).

WLANs security risks, if not addressed, could ultimately have an adverse effect on the adequate functioning of these networks. This realisation led to the next motivating factor.

1.2.3 ADDRESSING WLANs SECURITY RISKS

The following survey and study results indicate that organisations are not implementing necessary measures to enable them to operate their WLANs in a secure manner:

- ▣ According to a survey conducted by Ernst & Young, in which 1 300 organisations in 55 countries were surveyed, half of the respondents claimed that mobile technologies,

including wireless networks are a security concern but not all of these organisations are taking the necessary steps to manage the risks ("Global Information", 2005:13).

- ▣ A survey conducted by Deloitte revealed that 33% of the respondents have not taken any measures to protect themselves from "internal wireless communications exposures" ("2005 Global", 2005:13).
- ▣ A study conducted by the United States (U.S.) Government Accountability Office (GAO) revealed that federal agencies have to date not completely implemented chief controls such as policies, tools and practices to enable them to operate a WLAN in a secure manner ("Federal Agencies", 2005:1).

There exists an urgent need to implement necessary measures to mitigate WLANs security risks, as these risks can only be mitigated or reduced to an acceptable level rather than being totally eliminated (Park & Dicoi, 2003:60). The most apparent security risk of a wireless network is the ease with which an intruder can access the organisation's internal network (Maiwald, 2003:438). It is therefore essential to focus primarily on *mitigating WLANs intrusion security risks*. This realisation led to the following motivating factor.

1.2.4 MITIGATING WLANs INTRUSION SECURITY RISKS

Deploying appropriate countermeasures can reduce risks to an acceptable level (Ciechanowicz, 1997:223). It is, however, vital to justify the deployment of expensive countermeasures as well as the business incentive for this, through a risk analysis exercise (Fitzgerald, 1995:9; Paul, 2000:122). The prime deliverable of a risk analysis study is the identification of countermeasures for the threats that have been identified (Eloff, Labuschagne & Badenhorst, 1993:598). This indicates that it is necessary to conduct a comprehensive WLAN intrusion security risk analysis exercise, which will facilitate the proposition of suitable countermeasures to reduce WLAN intrusion security risks to a tolerable level.

1.3 PROBLEM STATEMENT AND RESEARCH QUESTIONS

This research recognises the importance of mitigating WLANs intrusion security risks. The problem area can be addressed by considering the following research questions:

1.3.1 WHAT ARE THE POSSIBLE TYPES OF INTRUSION ATTACKS THAT CAN BE LAUNCHED ON WLANs?

One of the most daunting challenges facing the security community is information in the form of intelligence that identifies how the enemy operates (Spitzner, 2003:15). It is therefore necessary to gain an understanding of how WLAN intruders mentally compose themselves for a WLAN invasion attack. Such information will make it possible to construct a taxonomy of the most cited and most probable WLAN intrusion attacks. This is a vital step because security problems must be comprehended and viewed as genuine problems prior to proposing a solution (Fitzgerald, 1995:8).

1.3.2 HOW SHOULD A WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE BE CONDUCTED?

This research question requires an expository overview of a select risk analysis methodology with a view of customising it specifically for conducting a WLAN intrusion security risk analysis exercise.

1.3.3 WHAT STEPS MUST AN ORGANISATION TAKE TO ENFORCE THE RESULTS OF A WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE?

A risk analysis terminates at the point where a recommendation is made to senior management to improve the security posture of the organisation. Actually taking heed of the results entails examining the follow-up activities of the WLAN intrusion security risk analysis exercise.

1.4 RESEARCH LIMITATIONS

The delineating factors of this research include:

- ▣ This dissertation focuses specifically on WLANs based on the IEEE 802.11 standard. Wireless Personal Area Networks (WPAN), such as Bluetooth based on the IEEE 802.15 standard and Wireless Metropolitan Area Networks (WMAN), WiMax or WirelessMan based on the IEEE 802.16 standard, are beyond the scope of this dissertation.

- There are a number of varying WLAN deployment options including but not limited to infrastructure-based, ad hoc and hotspots (Ciampa, 2006:204-205). Since most installations use infrastructure-based WLANs (Housley & Arbaugh, 2003:32; Held, 2003:10), this research is oriented towards a study of infrastructure-based WLANs.
 - There are two risk analysis approaches, qualitative and quantitative (Peltier, 2001:19; Vennaro, 2005:6). A *quantitative* approach hinges upon “numeric exposure estimates for risk” (Lichtenstein, 1996:20) such as monetary values, which are often difficult to obtain since the cost of hardware and software continuously fluctuate. Furthermore, it is difficult to quantify the exact damage a WLAN intrusion attack can cause to something abstract such as the reputation of an organisation. As a result only *qualitative* risk analysis methodologies will be discussed, as this methodology has been proven to be the most frequently used (Nosworthy, 2000:599; Blakley, McDermott & Geer, 2001:102). The assessment of this approach is based on a subjective low/medium/high (Saltmarsh & Browne, 1983:106) basis instead of concrete monetary values.
 - There are three classes of threats (Peltier, 2004:15; Stoneburner, Goguen & Feringa, 2001:13):
 - ▣ Natural threats, such as floods, tornadoes and earthquakes.
 - ▣ Human threats, both inadvertent and malicious.
 - ▣ Environmental threats, such as pollution and liquid leakage.People are the greatest security threat to an organisation regardless of their motive (Parker, 2001:61). People have statistically resulted in the greatest loss to information resources (Peltier, 2004:15). The 2005 Global Security Survey conducted by Deloitte revealed that most security breaches stem from human error or poor operational practices (“2005 Global”, 2005:14). Therefore, for the purpose of this research, *human threats*, either inadvertent or malicious, are discussed.
 - Software tools running on the *Microsoft Windows* operating system are used, as Windows is the prevailing operating system on most desktops (Howlett, 2005:21).
-

1.5 TERMINOLOGY USED IN THIS DISSERTATION

For the purpose of this dissertation, the following definitions apply.

INFORMATION SECURITY

Information Security encompasses the protection of digital information (Ciampa, 2006:256), as well as the crucial elements such as systems and hardware that use, store and transmit the information (Whitman & Mattord, 2004:4).

WIRELESS CLIENT

The term *wireless client* classifies any wireless device such as laptops, personal digital assistants (PDAs) and mobile phone handsets that are equipped with a wireless network interface card (WNIC) and is capable of receiving and transmitting information via radio waves.

WLAN INTRUDER

The term *WLAN intruder* classifies any individual who invades a WLAN without having the necessary privileges to do so. This individual can be an outsider or someone within the organisation. Thus, the term is broadly used with no regard to the origin or intent of the unauthorised individual.

1.6 STRUCTURE OF THIS DISSERTATION

This dissertation consists of four parts, subdivided into a number of chapters, of which parts II and III correlate to the WLAN intrusion security risk analysis and risk management process. The structure of this dissertation is tabulated below (table 1-1).

<p>PART 0: BACKGROUND</p> <p>CHAPTER ONE</p> <p>INTRODUCTION</p>
<p><i>Chapter one</i> serves as a background to the research problem for the dissertation, elaborating on aspects such as the motivating factors for the dissertation, the research limitations, an elucidation of the terminology and the structure of the dissertation.</p>
<p>PART I: TOWARDS UNDERSTANDING AND IMPROVING THE OCTAVE</p> <p>RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY FOR</p> <p>MITIGATING WLANs INTRUSION SECURITY RISKS</p> <p>CHAPTERS TWO AND THREE</p>

CHAPTER TWOAN EXPOSITORY OVERVIEW OF THE OCTAVE RISK ANALYSIS AND RISK
MANAGEMENT METHODOLOGY

Chapter two provides an overview of the OCTAVE risk analysis and risk management methodology. This chapter provides a critical analysis of these processes emphasising areas that need improvement to conduct a WLAN intrusion security risk analysis and risk management exercise successfully.

CHAPTER THREETHE OODA-OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY
FOR MITIGATING WLANs INTRUSION SECURITY RISKS

Chapter three examines the OODA cycle as a model to address the weaknesses of the OCTAVE risk analysis methodology. A new risk analysis and risk management methodology, OODA-OCTAVE is synthesised for mitigating WLANs intrusion security risks.

PARTS II to III

CHAPTERS FOUR TO SEVEN

Chapters four to seven correlate to the distinct phases of the OODA-OCTAVE risk analysis and risk management methodology for mitigating WLANs intrusion security risks. It is advisable for the reader at this stage to read chapter three. This will enable the reader to understand the structure of chapters four to six within the proper context of the WLAN intrusion security risk analysis and risk management process.

PART II: WLAN INTRUSION SECURITY ANALYSIS

CHAPTERS FOUR TO SIX

CHAPTER FOUR

OBSERVATION: KNOWLEDGE ELICITATION

Chapter four, correlating with the observation phase of the OODA cycle entails observing the WLAN operating environment, observing the WLAN intruder and the organisation's exposure to security risks. This provides an insight into the most important assets that require protection as well as the security vulnerabilities of these important assets. Information gathered from these activities is required for the knowledge elicitation phase necessary for the organisational evaluation.

CHAPTER FIVE
ORIENTATION: TECHNICAL VULNERABILITY ASSESSMENT AND RISK IMPACT
<i>Chapter five</i> , correlating with the orientation phase of the OODA cycle, consists of all the analysis activities of the OCTAVE risk analysis methodology. This includes threat assessment, technological vulnerability assessment and risk impact assessment.
CHAPTER SIX
DECISION: PROTECTION STRATEGY AND RISK MITIGATION PLAN
<i>Chapter six</i> , correlating with the decision phase of the OODA cycle, culminates in the organisation's decision to create a WLAN organisation-wide protection strategy and WLAN intrusion security risk mitigation plan that has to be presented to senior management for approval.
PART III: WLAN INTRUSION SECURITY RISK MANAGEMENT
CHAPTER SEVEN
CHAPTER SEVEN
ACTION: POST-OCTAVE ACTIVITIES
<i>Chapter seven</i> , corresponding with the action phase of the OODA cycle, comprises the post-OCTAVE activities. This includes implementation of the WLAN organisation-wide protection strategy and WLAN intrusion security risk mitigation plan as well as enacting the remaining risk management activities succeeding this.
PART IV: CONCLUSION
CHAPTER EIGHT
CONCLUSION AND FUTURE RESEARCH
The dissertation terminates with the concluding chapter, <i>chapter eight</i> , which examines whether the research objectives of chapter one have been satisfactorily attained. The extensibility of this research is examined. This chapter terminates with a reflection of possible areas for future research.

Table 1-1: Tabular representation of dissertation layout

The following diagram (figure 1-1) graphically depicts the structure of this dissertation.

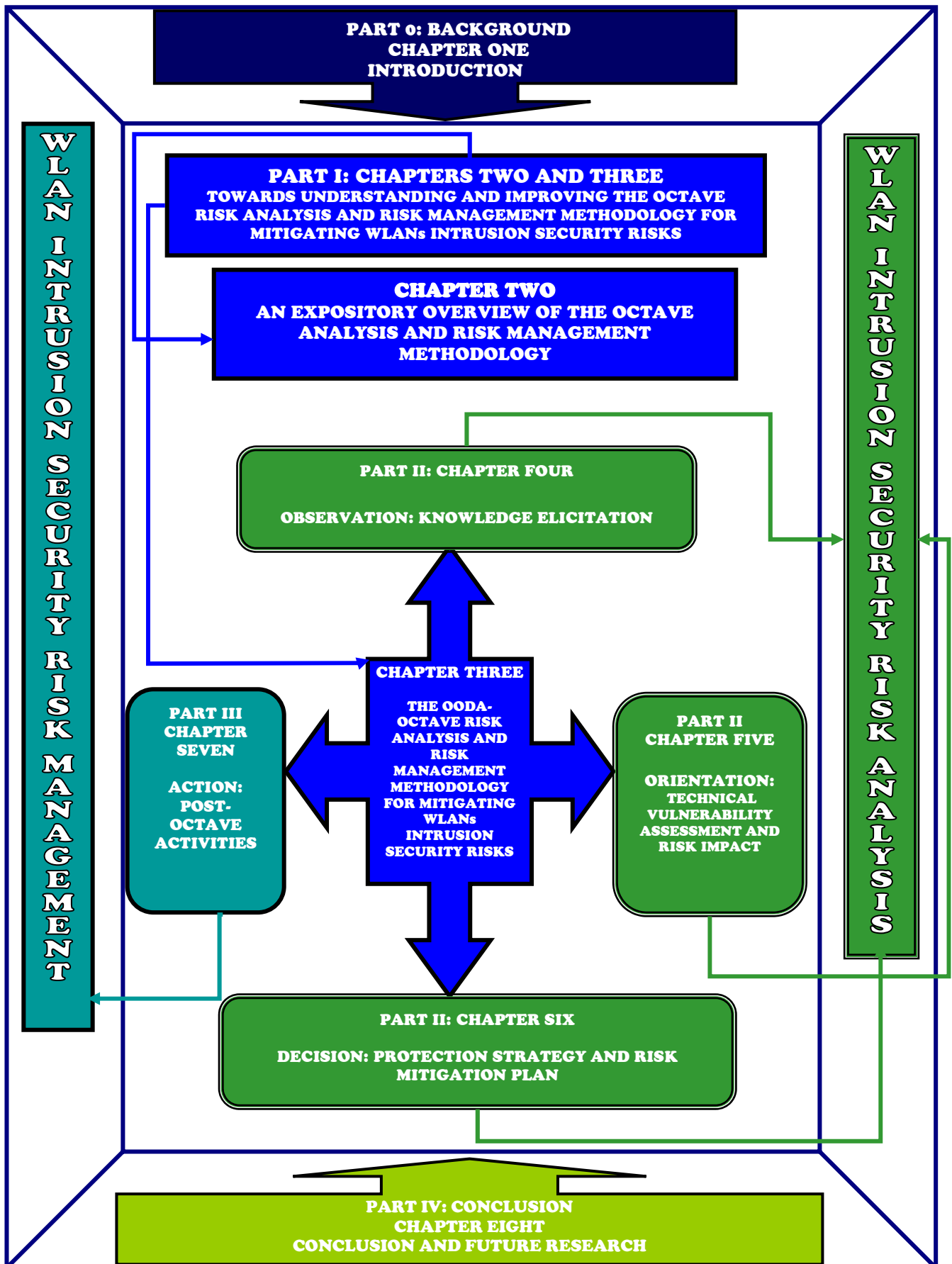


Figure 1-1: Graphical depiction of dissertation layout

PART

TOWARDS UNDERSTANDING AND IMPROVING THE OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY FOR MITIGATING WLANs INTRUSION SECURITY RISKS

CHAPTER TWO

AN EXPOSITORY OVERVIEW OF THE OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY

The average company today is a complex enterprise engulfed by rapid technological change and fierce global competition. You have to assess exposure to risk on an ever changing landscape.

-Arthur Levitt

Chairperson of the U.S. Securities Exchange Commission

CHAPTER THREE

THE OODA-OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY FOR MITIGATING WLANs INTRUSION SECURITY RISKS

*Machines don't fight wars. Terrain doesn't fight wars. Humans fight wars.
You must get into the mind of humans. That's where the battles are won.*

-Col John Boyd

A square graphic with a grey background and a white border. Inside the square, the number '2' is written in a large, white, serif font. The number is slightly offset to the right. The background of the square is filled with a repeating pattern of small, light grey icons, including arrows and symbols, arranged in a grid-like fashion.

CHAPTER

2

2. AN EXPOSITORY OVERVIEW OF THE OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY

2.1 INTRODUCTION

WLANs have "associated security risks that must be addressed" (Thomas, 2004:277). Information security risk analysis and risk management, therefore, need to be considered as integral elements in an organisation's business plan. The level of security in any organisation should be proportional to its risks. However, the concept of *risk* is the least understood concept to pervade the information security domain (Maiwald, 2003:145). This term is often used interchangeably and incorrectly for threats and vulnerabilities, but in reality, a risk "exists when there is a threat and a vulnerability that coincide" (Birch & McEvoy, 1992:50).

Organisations tend to evade considering the fact that security risks can be "controlled or minimised". Important aspects such as risk analysis, risk assessment and risk management, are therefore very seldom topical issues in boardroom agendas (May, 2002:10).

The objective of this chapter is to promote an understanding and improvement of these vital processes in terms of addressing the intrusion security risks of a WLAN operating environment.

2.2 STRUCTURE OF THIS CHAPTER

This chapter commences by defining the term *risk* and addressing the importance of managing risk. Thereafter the multitude of definitions and objectives regarding information security risk analysis, risk assessment and risk management processes are presented, with the view of standardising the meaning and objective of these processes. It is necessary to have a basic understanding of the processes prior to embarking on a comprehensive WLAN intrusion security risk analysis and risk management exercise.

The OCTAVE (Alberts & Dorofee, 2003) risk analysis and risk management methodology is discussed, as this specific methodology will be used for conducting the WLAN intrusion security risk analysis and risk management exercise. This chapter concludes by critically examining the OCTAVE risk analysis and risk management methodology and highlighting areas that need improvement to conduct a workable WLAN intrusion security risk analysis and risk management exercise successfully.

2.3 DEFINING RISK

The definitions of risk contrast based on different cultures, businesses and environments (Wei, Frinke, Carter & Ritter, 2001:1). Within the information security realm, risk is defined as the probability that a threat agent (cause) will exploit a system vulnerability (weakness) to create a loss to the confidentiality, integrity and availability of an asset (Carroll, 1996:459; "Security Risk", 2005:6).

The following concepts from the definition of risk require further elucidation. A *threat* can be defined as any person or object that presents danger to an asset (Whitman & Mattord, 2004:43) whereas a *vulnerability* is a weakness, flaw, hole or anything that may be exploited by a threat that then results in a damaging outcome (Broder, 1984:4; Stephenson, 2004:17). *Availability* is the requirement that enables authorised users continuous access to information and system resources (Bace, 2000:29). *Confidentiality* of information is the assurance that "information is accessible only to those who are authorised to view it" (Mash, 2002:11). *Integrity* is the assurance that a message has not been in any way modified in transmission, either deliberately or by transmission errors (Stanley, 2002:58). An *asset* is something tangible or intangible and of value to an organisation (Nosworthy, 2000:599; Josang, Bradley & Knapskog, 2004:63).

2.4 THE IMPORTANCE OF MANAGING RISK

Comprehending and managing IT security risk is paramount for protecting organisational resources (Gilliam, 2004:296). Managing risk is so important that a host of government and specific regulations (Deloitte & Touche, 2003:8) are in place to enforce various mechanisms to manage risks. The most prominent of these bodies include:

- ▣ The Basel II Capital Accords mandate banks to keep capital reserves explicitly to cover operational risks, including information security risks ("Overview of", 2003).

- ▣ The Federal Trade Commission (FTC), in response to the requirement stipulated by section 501(b) ("FederalTrade", 2002:36484) of the Financial Modernisation Act of 1999, also known as the Gramm-Leach Bliley Act or GLB Act issued a final safeguards rule that forces financial institutions to be liable for risks in each area of their operations. This is stipulated under paragraph b of Section 314.4 of the final safeguards rule ("FederalTrade", 2002:36489).
- ▣ The Sarbanes-Oxley Act of 2002 applies to corporations in the U.S. and abroad. The act requires the issuer of securities publicly traded on the U.S. financial markets to create a risk management model for their stakeholders (Raval, 2004:15).
- ▣ The Health Insurance Portability and Accountability Act (HIPAA) of 1996 establishes a standard for data security in healthcare organisations by outlining a set of technical, physical and administrative security practices to protect electronic patient data (Alberts & Dorofee, 2004:141). This regulation requires each healthcare organisation to conduct a security assessment of the threats that could exploit certain vulnerabilities, thereby gaining access to electronically protected health information (Johnson & Schulte, 2004:48; Geffert, 2004:22).
- ▣ Internal audit functions in the United Kingdom must comply with the 1999 Internal Control Guidance for Directors on the Combined Code (Turnbull Report) on Corporate Governance requirements, published by the Institute of Chartered Accountants in England and Wales to prescribe the undertaking of an analysis of business risks (Nixon, 2005:48).
- ▣ A prime responsibility of agencies under The Federal Information Security Management Act (FISMA) ("Department of", n.d.) is to perform a risk assessment.
- ▣ The South African King II report of July 2001 emphasises the importance of risk management (Veijeren, n.d.).

Prior to embarking on the WLAN intrusion security risk analysis and risk management exercise, it is important to have a general understanding of the terms *risk analysis*, *risk assessment* and *risk management*, as well as to comprehend the objectives of these processes. This is discussed in the next section.

2.5 TOWARDS UNDERSTANDING THE DEFINITION AND OBJECTIVE OF INFORMATION SECURITY RISK ANALYSIS, RISK ASSESSMENT AND RISK MANAGEMENT

The subsequent section surveys the literature to elicit the varying definitions and objectives of the terms risk analysis, risk assessment and risk management. Recurring key term(s) and important concepts for the definitions and objectives are *italicised* and displayed under every definition and objective in order to create a solitary comprehensive definition and objective of the terms risk analysis, risk assessment and risk management. This exercise serves to determine if these concepts are distinct, synonymous or interrelated.

2.5.1 DEFINITION OF RISK ANALYSIS AND RISK ASSESSMENT

Information security risk analysis and assessment has become a large research field since the evolution of network technology (Wei et al., 2001). To obtain a concise definition of the terms risk analysis and risk assessment, it is crucial to analyse the various definitions of these terms as reflected in the literature.

The terms risk analysis and risk assessment are open to a number of definitions including:

- ▣ Risk analysis is "the identification and valuation of assets, the identification of threats and their likelihood of occurrence, the assessment of the vulnerability or weakness and the severity thereof" (Moses, 1992:229-230).

identification and valuation of assets; identification of threats; likelihood of occurrence; assessment of the vulnerability or weakness and the severity thereof

- ▣ Risk analysis is the "process of identifying the risks to an organisation, assessing the critical functions necessary for an organisation to continue business operations, defining controls that are in place to reduce organisational exposure and evaluating the cost of such controls" (Forcht, 1994:420).

defining controls that are in place to reduce organisational exposure and evaluating the cost of such controls

- ▣ Risk analysis "should include threat and vulnerability relationships between business units and should be ongoing rather than periodic" (Babiak, Butters & Doll, 2005:183).

should include threat and vulnerability relationships; ongoing rather than periodic

- ▣ "At the heart of risk management is the evaluation of the potential impact of threats on the ability of a company to continue providing products or services to customers. This evaluation phase of the process is risk assessment (Paul, 2000:122). "Risk assessment is a process for tying together information gathered about business assets, their value and their associated vulnerabilities, to produce a measure of the risk to the business from a given project, implementation or design" (Paul, 2000:122). Risk assessments should also provide justification for the deployment of security controls (Paul, 2000:123).
heart of risk management; this evaluation phase of the process is risk assessment; business assets, their value and their associated vulnerabilities; justification for the deployment of security controls
- ▣ "Risk assessments provide a basis for establishing appropriate policies and selection of cost-effective techniques to implement those policies" ("GAO, Information", 1999:5).
basis for establishing appropriate policies; cost-effective techniques to implement those policies
- ▣ According to the National Institute of Standards and Technology Publication, (Stoneburner et al., 2001:E-2), risk assessment is synonymous with risk analysis and a part of risk management and entails identifying risks to system security, ascertaining the probability of occurrence, the resulting impact and the safeguards that would reduce this impact to an acceptable level.
identifying risks to system security; risk assessment is synonymous with risk analysis and a part of risk management; probability of occurrence; resulting impact and the safeguards that would reduce this impact to an acceptable level
- ▣ Information security risk analysis processes "are geared toward imagining and then confirming technical vulnerabilities in information systems so that steps can be taken to mitigate the risks those vulnerabilities create" (Blakley et al., 2002:98).
imagining and then confirming technical vulnerabilities; mitigate risks
- ▣ Risk analysis provides a "proactive methodology to identify vulnerabilities and threats to the corporation's information assets" (Martinez, 2001:268).
proactive methodology

Based on the key terms derived above, a comprehensive blended definition for the terms risk analysis and risk assessment is formulated:

Risk analysis is synonymous with risk assessment and forms the basis of risk management. It is a proactive, ongoing activity encompassing the identification and valuation of assets; the identification of real and perceived vulnerabilities associated with a particular asset and their severity; the identification of threats and the likelihood of their occurrence; the examination of threat and vulnerability relationships which result in the manifestation of risks; the impact of this risk manifestation with a view to institutionalising appropriate policies; defining existing controls and proposing viable corrective action so as to reduce the impact to the level which is acceptable for a particular environment.

Having established that risk analysis and risk assessment are interchangeable concepts, from this point forward these terms are used synonymously.

2.5.2 OBJECTIVE OF RISK ANALYSIS

It is now important to determine the objective of risk analysis having created a fitting definition for this process. Once again, the literature is scrutinised to obtain a multitude of objectives with the sole aim of creating a unified objective.

Various objectives of the risk analysis process include:

- ▣ The main goal in conducting a risk analysis is to determine the potential losses that could occur from intentional or inadvertent events (Caelli, Longley & Shain, 1989:85).

potential losses that could occur from intentional or inadvertent events

- ▣ The goal of risk assessments should be to comprehend the risks of the particular environment under assessment and to propose a strategy to mitigate these risks to an acceptable level (Vennaro, 2005:2).

comprehend the risks of the particular environment; mitigate these risks to an acceptable level

- ▣ Risk assessment broadly applicable to any type of risk and not strictly confined to information security risk, provide decision makers with information required to comprehend factors that can have negative repercussions for operations and outcomes and make knowledgeable judgements regarding the actions necessary to reduce risk ("GAO, Information", 1999:6).

any type of risk and not strictly confined to information security risk; reduce risk

- ▣ The objective of risk analysis should be the preparation of comprehensive information containing motivating factors for defining unacceptable risk and countermeasures to be implemented. This information should be presented to senior management for approval (Badenhorst & Eloff, 1990:342).
preparation of comprehensive information containing motivating factors for defining unacceptable risk and countermeasures to be implemented; to senior management for approval

Based on the above, a comprehensive blended objective of risk analysis is formulated:

The objective of risk analysis is to identify risks from potential or inadvertent events with a view to reducing the level of risk to an acceptable level. A comprehensive report on the justification for the implementation of countermeasures to reduce the risk to an acceptable level is submitted to senior management for approval. The risks identified are not exclusive to information security and can include any type of risk.

Having established that risk analysis is the foundation of risk management, it is imperative to examine the risk management process. This is focal point of the subsequent section.

2.5.3 DEFINITION OF RISK MANAGEMENT

IT risk management is regarded as being "a perennial top 10 business and technology priority for CIOs" (Hunter & Aron, 2005:2). Risk management is, however, often "shunned or given half-hearted support" because it is simply not "well understood" (Ozier, 1995:221). There is therefore a pivotal need to understand the information security risk management process with a view to standardising the definition and objective of this process.

The term risk management is open to a number of definitions listed below.

- ▣ "Risk management is the identification of threats and the implementation of measures aimed at reducing the likelihood of those threats occurring and minimising any damage if they do". "Risk analysis and risk control form the basis of risk management where risk control is the application of suitable controls to gain a balance between security, usability and cost" (Nosworthy, 2000:600).
implementation of measures aimed at reducing the likelihood of those threats occurring and minimising any damage if they do; Risk analysis and risk control

form the basis of risk management where risk control is the application of suitable controls to gain a balance between security, usability and cost

- ▣ According to the National Institute of Standards and Technology Publication (Stoneburner et al., 2001:E-2), risk management is the process of "identifying, controlling and mitigating information system related risks" and encompasses "risk assessment, cost-benefit analysis and the selection, implementation, test and security evaluation of safeguards." This system review must consider "both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations and laws."

controlling and mitigating information system related risks; encompasses risk assessment; cost-benefit analysis; implementation, test and security evaluation of safeguards

- ▣ Risk management entails allocating limited resources to, "mitigate risks, transfer risks or recover from risk events" (Lewis & Davis, 2004:183).

mitigate risks, transfer risks or recover from risk events

- ▣ "Risk management should be an ongoing activity that includes phases for assessing risk, implementing controls promoting awareness and monitoring effectiveness" (Paul, 2000:122).

ongoing activity; assessing risk; implementing controls; promoting awareness; monitoring effectiveness

Based on the above, a blended definition of risk management is formulated:

Risk analysis is the underpinning activity of risk management, where risk management is the ongoing process of planning, implementing, promoting awareness and monitoring of viable security measures to mitigate, transfer, eliminate or control the risk to an acceptable level.

2.5.4 OBJECTIVE OF RISK MANAGEMENT

It is important to determine the objective of risk management having created a fitting definition for this process. Once again, it is necessary to study the literature to obtain a multitude of objectives with the sole aim of creating a unified objective.

Various objectives of the risk management process include:

- ▣ The aim of risk management is "reduce business exposure by balancing countermeasures investment against risk" (Birch & McEvoy, 1992:45).

reduce business exposure by balancing countermeasures investment against risk

- ▣ The purpose of risk management is "to minimise the expected loss" (Suh & Han, 2003:150).

to minimise the expected loss

- ▣ The goal of risk management is "select risk mitigation, risk transfer and risk recovery measures so as to optimise the performance of an organisation" (Jacobson, 2002:1).
select risk mitigation, risk transfer and risk recovery measures so as to optimise the performance of an organisation

Based on the above, the objective of risk management is formulated:

The objective of risk management is the implementation of appropriate risk mitigation, risk transfer and risk recovery measures to reduce business exposure by balancing countermeasure investment against risk.

The aforementioned sections served to create a solitary comprehensive definition of the terms risk analysis and risk management. The objective of these processes was also determined. Armed with this fundamental information, it is possible to commence a WLAN intrusion security risk analysis exercise having established that risk analysis is the underpinning activity of risk management.

2.6 CONDUCTING A WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE

Since it is so easy to implement a wireless network, all too often no proper risk analysis is done rendering these networks susceptible to a great number of risks (Von Solms & Marais, 2004:634). The most obvious security risk of a wireless network is an intruder's ease of accessing the organisation's internal network (Maiwald, 2003:438). It is therefore crucial to examine the importance of conducting a *WLAN intrusion security risk analysis* exercise. This is the focal point of discussion of the ensuing section.

2.6.1 THE IMPORTANCE OF CONDUCTING A WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE

Wireless access significantly increases the risk of a security compromise (Peikari & Fogie, 2003:291), primarily because of the following features of these networks (Yanga^a, Xie &

Sun, 2004:553; "Wireless LANs: Is", 2002-2005:1-2; Sutton, 2002:4; Wells, 2002:71; "Best Practices", 2004:2):

- ▣ WLANs have obliterated the need for physical access to wires, making these networks prone to attacks from passive eavesdropping to active interfering. Installing a wireless network has actually been compared "to putting a network point that accesses a company's network on a public sidewalk" (Von Solms & Marais, 2004:633).
- ▣ It is virtually impossible to control the WLAN range and signal propagation so attacks on a WLAN can occur anywhere, anytime without any sign of the attacker.
- ▣ WLANs are inherently weak with respect to security, which may result in a security breach.

There is therefore a dire need to perform a WLAN intrusion security risk analysis exercise. If properly conducted, risk analysis can offer organisations a number of benefits (Forcht, 1994:421; Broder, 1984:3; "GAO, Information", 1999:16; Broderick, 2001:15; Kittelberger, 1983:9; Pfleeger & Pfleeger, 2003:527; In et al., 2005:505; Shaffer & Simon, 1994:202), listed below.

- ✓ Identification of all assets, vulnerabilities and controls.
- ✓ Assurance that the most crucial risks have been identified and appropriately addressed on an ongoing basis.
- ✓ Coming to a consensus regarding which risks are the greatest and what measures should be taken to reduce these risks to an acceptable level.
- ✓ Justification for the acquisition of and expenditure on deploying security controls.
- ✓ Identification and prescription of remedial action in the event of a successful security breach that overrides the security controls designed to protect the information.
- ✓ Demonstration of the current security position of the organisation.
- ✓ Supporting decision-making for information security policies.
- ✓ Providing a heightened degree of interest in security by analysing the strengths and weaknesses of security to all hierarchical organisational levels, ranging from management to operations.
- ✓ Providing a means of communicating the risk analysis findings to business unit managers and senior management.

Once organisations understand the pressing need for conducting a WLAN intrusion security risk analysis exercise and the benefits they can accrue from conducting this process, the next step is actually conducting this exercise. Fortunately, formal methodologies for general and specific environments such as Belief-Based Risk Analysis (Josang et al., 2004), CRAMM ("CRAMM Expert", 2003), Cobra ("COBRA - Security", n.d.), CORAS ("CORAS:A Platform", n.d.), EBIOS ("Expression des", 2004), FRAAP (Peltier, 2005), ISRAM (Karabacak & Sogukpinar, 2005), MARION (Coopers, Theron & Du Toit, 1988), LAVA (Smith, 1987), MELISA ("The MARION and", 1990), MEHARI ("Méthode HarmonisèΠe", 2004), OCTAVE (Alberts & Dorofee, 2003), RaMex (Kailay & Jarratt, 1995) and The Buddy System (Jenkins, 1998) that encompass the underpinning principles of risk analysis with well-documented processes can be used.

The following section discusses a well-known qualitative information security risk analysis methodology, *Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE^{SM1})*, as this methodology will be used for conducting the WLAN intrusion security risk analysis exercise.

2.6.2 BACKGROUND: A SYNOPSIS OF THE OCTAVE RISK ANALYSIS METHODOLOGY

There are several reasons for selecting the OCTAVE risk analysis methodology:

- ▣ OCTAVE addresses both organisational and technological issues pertaining to information security risks (Alberts & Dorofee, 2003:12). Other approaches tend to exclude the business processes, focusing solely on the technical threats and vulnerabilities (Coles & Moulton, 2003:488). This aspect is important because senior managers are now coming to the realisation that there are grave human and organisational risks linked with the use of IT (McKeen & Smith, 2003:61).
- ▣ OCTAVE involves people from various hierarchical levels of prime business units, as well as the from the information technology department, in the risk analysis exercise. This is important because, in over 75% of businesses, security strategy is incorrectly ascribed to the IT department (May, 2003:13). Furthermore, risk analysis should

¹ Operationally Critical Threat, Asset and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

cater for the participation of both the manager and staff in the process (Karabacak & Sogukpinar, 2005:149).

- ▣ OCTAVE has broad support in U.S. government agencies such as NASA and the DOD and its adoption in the private sector is escalating (Vennaro, 2005:7-8).
- ▣ OCTAVE is free and vendor neutral and has been developed by the Software Engineering Institute (SEI), a prestigious centre of technological expertise (Lanz, 2002:21-22).

There are two OCTAVE methods, one for larger, more experienced organisations and OCTAVE-S for smaller, inexperienced organisations (Alberts, Dorofee, Stevens & Woody, 2003:15). For the purpose of this dissertation, only the OCTAVE methodology as applied to large organisations is addressed, as this methodology will ultimately be used to address the intrusion security risks of an enterprise-wide WLAN operating environment.

The SEI (Alberts & Dorofee, 2003:15) developed OCTAVE. OCTAVE is a self-directed risk analysis methodology, which means that different hierarchical members within the organisation conduct the risk analysis and experts are consulted only for very specific and specialised needs. This ultimately results in profound dedication and interest in the risk analysis process, thereby manifesting in greater commitment to the results.

OCTAVE is a systematically structured risk analysis methodology that provides guidance for conducting an analysis of the threats, vulnerabilities, security requirements and levels of risk associated with an organisation's critical technical and non-technical assets. The result of this analysis is the creation of an organisation-wide protection strategy and a risk mitigation plan to reduce the risks to the assets identified as crucial.

The OCTAVE process comprises three phases (Lanz, 2002:22) emphasising, the organisational, technological and analysis aspects of a security risk analysis. Each phase consists of a predefined number of processes (figure 2-1).

1. Phase 1 (Organisational View): Build asset-based threat profiles.
2. Phase 2 (Technological View): Identify infrastructure vulnerabilities.
3. Phase 3 (Security Strategy and Plan Development): Develop security strategy and plans.

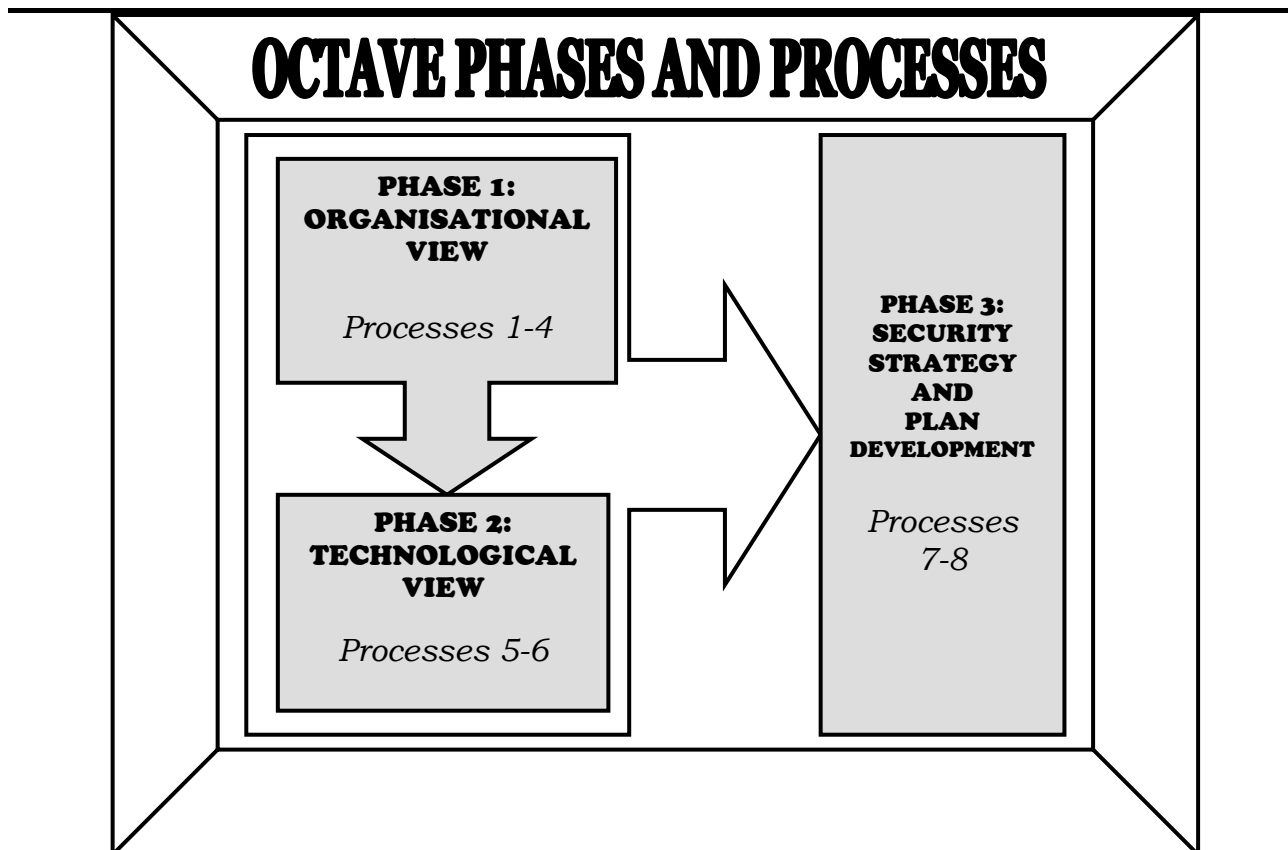


Figure 2-1: OCTAVE phases and processes

2.6.2.1 PHASE 1: ORGANISATIONAL VIEW

In phase 1, the analysis team comprising people who have a great deal of knowledge regarding the organisation as well as its business and technological undertakings hold a series of workshops with senior managers (process 1), operational area managers (process 2) and regular and IT staff (process 3) to extract information regarding (Alberts & Dorofee, 2003:84):

- ▣ The most critical technical and/or non-technical assets and the threats to these assets. The participants brainstorm a list of assets.
- ▣ The identification of scenarios that threaten the most important assets. The participants brainstorm a list of possible threat scenarios.
- ▣ The importance of confidentiality, integrity and availability in protecting these assets.
- ▣ The organisation's current protection strategy if any as well as the weaknesses in the organisation's policies and practices. The OCTAVE catalog of practices may be used for this purpose. The catalog comprise two types of practices (Alberts & Dorofee, 2003:85):

- ▣ Strategic Practices, which are well-documented good management practices that, remain stable over a period of time.
- ▣ Operational Practices which change with advancements in technology.

This phase concludes with process 4 (threat assessment), which is the identification of threats to every critically identified asset, resulting in the creation of a threat profile for that particular asset (Alberts & Dorofee, 2003:112).

2.6.2.2 PHASE 2: TECHNOLOGICAL VIEW

OCTAVE focuses on those portions of the computing infrastructure that are the chief key components of the crucially identified assets (process 5) (Alberts & Dorofee, 2003:137). A vulnerability scan is conducted for the selected components to uncover technological weaknesses (process 6) (Alberts & Dorofee, 2003:158). It may be necessary to outsource this activity to technical experts. The analysis team should, however, evaluate the results to ensure the same high degree of interest and commitment to the risk analysis process.

2.6.2.3 PHASE 3: SECURITY STRATEGY AND PLAN DEVELOPMENT

In the risk analysis process (process 7), the impact of threats on each asset is identified to reflect the subjective high/medium/low impact on each threat resulting in a risk profile for each critically identified asset (Alberts & Dorofee, 2003:171). This is a qualitative determination and deals with the organisation's risk tolerance level. The organisational protection strategy and the risk mitigation plan for the critical assets are drafted (process 8A) (Alberts & Dorofee, 2003:193). The catalog of practices is updated to reflect the new strategic and operational plans for the organisation.

Phase 3 consolidates the information from phases 1 and 2 and creates a vision for long-term organisational protection and a mitigation plan for mid-term vulnerabilities associated with the critical assets. Results are sent to senior management for approval (process 8B) (Alberts & Dorofee, 2003:229).

The following diagram (figure 2-2) depicts the OCTAVE risk analysis activities.

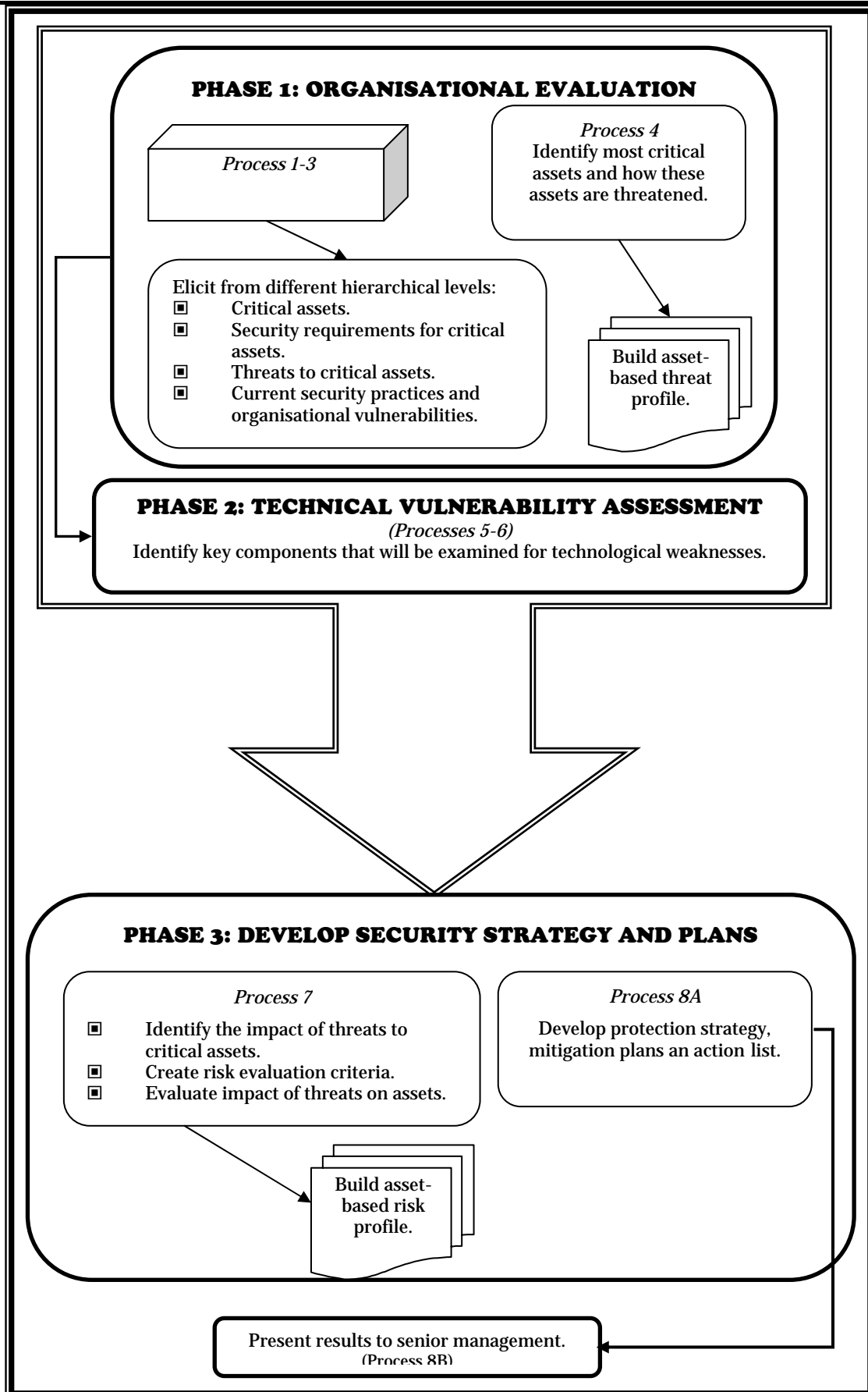


Figure 2-2: OCTAVE risk analysis activities

Since the OCTAVE risk analysis methodology will be used for conducting the WLAN intrusion security risk analysis exercise, it is vitally important to uncover any major flaws that this methodology may have on a general level. The following section assesses the overall strength of the OCTAVE risk analysis methodology.

2.6.2.4 ASSESSING THE STRENGTH OF THE OCTAVE RISK ANALYSIS METHODOLOGY

The General Accounting Office ("GAO, Information", 1999:11-15) framework which outlines the features a concrete risk analysis methodology should possess is used to assess the strength of the OCTAVE risk analysis methodology.

- ▣ The GAO guide was created for the sole purpose of providing federal managers with guidelines on how to perform an ongoing information security risk assessment by providing examples of four organisations that have institutionalised good risk assessment approaches. The guide discusses the factors that these organisations identified as being critical to the success of their risk assessment exercises. These organisations were selected upon recommendations from government and private sector sources including the National Institute of Standards and Technology (NIST), Office of Management and Budget, private consulting firms, professional associations, a risk assessment software developer and GAO auditors ("GAO, Information", 1999:48).

The OCTAVE risk analysis methodology strength test is in appendix A. This strength test illustrates that OCTAVE is a sound risk analysis methodology and can thus be used for conducting the WLAN intrusion security risk analysis. There is however per se no perfect risk analysis methodology that suits all organisations as every organisation is indeed unique in its characteristics (Lichtenstein, 1996:21). This is particularly true of a WLAN operating environment as WLANs have certain unique characteristics as outlined in section 2.6.1.

The following section outlines the general weaknesses of the OCTAVE risk analysis methodology, which may impinge on a WLAN intrusion security risk analysis exercise.

2.6.2.5 LIMITATIONS OF THE OCTAVE RISK ANALYSIS METHODOLOGY

The drawbacks of the OCTAVE risk analysis methodology include (Lanz, 2002:23; Passori, 2004:2; Vennaro, 2005:8; Broodryk, 2005:1; Timothy, 2005):

- ☒ Formal training is required in the use of the methodology.
- ☒ The collaborate approach which requires people from different hierarchical levels to work together may not be possible because people may not work harmoniously with one another.
- ☒ This methodology enlists a great investment in human resources and time for implementing the process and managing the documentation. Working in a wireless networking environment means subjection to an array of threats on a continuous basis. Network security is a "dynamic and fluid process" with security risks changing as social conditions change ("Network Security", 2005:1). Any organisation operating a WLAN needs to be extremely agile in preventing intrusion attacks as an attack can cause irrevocable damage. The non-static nature of this environment means that there is a requirement for a risk analysis methodology that is rapid to execute.
- ☒ An enormous amount of paperwork is involved. Although an automated tool is available (figure 9-1), this tool is expensive and rigid.
- ☒ This methodology largely relies on the identification of assets and threat scenarios by means of a brainstorming process, something that may be difficult for someone who is not conversant with information security issues.
- ☒ The eight OCTAVE processes themselves encompass a number of activities. For example, process 7 consists of four activities, including the creation of a narrative impact description, creating the risk evaluation criteria, evaluating the impact of threats on critical assets, and creating a risk profile. All these phases, processes and activities may overwhelm an organisation and give the illusion that conducting a WLAN intrusion security risk analysis process using the OCTAVE risk analysis methodology is a complex and daunting challenge.

Having established that risk analysis is the foundation of risk management, the next step is to determine how a WLAN intrusion security risk management process is conducted. This is the focal point of the next section.

2.7 CONDUCTING A WLAN INTRUSION SECURITY RISK MANAGEMENT EXERCISE

Like risk analysis, risk management also has a number of formal methodologies. OCTAVE has a number of post-OCTAVE activities. These are typical risk management activities (Alberts & Dorofee, 2003:10) including:

-
- ▣ Planning how to implement the protection strategy and risk mitigation plans.
 - ▣ Implementing the plans.
 - ▣ Monitoring the plans for effectiveness and progress.
 - ▣ Controlling by taking appropriate corrective action for any variations in the execution of the plan.

To ensure that post OCTAVE covers all the risk management activities, the activities of a generic risk management methodology, the Australian/New Zealand standard on risk management ("Standards Australia", 2004) is examined to identify any gaps within the post-OCTAVE activities. The AS/NZS 4360:2004 is "one of the most popular standards in publication" ("Tutorial Notes:", 2004:1) and the only internationally accepted risk management standard ("Standards, methodologies,", 1998-2006).

2.7.1 AUSTRALIAN/NEW ZEALAND STANDARD FOR RISK MANAGEMENT

The Australian/New Zealand Standard for risk management provides the following generic framework for managing risk:

- ▣ Establish the context.
- ▣ Risk identification.
- ▣ Risk analysis.
- ▣ Risk evaluation.
- ▣ Risk treatment.
- ▣ Monitoring and review.
- ▣ Communication and consultation.

Precluding the risk analysis activities reveals the following risk management activities:

- ▣ Monitoring and review.
- ▣ Communication and consultation which is promoting awareness of the plans.

From the above, it can be inferred that post-OCTAVE lacks the following activity:

- ▣ Promoting awareness of the plans.

Therefore, a comprehensive risk management methodology using post-OCTAVE activities comprises the following activities:

- ▣ Planning how to implement the protection strategy and risk mitigation plans.

- ▣ Implementing the plans.
- ▣ Promoting awareness of the plans.
- ▣ Monitoring the plans for effectiveness and progress.
- ▣ Controlling by taking appropriate corrective action for any variations in the execution of the plan.

The following section critically reviews the OCTAVE risk analysis and risk management methodology.

2.8 CRITICAL EVALUATION OF THE OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY

The following observations from the expository investigation of the OCTAVE risk analysis and risk management methodology were drawn.

- ▣ Despite a few shortcomings that may influence a WLAN intrusion security risk analysis, OCTAVE is an effective risk analysis methodology as indicated by the GAO strength test (appendix A). Therefore, the OCTAVE risk analysis methodology can be used for conducting the WLAN intrusion security risk analysis exercise after ensuring that its shortcomings have been overcome.
- ▣ It is established that there are post-OCTAVE activities that are typical risk management activities. These activities were analysed and expanded. Post-OCTAVE can therefore, successfully be used for conducting the WLAN intrusion security risk management exercise.

2.9 CONCLUSION

Conducting an information security risk analysis and risk management process is a crucial undertaking that needs to be performed by any organisation wishing to protect its most critical assets. This chapter has promoted an understanding and serves to standardise the definition and objective of the information security risk analysis, risk assessment and risk management processes. It is important to understand these basic concepts prior to embarking on a comprehensive WLAN intrusion security risk analysis and risk management exercise.

The OCTAVE risk analysis and risk management methodology has been discussed and critically reviewed, as it will be used for conducting the WLAN intrusion security risk

analysis and risk management exercise. It has been established that despite the fact that OCTAVE is a solid risk analysis methodology, it does have a few general shortcomings that may hamper a successful WLAN intrusion security risk analysis. The OCTAVE risk management methodology can be used for conducting the WLAN intrusion security risk management exercise successfully. The next chapter focuses on improving the OCTAVE risk analysis methodology in preparation for conducting a WLAN intrusion security risk analysis exercise.



CHAPTER

3. THE OODA-OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY FOR MITIGATING WLANs INTRUSION SECURITY RISKS

3.1 INTRODUCTION

Every organisation is subject to a succession of risks that could impede its "business operations, growth or profitability" (Moeller, 2004:72). The only environment that is genuinely devoid of risks is one whose future is not marred by uncertainty ("Microsoft Operations", 2004:5). Regrettably, only a minority of organisations actually consider all of the possible risks to which they are exposed to from an information security viewpoint (Howlett, 2005:9). Risks must be managed, which means that they must be identified and analysed and that corresponding mitigation plans must be developed and implemented (Carr, 1997:24-25). These activities are covered by the risk analysis and risk management processes. Neglecting to perform these processes can culminate in "serious financial impacts, commercial embarrassment and fines or sanctions from regulators" (Shaw & Daniels, 2002:14).

The preceding chapter provided a general understanding of these vital processes, stressing the importance of conducting a WLAN intrusion security risk analysis in particular. The OCTAVE risk analysis methodology was found to be flawed in certain respects. The activities of the OCTAVE risk management methodology were analysed and expanded and can be used for conducting the WLAN intrusion security risk management exercise successfully.

The objective of this chapter is therefore to propose a risk analysis and risk management methodology for mitigating WLANs intrusion security risks by overcoming the weaknesses of the OCTAVE risk analysis methodology.

3.2 STRUCTURE OF THIS CHAPTER

This chapter commences with the historical genesis of the Observation-Orientation-Decision-Action (OODA) decision-making cycle. Justification for the selection of this cycle to overcome the weaknesses of the OCTAVE risk analysis methodology is provided.

A new risk analysis and risk management methodology for mitigating WLANs intrusion security risks, OODA-OCTAVE is synthesised, by coalescing the OODA cycle with the OCTAVE risk analysis and risk management methodology. This methodology combines the psychological and temporal aspects of the OODA cycle with the OCTAVE risk analysis methodology to address all the gaps of the OCTAVE risk analysis methodology while remaining true to the OCTAVE risk analysis and risk management methodology.

3.3 THE OODA DECISION-MAKING CYCLE

The OODA decision-making cycle, selected to overcome the deficiencies of the OCTAVE risk analysis methodology, is discussed in the ensuing section.

3.3.1 BACKGROUND: A SYNOPSIS OF THE OODA CYCLE

The OODA cycle (figure 3-1), is a "simple, powerful and insightful model" (Good, 2005:3), immortalised by the late U.S. Air Force Colonel John R. Boyd (1927-1997). The historical development of this cycle stems from the Korean War. Colonel Boyd noted that the performance of the slow U.S. F-86 Sabre fighter aircrafts totally outshone that of the far superior MiG-15 Korean planes. He was perplexed by this situation and attributed the success of the U.S. fighter pilots to the following two factors (Wilson, 2001:14; Chester, 1996:60; Pech & Durden, 2003:169):

1. A larger canopy that provided a more eminent field of vision.
2. A more maneuverable aircraft with "high powered and highly effective hydraulic controls" (Lind, 1985:5) which facilitated faster movement. This meant that the U.S. fighter aircraft had the power to reposition faster from one manoeuvre to another during aerial dog-fights. This rendered the MiG pilots' reaction to the tactical situation ineffective. Such agility manifested in the U.S. pilots' 10 to 1 (Hammond, 2001:36; Brookhiser, 1986:40) kill ratio against the superior MiG-15 Korean planes.

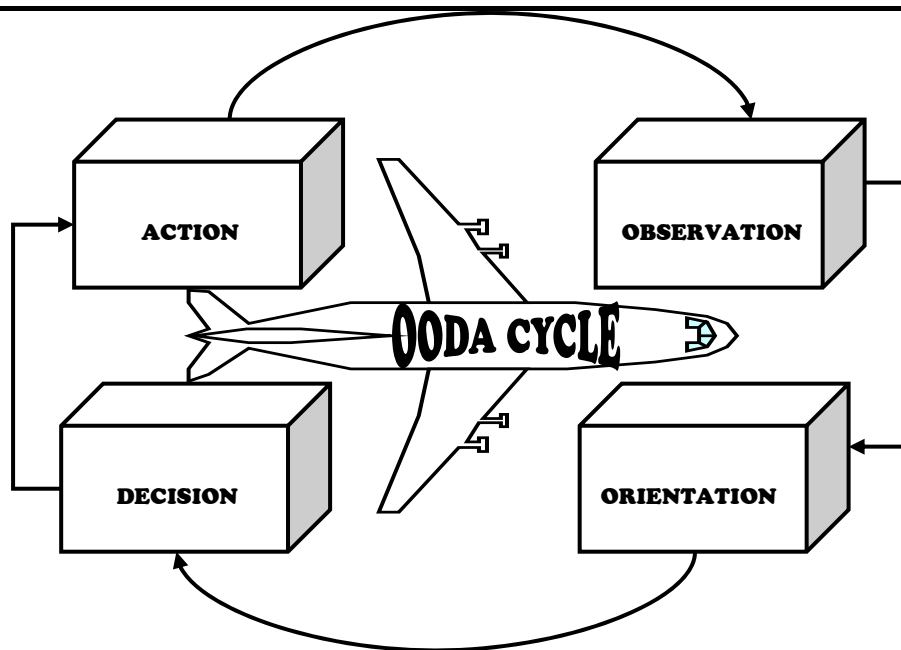


Figure 3-1: The OODA cycle

Based on this observation, he developed the OODA cycle, a theoretical model that can be extrapolated to any direct conflict. The basic tenets of the OODA cycle entail that each party to a conflict (Coram, 2002; Polk, 2000):

- ▣ Observe oneself, the physical surroundings and the enemy, due to having a greater field of visibility.
- ▣ Orient oneself by creating a mental image or snapshot of the situation.
- ▣ Decide what to do by considering all the factors present at the time of orientation.
- ▣ Act, i.e. implement the decision.

Boyd's OODA cycle evolved in the following premises (Fadok, 1995:14; Lind, 1985:5):

- ▣ Psychological: The sole premise of conflict is to destroy the spirit of the enemy by creating difficult operational and strategic situations.
- ▣ Temporal (Speed): The psychological paralysis can be created by moving faster through a number of iterations of the cycle thus inhibiting the adversary's time to decide and act by a greater margin. The idea is to get "inside the mind and decision cycle of the adversary" (Coram, 2002:335).

It is these aspects of psychology and tempo that are lacking in the OCTAVE risk analysis methodology. The next section examines how the OODA cycle addresses some of the gaps of the OCTAVE risk analysis methodology.

3.4 ADDRESSING THE WEAKNESSES OF THE OCTAVE RISK ANALYSIS METHODOLOGY

The OCTAVE risk analysis methodology suffers from several limitations (section 2.6.2.5); including an astonishingly long time to conduct the process and the requirement for the identification of assets and corresponding threat scenarios via a brainstorming process. The OODA cycle address both of these limitations. The predominant theme of the OODA cycle is that in order to annihilate the adversary, it is necessary to ("What is Killing", 2004:3):

- ▣ Disrupt the adversary's OODA cycle, thereby rendering the adversary's actions ineffective. This effectively means understanding the mindset of the WLAN intruder. Understanding how these itinerant intruders mentally compose themselves for a WLAN intrusion attack unravels typical threat scenarios that an intruder can exploit. This is in accord with information security strategy and tactics, which largely resemble those used in warfare (Whitman & Mattord, 2004:287) by drawing on the philosophy of Sun Tzu who states, "If you know your enemy and know yourself, you need not fear the result of a hundred battles..." (Tzu, 1988). The Honeynet Project echoes the same sentiment by stating that one first has to know one's attacker before one can defend oneself (The Honeynet Project, 2002:1). It is precisely this kind of intelligence regarding the enemy and how it attacks, together with its corresponding motives and tactics, that is lacking in network security (The Honeynet Project, 2002). Consequently, it is essential to study the cognitive processes of the enemy in order to develop an intuitive understanding of the most important assets that need the most protection, as well as of scenarios that threaten these assets. It is not possible to do this by a brainstorming process. Therefore, obtaining an understanding of the information flow of its adversary enables an organisation to examine systems proactively, correcting vulnerabilities before they are exploited, by making informed choices regarding protection strategies.
- ▣ Traverse more quickly through one's own loop to disorient the enemy. A fundamental understanding of the WLAN intruder's invasion techniques makes it possible for the organisation to rapidly determine the impact of these attacks. A high risk impact signals the proposition of an enterprise-wide protection strategy and risk mitigation plan to subdue the adversary prior to the manifestation of any attack.

The OODA cycle also ensures that the OCTAVE risk management process is recognised as a vital follow-up activity of the risk analysis process in the following manner:

- ▣ The OODA cycle has a clearly delineated element, *action*, which advocates executing the decision and this element is an integral part of the cycle. This conforms to typical risk management activities.

To overcome the drawbacks of the OCTAVE risk analysis methodology and include the OCTAVE risk management methodology as a vital follow-up activity, the OODA elements are assimilated with the OCTAVE risk analysis and risk management activities, resulting in the synthesis of a new risk analysis and risk management methodology, OODA-OCTAVE.

The intricacies of the OODA cycle with the intertwining of the four phases (figure 3-2) as espoused by Colonel Boyd (Boyd, 1995) manifest in a multitude of loops. Each loop is examined and fused with the phases and processes of the OCTAVE risk analysis and risk management methodology in order to enhance these processes. The next section discusses this newly developed risk analysis and risk management methodology for mitigating WLANs intrusion security risks.

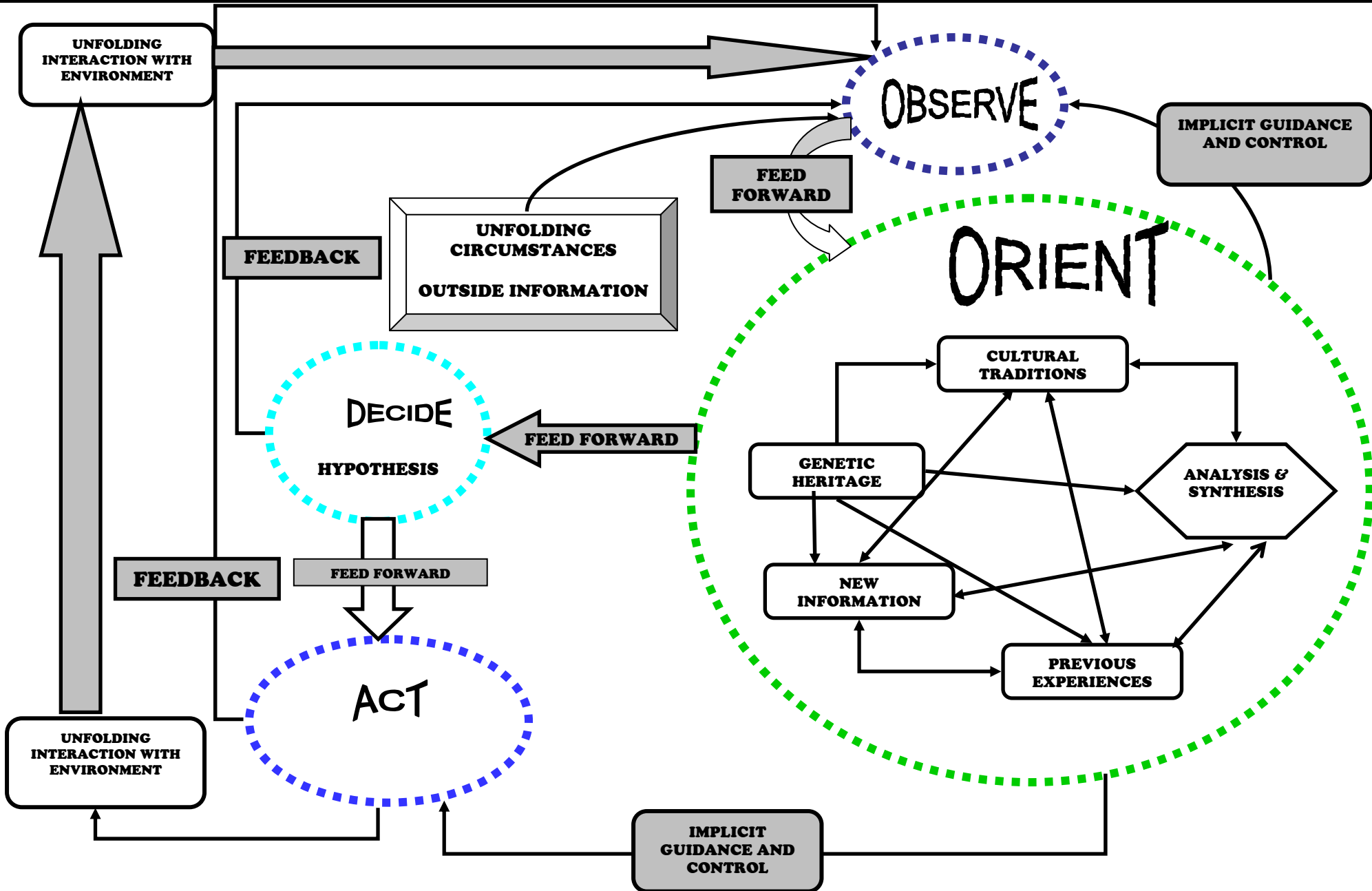


Figure 3-2: Reproduction of Colonel John R. Boyd's sketch of the OODA cycle as espoused in his summation, "A Discourse on Winning and Losing" on 28 June 1995

3.5 THE OODA-OCTAVE RISK ANALYSIS AND RISK MANAGEMENT METHODOLOGY FOR MITIGATING WLANs INTRUSION SECURITY RISKS

A new risk analysis and risk management methodology, OODA-OCTAVE is synthesised (figure 3-3). It combines the temporal and psychological aspects of the OODA cycle with the OCTAVE risk analysis methodology in order to address some of the gaps in the latter.

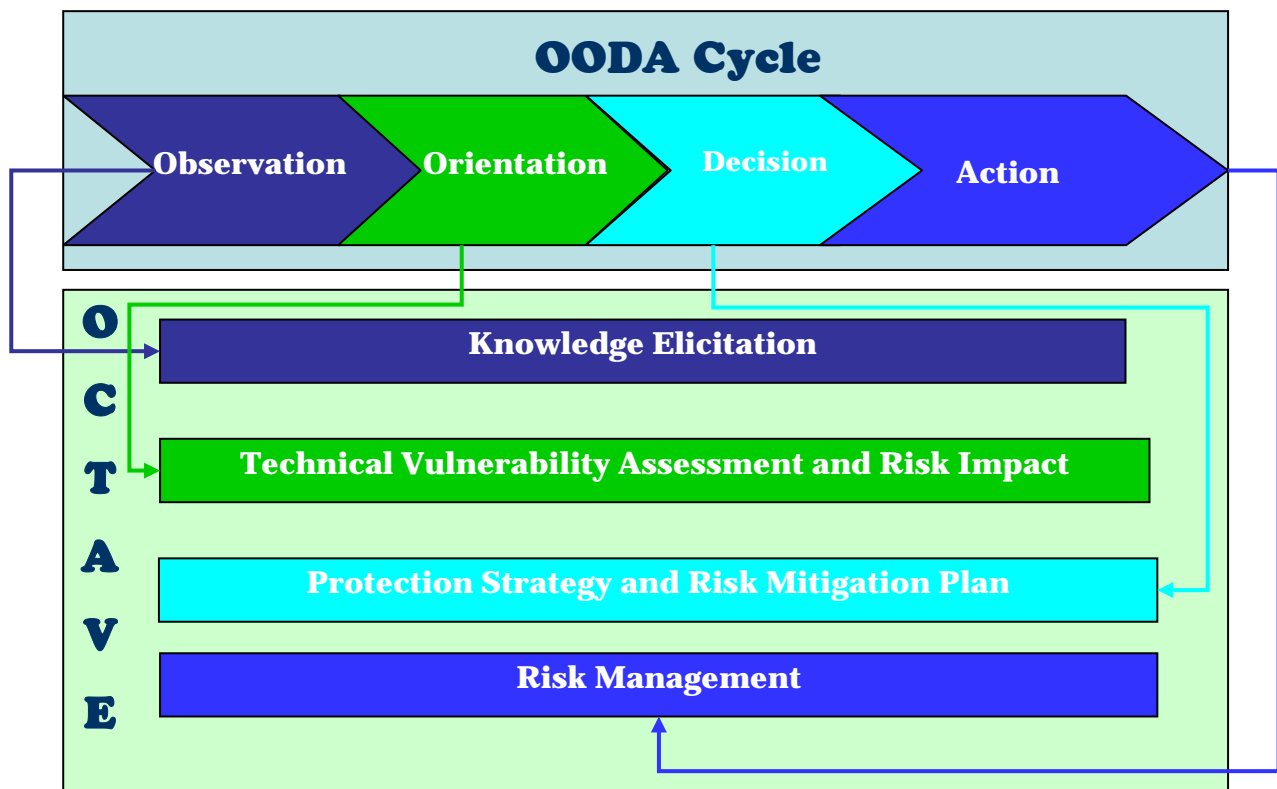


Figure 3-3: High-level diagram depicting the OODA-OCTAVE risk analysis and risk management methodology for mitigating WLANs intrusion security risks

3.5.1 WLAN INTRUSION SECURITY RISK ANALYSIS

The OCTAVE risk analysis activities are combined with the OOD elements as follows.

3.5.1.1 OBSERVATION – KNOWLEDGE ELICITATION

In the observation phase (figure 3-2), the current environment, the subject and the adversary are observed. Information is received from outside the environment as well as in terms of feedback from previous OODA cycles (Owen, Burstein & Mitchell, 2004:19). In this phase, the data of situational analysis is collected (Schechtman, 1996:35). When this information is applied to a WLAN operating environment, the organisation can observe the WLAN operating environment, the WLAN intruder and its own exposure to security

attacks and obtain data regarding the security posture of its WLAN operating environment and its susceptibility to invasion attacks.

From this, it is possible to deduce which assets are important and require the most protection and to uncover the vulnerabilities of these assets. Such information forms the input required for phase 1 (processes 1-3) of the OCTAVE risk analysis process. Information gathered from these activities is required for the knowledge elicitation phase necessary for the organisational evaluation. This input solves two other problems of the OCTAVE risk analysis methodology:

- ✓ The challenges of collaboration among members from different hierarchical levels in the organisation. Phase 1, processes 1-3 normally require a host of workshops and structured interviews with members of different hierarchies in the organisation to elicit their views on what they construe as being the most important assets and the corresponding threats to these assets. The need for time-consuming workshops and structured interviews is eliminated. This shortens the OCTAVE risk analysis process and reduces the paperwork.
- ✓ It also solves the problem of identifying assets and corresponding threat scenarios from participants via a brainstorming process. Important assets can be identified from observing the WLAN operating environment and the threat scenarios can be identified from studying the WLAN intruder's decision-making cycles.

3.5.1.2 ORIENTATION: TECHNICAL VULNERABILITY ASSESSMENT AND RISK IMPACT

Orientation, which is how one analyses/synthesises a situation and creates mental images based subjectively on ones experience, culture, heritage and long-term memories stored in one's subconscious directly guides decision but is in itself also shaped by observation, action and new feedback (Hammonds, 2002:98) (figure 3-2). New information from the observation phase is fused into the "existing mental framework" and the process of destruction and creation begins (Schechtman, 1996:35).

- ▣ Destruction (analysis) entails decomposing a problem into sub-problems that are comprehended easily.
- ▣ Analysing and interpreting information facilitates the creation (synthesis) of new knowledge, expands on existing knowledge and permits knowledge to be reused (Owen et al., 2004:25).

The orient phase terminates at a point where the subject achieves a "coherent state of situational knowledge" (McCauley-Bell & Freeman, 1996:1581). Situation awareness is to "build awareness of complex, evolving situations in a timely and accurate manner" (Bladon, Hall & Andy Wright, 2002:886). More succinctly, orientation centres on organising the information so as to make an initial assessment (Blodgett, Gendreau, Guertin, Potvin & Seguin, 2003:146). This entails grouping all the analysis activities of the OCTAVE risk analysis methodology and equates with phase 1 (process 4) (threat assessment), phase 2 (processes 5 and 6) (technological vulnerability assessment) and phase 3 (process 7) (risk impact assessment). Logically grouping these phases and processes facilitates a better understanding of the OCTAVE risk analysis methodology. These activities encompass analysing and consolidating information and conclude in a state where the organisation has knowledge of its unique WLAN intrusion security risks (situation awareness).

3.5.1.3 DECISION: PROTECTION STRATEGY AND RISK MITIGATION PLAN

In the decision phase (figure 3-2), situational knowledge gleaned from the orientation phase facilitates a hypothesis to be developed, charting a course of action. This means carefully weighing the repercussions of a situation and proposing an action plan proposed (McCauley-Bell & Freeman, 1996:1581). This equates to phase 3 (process 8A) of the OCTAVE risk analysis process, where an organisational protection strategy and risk mitigation plan is proposed. It is possible to re-enter the observation phase from the decision phase prior to embarking on a course of action. This may be a necessary activity to reaffirm previous activities or to consolidate new observations.

3.5.2 WLAN INTRUSION SECURITY RISK MANAGEMENT

The OCTAVE risk management activities are coalesced with the action element of the OODA cycle as follows:

3.5.2.1 ACTION: POST-OCTAVE ACTIVITIES

In the action phase (figure 3-2), the decision is executed by implementing the action. Action should be executed swiftly, unpredictably and disproportionately in order to confuse the intruder (Spitaletta, 2003:41). This correlates to the post-OCTAVE activities where the actual implementation of the organisation-wide protection strategy and proposed countermeasure is done. A *countermeasure* is "a technical or non-technical

security method used to counteract a threat to a system" (Kailay & Jarratt, 1995:450). At the same time, any new interaction with the environment is fed into the observation phase to commence the cycle anew. The loop from action back into observation equates to the continuous monitoring aspect of risk management.

The implicit guidance and control from orientation to both observation and action illustrate that once a situation has been correctly analysed, it is possible to go directly from observing the situation to taking action without having to go through the intermediate orientation and decision phases. This means that if the same observations are made, it is possible to go directly from the knowledge elicitation phase directly to the risk management phase, circumventing the orient phase. This means the same protection strategy and risk mitigation plan can be enforced.

- ✓ This facilitates shortening of the OCTAVE risk analysis and risk management process.

The limiting factors of the OCTAVE risk analysis methodology include amongst others a great deal of investment in human time, resources and formal training. To overcome this problem the researcher has developed a database for storing all of the WLAN intrusion security risk analysis and risk management information (figures 3-4 to 3-5). Appendix E contains details regarding the logical design of the database.

The database serves to encapsulate both the OCTAVE risk analysis and risk management processes consolidated with the OODA cycle by permitting the organisation to cycle faster through the risk analysis process and include the OCTAVE risk management process as a vital component follow-up activity to the risk analysis process.

- ✓ This database precludes the need to invest in human resources, paper resources and formal training, thus shortening the cycle.
- ✓ The OCTAVE phases, processes and activities are succinctly laid out. There is no explicit mention of any phase number or process number such as phase 1, process 3, thereby providing an uncomplicated view of the OCTAVE risk analysis process.

The OODA-OCTAVE Risk Analysis and Risk Management Methodology for Mitigating WLANs Intrusion Security Risks

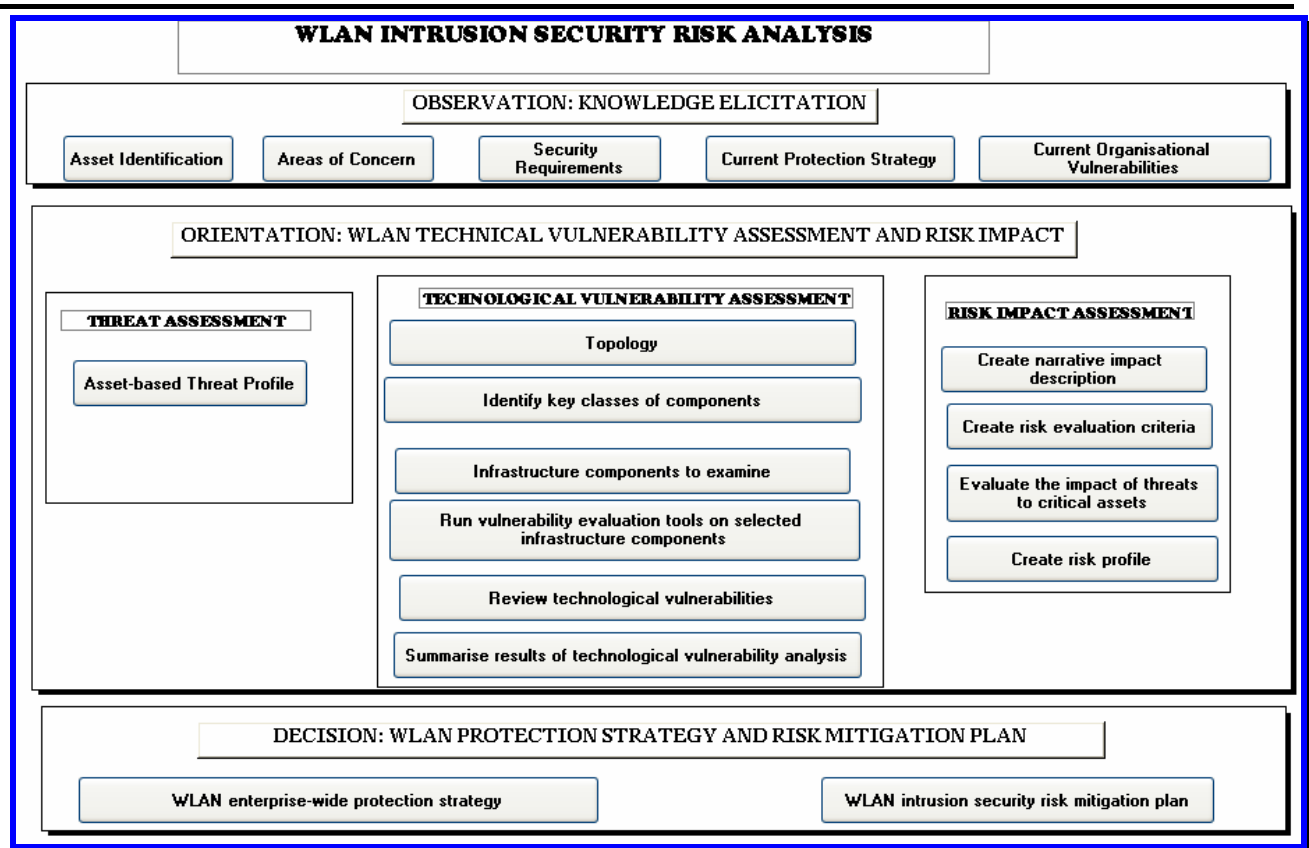


Figure 3-4: Database for storing WLAN intrusion security risk analysis information

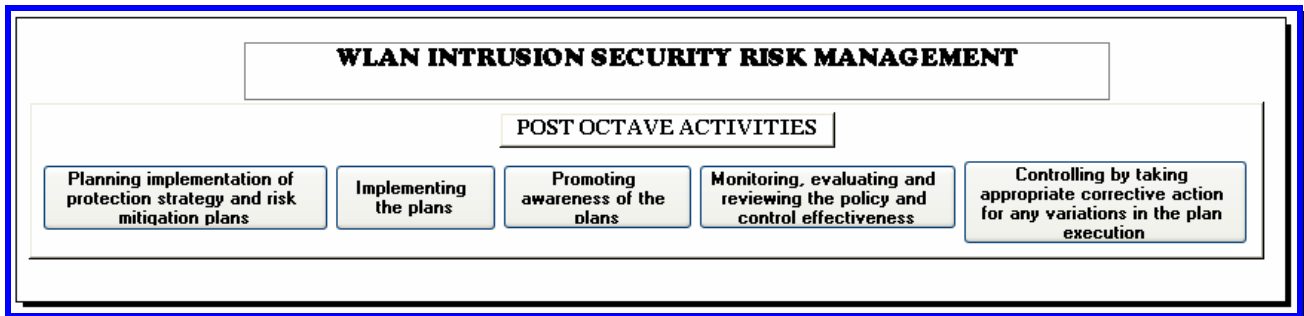


Figure 3-5: Database for storing WLAN intrusion security risk management information

Figure 3-6 is a detailed diagram depicting the OODA-OCTAVE risk analysis and risk management methodology for mitigating WLANs intrusion security risks.

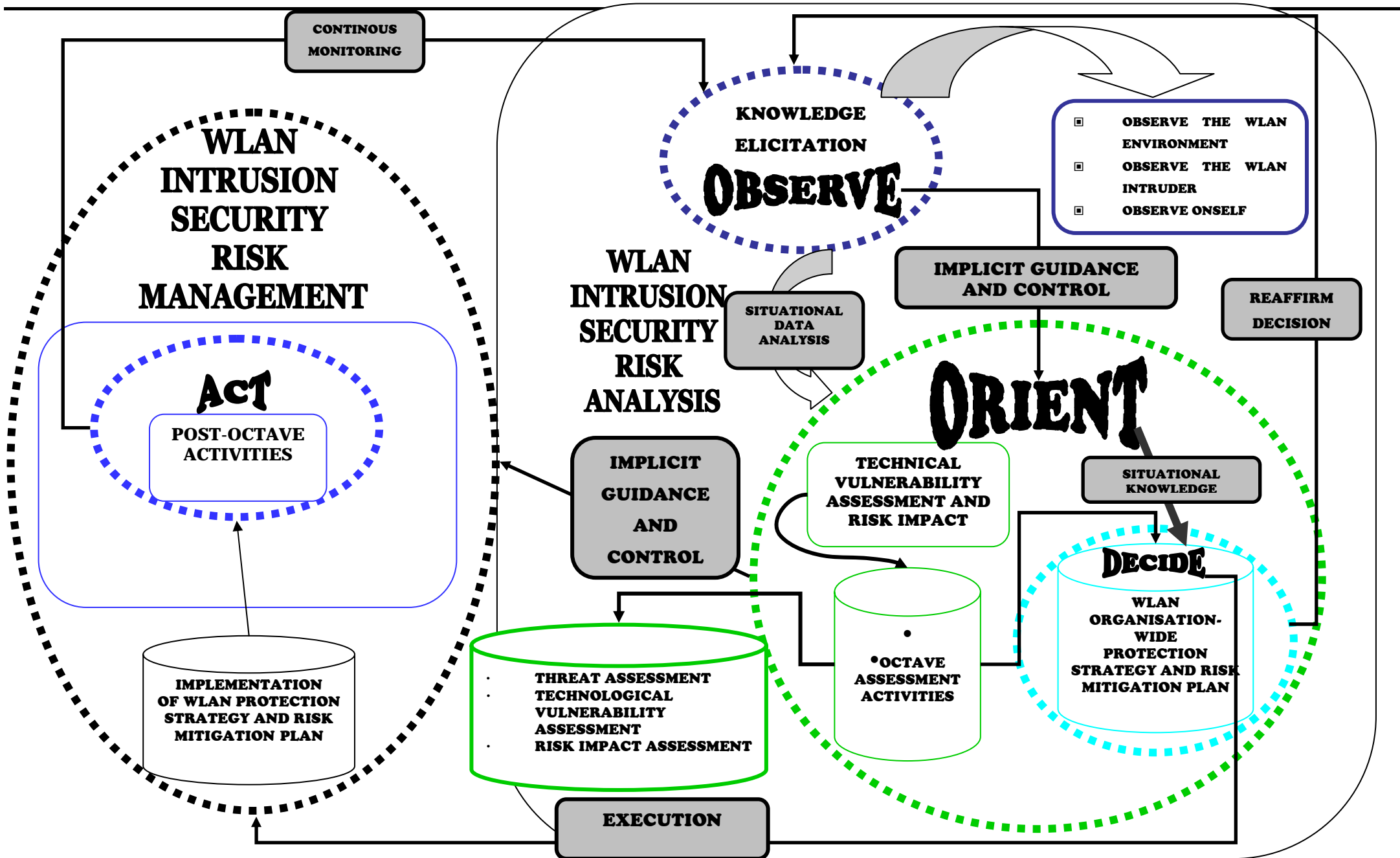


Figure 3-6: The OODA-OCTAVE risk analysis and risk management methodology for mitigating WLANs intrusion security risks

3.6 CONCLUSION

This chapter centred on the proposition of the OODA-OCTAVE risk analysis and risk management methodology for mitigating WLANs intrusion security risks. This methodology serves to solve the problems regarding the OCTAVE risk analysis methodology and ensure that risk management is included as a vital follow-up component to risk analysis. The next chapter commences the WLAN intrusion security risk analysis exercise with the first phase, observation: knowledge elicitation.

PART



WLAN INTRUSION SECURITY RISK ANALYSIS

CHAPTER FOUR

OBSERVATION: KNOWLEDGE ELICITATION

Wireless LANs are a breeding ground for new attacks because the technology is young and organic growth creates the potential for a huge payoff for hackers.

- Pete Lindstrom, Hurwitz Group

September 2002

CHAPTER FIVE

ORIENTATION: TECHNICAL VULNERABILITY ASSESSMENT AND RISK IMPACT

It will not do for the army to act without knowing the opponent's condition, and to know the opponent's condition is impossible without espionage

-Du Mu

CHAPTER SIX

DECISION: PROTECTION STRATEGY AND RISK MITIGATION PLAN

Wireless IDS is needed not only for people that have deployed WLANs, but also for enterprises that have not deployed one. And the reason why is that attacks from a WLAN into a wired network are a very real threat

- Brian Mansfield



CHAPTER

4. OBSERVATION: KNOWLEDGE ELICITATION

4.1 INTRODUCTION

WLANs can be used primarily as an extension to supplement fixed-wired networks (Panko, 2005:218; Fung, 2005:184) or may function as independent networks ("Federal Agencies", 2005:6). This underlines the importance of having a basic understanding of these networks, particularly the security issues as security is "perhaps the biggest shortcoming of the 802.11 standard" (Khan & Khwaja, 2003:69).

The mobile environment has generated novel vulnerabilities that do not exist in fixed-wired networks (Zhang, Lee & Huang, 2003:545), vulnerabilities, which if exploited by malicious intruders could manifest in risks. It is therefore crucial to understand and mitigate these risks before they have dire consequences. A security assessment can aid in managing the security risks within an organisation (Baccam, 2004:2). This chapter commences with the conduction of a WLAN intrusion security risk assessment.

The objective of this chapter is to uncover all the operational issues prevalent in a WLAN operating environment that may lead to an invasion attack.

4.2 STRUCTURE OF THIS CHAPTER

This chapter commences with the conduction of the WLAN intrusion security risk analysis process. The preparatory activities as well as the activities required for the knowledge elicitation phase required for the organisational evaluation are covered.

The observation phase of the OODA cycle encompasses three aspects as outlined in the previous chapter. These three aspects include observing the environment, observing the enemy and observing oneself. This chapter, is therefore, structured according to these three aspects.

The first aspect, observing the environment entails studying the WLAN operating environment. This chapter commences with a synopsis of WLANs, elaborating on aspects such as the benefits and drawbacks of deploying this technology in contrast to fixed-wired networks, the components and architecture of WLANs as well as the most common standards in WLAN technology. The next phase, observing the enemy consists of an in-depth study of the OODA cycle of WLAN intruders to obtain an understanding of their information flow. The final aspect is observing oneself, which is an expository overview from the organisation's side to determine how secure its WLAN operating environment really is.

The following diagram (figure 4-1) depicts the role of this chapter within the overall context of the dissertation.

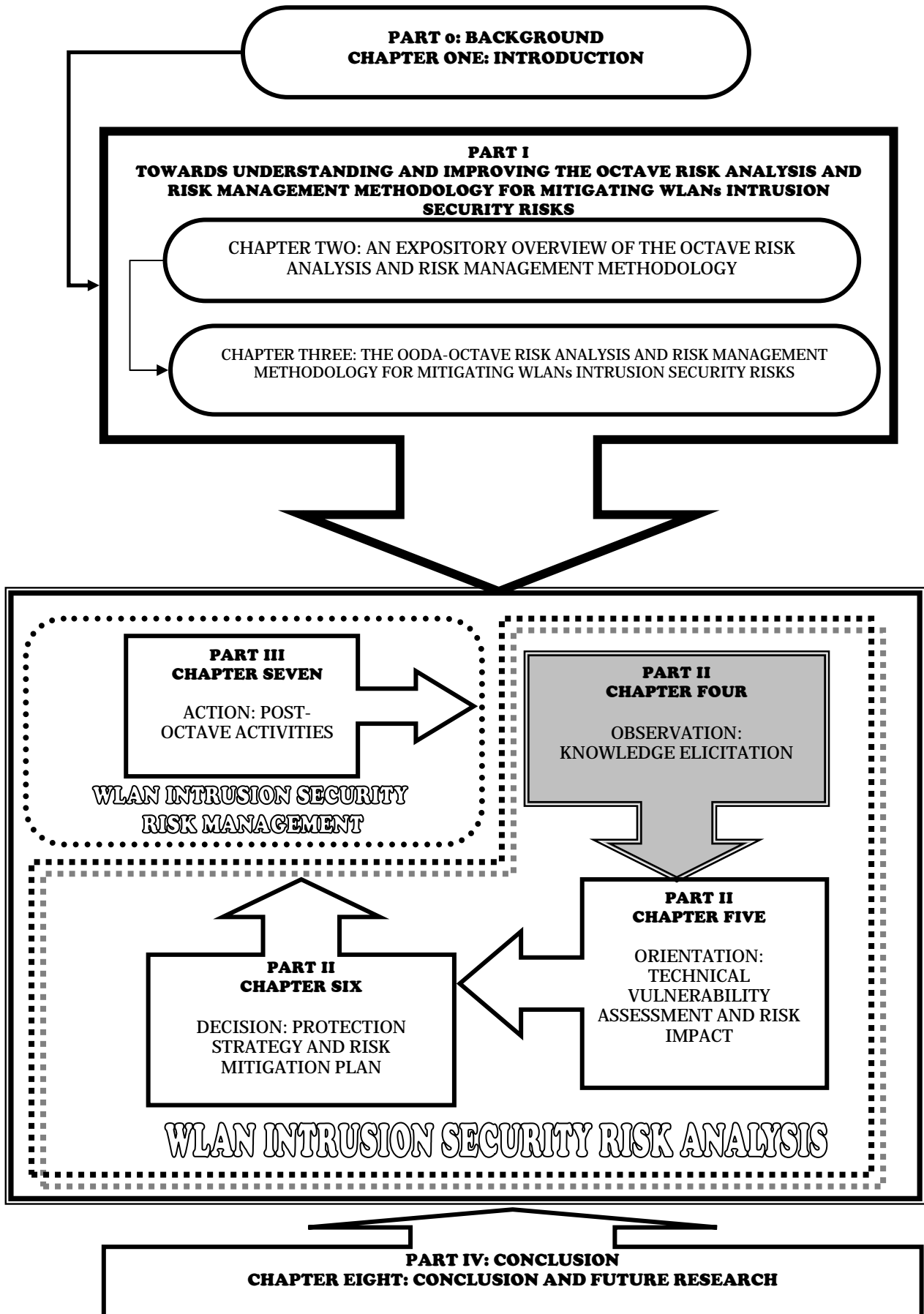


Figure 4-1: The role of chapter four within the overall context of the dissertation

4.3 TERMINOLOGY USED IN THIS CHAPTER

For the purpose of this chapter, the following definitions apply.

BANDWIDTH

Bandwidth is the amount of data that can typically be transferred over a communications medium and is measured in bits per second (bps), where kilobits per second (kbps) is 1 000 bps, megabits per second (Mbps) is a million bps and gigabits per second (Gbps) is 1 billion bps (Gallo & Hancock, 2002:55).

HERTZ (HZ)

Hertz is the chief unit of measurement for radio frequencies (Palmer, 2004:360) and is "the number of cycles being carried per second" (Hallberg, 2003:14). *Megahertz (MHz)* is "the measurement of cycles in millions of cycles per second" and *gigahertz (GHz)*, "billions of cycles per second" (Stair & Reynolds, 2006:94).

IP ADDRESS

An *IP address* is a 32-bit dotted decimal address, where each byte can be represented in dotted decimal notation as four numbers ranging from 0 to 255 separated by periods (Ciampa, 2006:179; McCullough, 2004:35).

OSI MODEL

The *OSI model* is a theoretical model used to standardise communications across networks and outline the interoperability between their components (White, 2004:16).

Commencing the WLAN intrusion security risk analysis process entails executing the following preparatory activities.

4.4 PREPARATION FOR THE WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE

A designated leader is ascribed the task of conducting the risk analysis process. The researcher assumes this role. Scribes are responsible for documenting the risk analysis information. The database is used to record the WLAN intrusion security risk analysis information.

The researcher investigated a typical WLAN operating environment at the University of South Africa (UNISA). The preparatory activities for the WLAN intrusion security risk

exercise include obtaining senior management sponsorship and delineating the scope of the evaluation. The researcher obtained the necessary permission from the network administrator at UNISA and limited the scope of the evaluation to analyse the infrastructure-based WLAN. This information is stored in the database (figure 4-2). It is also necessary to assemble an analysis team. A small analysis team comprising the IT manager and two WLAN users was assembled. The analysis team was informed of the true meaning and objective of risk analysis and risk management (sections 2.5.1 to 2.5.4) and introduced to the OCTAVE risk analysis and risk management methodology using the database and figure 2.2.

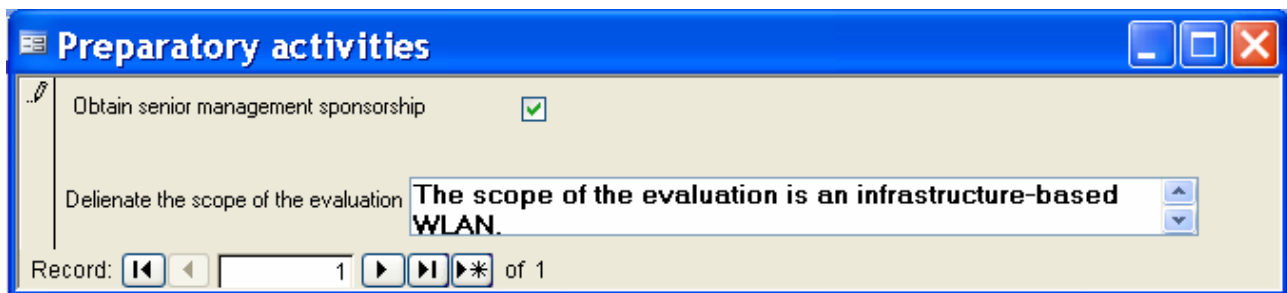


Figure 4-2: WLAN intrusion security risk analysis preparatory activities

The next section covers the activities of the knowledge elicitation phase.

4.5 OBSERVING THE ENVIRONMENT - BACKGROUND: A SYNOPSIS OF WLANS

An IEEE 802.11 WLAN is a group of wireless clients located in a limited geographical area that use radio frequency (RF) technology to receive and transmit at rates of up to 2 Mbps in the air (Housley & Arbaugh, 2003:32; Dean, 2003:437; White, 2004:99). *Radio frequencies* are "high frequency alternating current (AC) signals passed along copper wire or conductor until an antenna radiates them into the air" (Lewis & Davis, 2004:53).

WLANs provide a number of advantages and disadvantages over traditional fixed-wired networks. The following section briefly surveys the benefits and drawbacks of deploying WLANs in relation to their wired counterparts.

4.5.1 BENEFITS OF DEPLOYING WLANs

Some of the most compelling benefits of deploying WLANs include (Park & Dicoi, 2003:60; Karygiannis & Owens, 2002:12; Park, Ganz & Ganz, 1998:237; Carter, 2005: 27):

- ▣ Flexibility: It is possible to install WLANs more easily, cost-effectively and much more rapidly than traditional fixed-wired networks.
- ▣ Mobility: WLAN users can access network files and the Internet any time without been confined to a wiring infrastructure.
- ▣ Easy expansion: It is easy to add wireless clients to a WLAN by equipping them with a wireless network adapter card. Adding computers to fixed networks entails drilling holes and running cables.

4.5.2 DRAWBACKS OF DEPLOYING WLANs

The drawbacks of deploying WLANs include (Dean, 2006:311; McCullough, 2004:8; Palmer, 2004:363):

- ▣ Wired networks transmit much more data per second than wireless networks. The reason for this is that 802.11 uses the CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) to access the shared medium. This means that a wireless client after sensing that the medium is idle, sends a small frame called a request to send (RTS) stipulating the time it requires the medium. A *frame* is a unit of data sent over a network carried at the Data Link layer (layer 2) of the OSI model (Palmer & Sinclair, 2003:7). The receiving wireless client acknowledges the request by sending a small packet called clear to send (CTS). A *packet* is a unit of data sent over a network carried at the Network layer (layer 3) of the OSI model (Palmer & Sinclair, 2003:7). The sending wireless client sends the data frames for which the receiving wireless client issues an acknowledgement packet (ACK) to the transmitting wireless client to indicate that it has successfully received the packet. This use of ACK packets creates additional overhead, which culminates in wireless networks achieving between one-third and one-half of their theoretical maximum throughput. Throughput is the "actual amount of data that can be transferred" (Tomsho, Tittel & Johnson, 2004:412).
- ▣ Wired networks are prone to interference but to a lesser degree than wireless networks. Wired networks are not impeded by obstacles and interference such as hills and stormy weather (Palmer, 2004:363), as are wireless networks. Furthermore, the performance degradation of wired networks over the same distance is less than that of wireless networks.

WLANs operate in the 2.4 GHz, Industrial, Scientific and Medical (ISM) frequency spectrum using either frequency-hopping spread spectrum (FHSS) or direct-sequence spread spectrum (DSSS) (Khan & Khwaja, 2003:59) where the local RF regulatory body does not require the end-user to purchase a license to use the airwaves.

Spread spectrum entails using a greater bandwidth than that which is actually required in order to support a given data rate (Stallings, 2004:33). In *FHSS*, the signal jumps from one frequency to another within a band in a synchronisation pattern known to the channel's receiver and transmitter (Maxim & Pollino, 2002:172; Dean, 2003:420; Stallings, 2001:21). In *DSSS*, a signal's bits are spread into a sequence of multiple bits and allotted over different frequencies at once. Each bit is coded in such a way that the receiver upon receiving the bits can reassemble the original signal (Dean, 2003:420).

Over the years, the IEEE has developed a host of standards for the computer and electronics industry (Miller, 2003:9). 802.11, the first standard for WLANs was published on 26th June 1997 (Barnes et al., 2002:133).

Over the years, the IEEE has expanded the 802.11 standards to include the following variants:

4.5.3 IEEE STANDARDS

The most popular 802.11 extensions regarded as "de facto standards" ("Wireless LAN", 2005:2) include 802.11b, 802.11a and 802.11g (Khan & Khwaja, 2003:58; Dean, 2003:440). These three standards are discussed below.

4.5.3.1 802.11b

The most widely deployed standard, 802.11b, approved in September 1999 (Maxim & Pollino, 2002:175), also known as wireless fidelity or WiFi, specifies a data rate of up to 11 Mbps using DSSS in the 2.4 GHz ISM frequency band. For 802.11b, a total of 14 channels are defined by the IEEE standard in the ISM band with each channel occupying 22 MHz. (Dean, 2003:440; Park & Dicoi, 2003:61; Flickenger, 2003:4).

4.5.3.2 802.11a

802.11a, presented in 2002 (White, 2004:222) establishes a new unlicensed frequency band for wireless networking and increases throughput for networks to 54 Mbps (Kapp, 2002:84) using frequencies in the 5 GHz (Stallings, 2004:34) Unlicensed National Information Infrastructure (UNII) band (Park & Dicoi, 2003:61). The UNII is reserved for devices that provide a short range as well as high-speed wireless digital communication (Ciampa, 2006:52). 802.11a uses orthogonal frequency division multiplexing (OFDM), in which 52 carriers are used in transmitting data from a single source to obtain a 54 Mbps channel bit rate (Varshney, 2003:102).

4.5.3.3 802.11g

The 802.11g specification, approved by the IEEE in May 2003 (Tanzella, 2003:3) has a data transmission rate of up to 54 Mbps in the 2.4 GHz band and is backward compatible with 802.11b (Carter, 2005:37).

When the 802.11b standard was established in 1999 (Dean, 2006:314), the IEEE added new Physical and Data Link layers to the OSI model (figure 4-3) without any variation to the other layers of the OSI model.

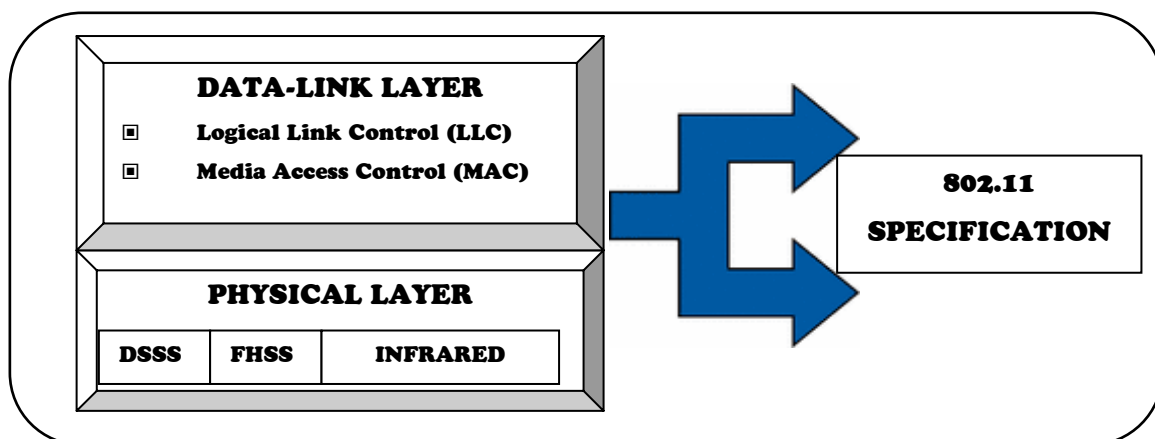


Figure 4-3: Addition of Physical and Data Link layers to the OSI model

The Physical layer dictates the transmission mode of data. The Physical medium has three layer specifications (Tanzella, 2003:2, Stallings, 2001:21):

- ▣ Direct-sequence spread spectrum (DSSS) operating in the 2.4 GHz ISM band.
- ▣ Frequency hopping spread spectrum (FHSS) operating in the 2.4 GHz ISM band.
- ▣ Infrared, a relatively unused technique in networking (Kapp, 2002:82).

The Data Link layer comprises the Media Access Control (MAC) layer and the Logical Link Control (LLC) layer (Tanzella, 2003:2):

- ▣ The MAC layer describes how computers receive and transmit data and maintain communication with other wireless clients after being authenticated successfully (McCullough, 2004:31).
- ▣ The 802.11 standard does not specify any changes to the LLC layer. This layer provides error and flow control as well as an interface to higher layers in the OSI model (Stallings, 2004:32). All modifications are confined solely to the MAC sublayer of the Data Link layer (Ciampa, 2001:92).

The MAC protocol permits only one client to transmit at a given point in time and that data transmitted is in blocks or MAC frames (figure 4-4).

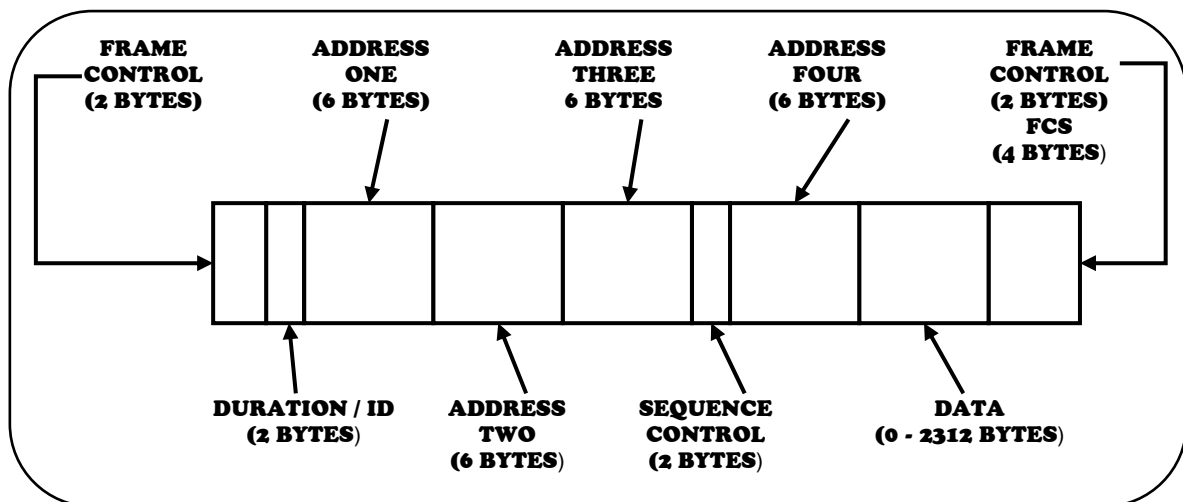


Figure 4-4: Format of an IEEE 802.11 frame

It is important to understand 802.11 frames as they contain useful information that permits monitoring (Yang^c, Xie & Sun, 2004:1951). This information can provide insight to determine whether an intrusion attack has taken place. Frames are divided into three groups (Dean, 2006:313; Forouzan, 2003:339):

1. Management frames are those involved in communication between wireless clients and access points (APs). Wireless clients and APs are the basic components of WLANs. The following section provides a discussion of these components.
2. Control frames are those related to medium access and data delivery.
3. Data frames are those that carry the data sent between stations.

4.5.4 ARCHITECTURE OF WLANs

The basic components of a WLAN constitute:

- ▣ A wireless client equipped with a wireless network interface card (WNIC). The WNIC functions at the Physical and Data Link layers of the OSI model. Every WNIC has a MAC address, a 48-bit number set (Palmer, 2004:263) that provides identification at layer 2 of the OSI model (Carter & Shumway, 2001:113). The first 24 bits is a 24-bit organisationally unique identifier (OUI) that indicates the manufacturer of the WNIC which if known can reveal the name of the manufacturer from a searchable database ("IEEE OUI and", n.d.) The other 24 bits denote a 24-bit unique card identifier. The WNIC possesses an antenna making it possible to send and receive wireless signals.
- ▣ An access point (AP) that effectively functions as a bridge between the wired and wireless networks. An AP consists of an antenna, a radio transmitter/receiver on one end and MAC bridge to the wired infrastructure at the other end through which it is able to communicate with all devices connected to the wired network such as printers and servers. If the AP is able to connect the WLAN to any other type of network or to the Internet, it must also act as a router (Khan & Khwaja, 2003:48). A *router* allows "multiple users to share a single broadband Internet connection and directs traffic by routing data between clients" (McCullough, 2004:11).

The wireless client and the AP communicate via radio waves. A *radio wave* occurs when an electric current passes through a wire emanating a magnetic field in the space around the wire (Ciampa, 2001:34). Every AP also has a number called a basic station system ID (BSSID) assigned to it. The BSSID is essentially the MAC address of the AP (Howlett, 2005:318).

The AP functions as the base station for the WLAN and "the set of wireless devices with which a single AP communicates defines a basic service set (BSS)" (Shay, 2004:450). Two types of BSS identifiers exist, the infrastructure BSS and the independent BSS (IBSS) (Sharma, 2004:115).

4.5.4.1 INDEPENDENT BSS (IBSS)

An IBSS (figure 4-5) also called an ad hoc network or peer-to-peer network (Flickenger, 2003:18) is a network created spontaneously to cater for some immediate need. There is

no AP present and each wireless client simply communicates with other clients. This opens a completely new avenue of security issues that is beyond the scope of this study.

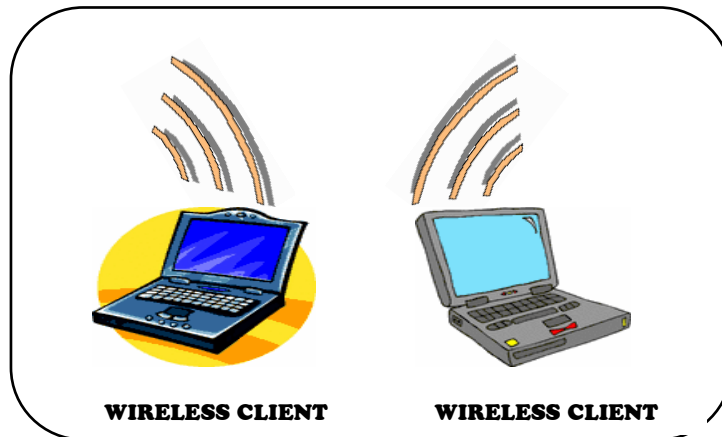


Figure 4-5: Independent BSS

4.5.4.2 INFRASTRUCTURE BSS

An infrastructure BSS comprises at least one AP, which is the central hub for the WLAN (figure 4-6).

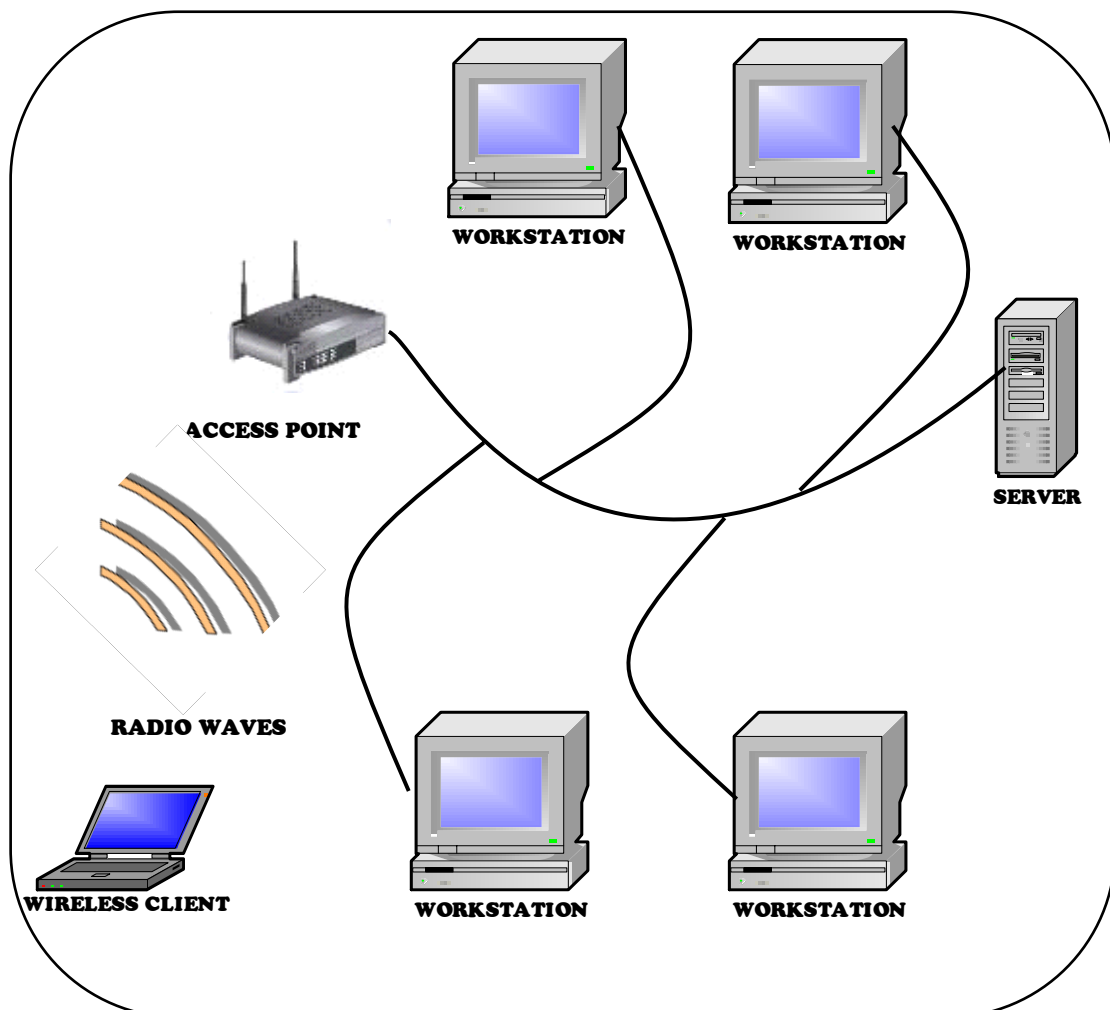


Figure 4-6: Infrastructure BSS

The scope of the WLAN intrusion security risk analysis exercise is an infrastructure BSS at the University of South Africa (UNISA). This WLAN environment is a small environment with one Cisco Aironet Series 1200 AP and 10 wireless clients all equipped with Cisco Aironet 802.11a/b/g WNICs.

The collection of all basic service sets is called an extended service set (ESS), where several APs can serve a large number of WLAN clients over a greater area (figure 4-7), resulting in larger networks. Wireless clients can roam between these APs without losing connectivity to the WLAN. The ESS has an alphanumeric value (ESSID) programmed into the router to denote which subnet it is part of. A distribution service set (DSS) facilitates communication between wireless clients and APs on different BSSs.

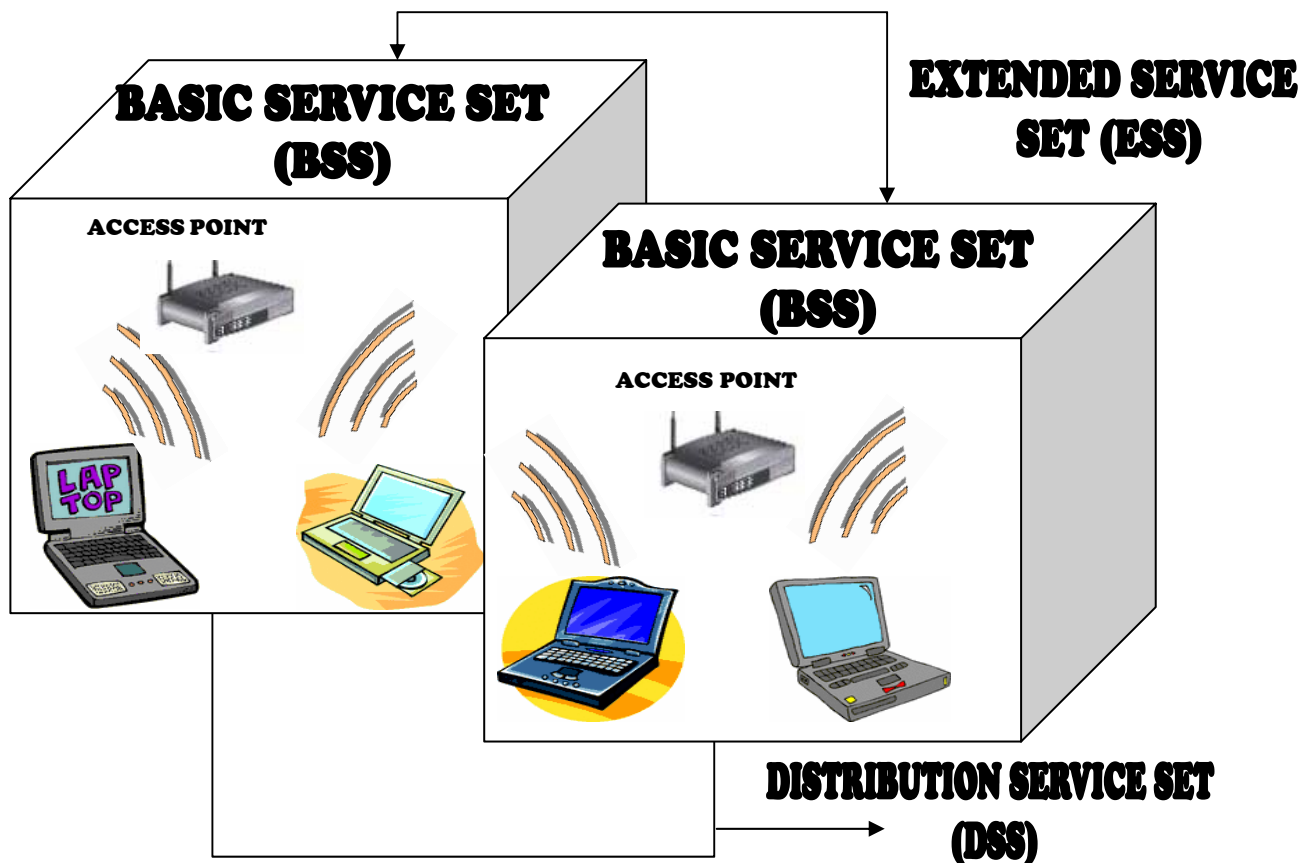


Figure 4-7: An ESS and DSS infrastructure network

In order for wireless clients to communicate with an AP, the wireless client establishes a relationship called association with the AP (Peikari & Fogie, 2003:137). Two types of scanning accomplish the association process (Held, 2003:46). Various types of management frames are exchanged (Edney & Arbaugh, 2004:55):

- APs transmit beacon frames containing a unique identifier called a service set identifier (SSID), a 32 byte or less than 32 bytes network name (Berghel & Uecker, 2004:15) for the BSS which wireless clients use in order to authenticate with the WLAN, a process termed passive scanning (Carter, 2005:312). The wireless client determines which AP has the clearest and strongest signal. The wireless client sends an authenticate message to this AP. The AP responds with an authenticate response. The client then sends an associate request management frame including its capabilities and supported rates to which the AP responds with an associate response management frame containing a 2-byte status code if the association was successful (Yang^c et al., 2004:1951) as well as the station ID number for the particular client (Ciampa, 2001:109). The station can now begin transmitting and receiving information on the WLAN.
- In order for a wireless client to find new APs, the wireless client transmits probe frames to discover APs, a process termed active scanning (Dean, 2006:312) to which APs issue a probe response. Wireless clients can therefore obtain information about APs in the area.

Upon successful association with an AP as illustrated in figure 4.8 of the sample UNISA WLAN operating environment, the AP can then share this information with other APs, facilitating the task of a client re-associating with another AP.

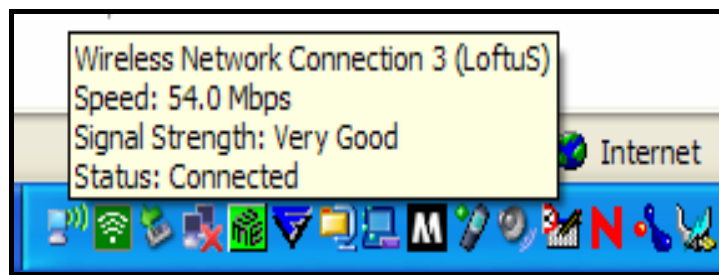


Figure 4-8: Successfully associating with an AP in the sample UNISA WLAN operating environment

Studying the WLAN operating environment aids in identifying critical assets. This is required for the first activity of the knowledge elicitation phase; covered in appendix C Information required for the remaining activities of the knowledge elicitation phase is obtained by studying the OODA cycle of the WLAN intruder. This is covered in the following section.

4.6 OBSERVING THE INTRUDER: OODA CYCLE OF THE WLAN INTRUDER

Metaphorically, "security is like a game of chess" (Wagner & Soto, 2000:255) in the sense that one must foresee all sorts of moves that the WLAN intruder may make and consequently enforce the necessary security measures to avert these attacks. The following section focuses on the OODA cycle of the WLAN intruder. The essence of this is to gain an understanding of how WLAN intruders operate in order to defend a network against intrusion attacks.

4.6.1 OBSERVATION

In order to launch an intrusion attack on WLANs, the WLAN intruder first has to observe the external environment by discovering the presence of APs. This activity, commonly referred to as *war driving*, takes place when an attacker "accesses a company network from outside the physical perimeter of the company facility" (Stewart, 2004:367).

War driving or WLAN discovery, is accomplished by using active and/or passive scanners. Appendix B contains examples of WLAN discovery using active and passive scanners for selected areas in South Africa.

Another mode of discovering APs is by *war chalking*. War chalking entails drawing certain symbols to indicate the presence of APs. These symbols include open node indicating that an AP is broadcasting its SSID, closed node meaning that the SSID is not being broadcast by an AP and WEP node indicating that communications are being encrypted through the use of WEP keys (Quinion, 2002).

Having discovered the presence of WLANs, the next step is to uncover the security holes of these networks in order to launch an invasion attack. This activity is covered in the orientation phase of the OODA cycle of the WLAN intruder.

4.6.2 ORIENTATION

Orientation is the interaction of mental images, views or impressions. It is shaped by "genetic heritage, cultural traditions, views, previous experiences and unfolding circumstances" (Hammond, 2001:164).

Equating this to the OODA cycle of the WLAN intruder, the orientation phase is shaped by the inherent vulnerabilities of WLANs, peoples' experiences using WLANs that have been highlighted in the media, books, Internet, journal articles and by vulnerabilities that are discovered and exploited on a continuous basis. This next section explores the orientation phase of the WLAN intruder.

4.6.2.1 CULTURAL TRADITIONS

Literally, the word *cultural* refers to "a way of life" ("Cambridge Dictionaries", n.d.) and *traditions* to a principle or mode of acting adopted by a group of people ("Cambridge Dictionaries", n.d.). Applying this to WLANs security equates to the customs adopted in achieving security on these networks. Encryption and authentication within the APs and the WLAN cards are the fundamental tenets of security on WLANs ("Wireless LAN Policies", 2003:2; "WIRELESS LANs:Risks", 2003:1; Williams, 2001:91).

Wired Equivalent Privacy (WEP), a link-layer security protocol (Flickenger, 2003:221) has prevailed since the inception of the 802.11 standard in 1999 (Carter, 2005:190). WEP is the current security method for WLANs and provides authentication and encryption at the MAC layer of the OSI model (Tanzella, 2003:4). *Encryption* entails transforming code into an unreadable format by combining the code and a key to "produce random-looking numbers" (Edney & Arbaugh, 2004:19) and then restoring it to its original form at the destination (McCullough, 2004:167). WEP is based on the Ron's Code4 (RC4) stream cipher (Adelstein et al., 2004:482), a symmetric cipher which means that the same key is used for both encryption and decryption (Khan & Khwaja, 2003:124). A *stream cipher* "is a mathematical algorithm that expands a short key into an infinite pseudorandom key stream" (Held, 2001:51).

Below is an overview of how WEP accomplishes authentication and encryption on WLANs.

- ▣ *Authentication* is the process of verifying that a "user has permission to access the network" (Ciampa, 2001:110). Two modes of authentication are defined by WEP (Khan & Khwaja, 2003:128):
 - ▣ Open Systems Authentication-In this mode, any wireless client can associate with an AP and gain access to the network (Regan, 2003:8).
 - ▣ Shared Key Authentication-In this mode, both the wireless clients and the AP must have preconfigured matching WEP keys. The wireless client sends an

authentication request to the AP. The AP generates a challenge and sends this challenge to the wireless client. The wireless client uses its cryptographic key that is shared with the AP. WEP encrypts the challenge and if this challenge is successfully decrypted by the AP, the client will be able to authenticate with the AP.

■ *Encryption*

The WEP encryption (figure 4-9) process consists of the following steps (Arora, 2003):

- ▣ The sender generates a 24-bit initialisation vector (IV) which is concatenated with a secret key to produce a unique key for every packet.
- ▣ The key stream sequence is generated by plugging the unique key into the RC4 PRNG, a pseudo-random number generator (Lewis & Davis, 2004:194).
- ▣ WEP appends a 32-bit cyclic redundancy check (CRC) to the end of the plaintext. The CRC is used as an integrity check value (ICV) to detect any changes in the plaintext message.
- ▣ An exclusive OR (XOR) between the plaintext plus the CRC combination and the key stream yields the ciphertext. The IV, which is pre-pended to the ciphertext is transmitted in clear text. *Exclusive or (XOR)*, is a Boolean operator that contrasts two numbers to ascertain whether they are the same or not. If the numbers are the same, a "0" is returned; else, a value of "1" is returned (Sutton, 2002:6).

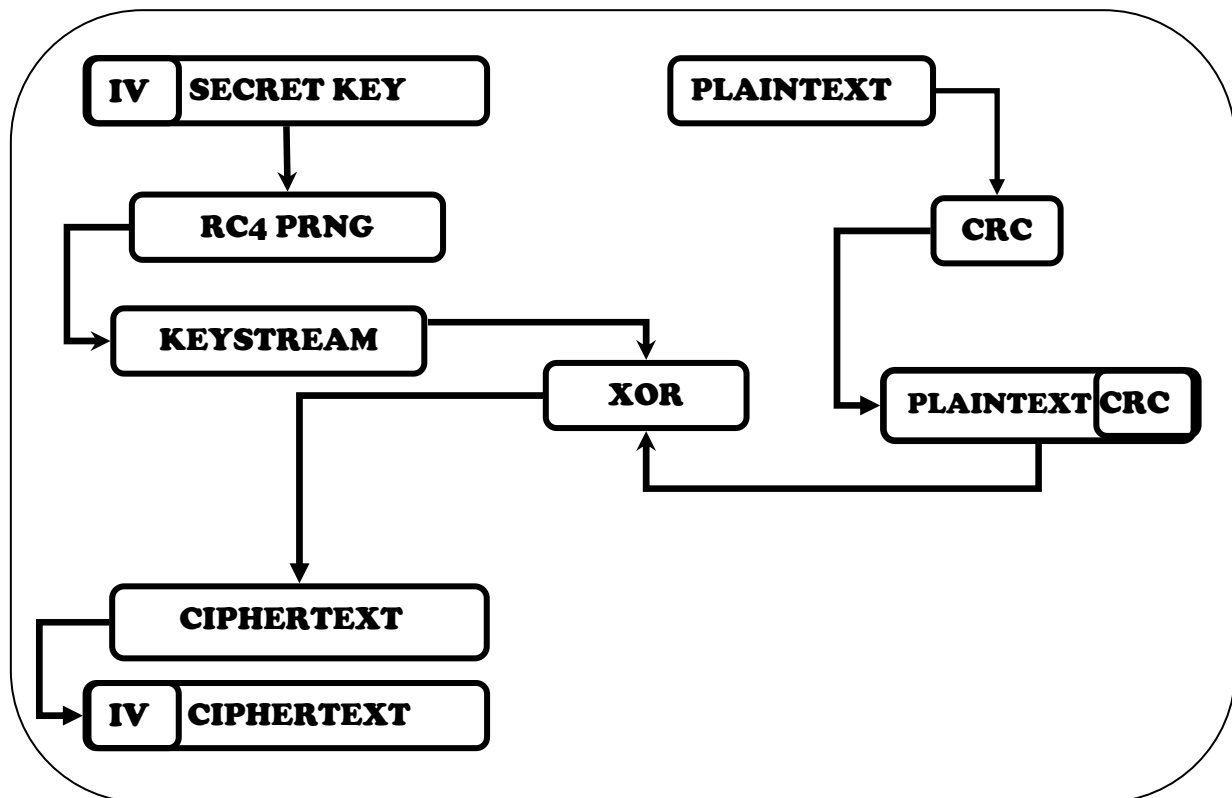


Figure 4-9: WEP encryption

4.6.2.2 PREVIOUS EXPERIENCE

Previous experience when mapped to a WLAN environment refers to citing known security issues regarding these networks.

4.6.2.2.1 WEP

The development of WEP has been primarily to address the security issues with WLANs. Ironically, the introduction of WEP has brought about its own set of security problems. (Fluhrer, Mantin & Shamir, 2001; Borisov, Goldberg & Wagner, 2001; Arbaugh, Shankar & Wan, 2001; Stubblefield, Ioannidis & Rubin, 2002; Walker, 2000).

There are several reason for the weaknesses of WEP (Peikari & Fogie, 2003; McCullough, 2004; Campbell, 2003; Regan, 2003; Lewis & Davis, 2004; Ciampa, 2006):

- ▣ WEP keys are statically assigned which means they are not likely to be changed. This makes it virtually impractical to protect the key. Furthermore, the APs and the wireless clients use the same key. This means that if WLAN intruders gain possession of this key, they can easily authenticate to the WLAN since wireless clients are authenticated and not specific users.

-
- Authentication between the wireless client and the AP is a one-way authentication. The AP authenticates the wireless client, without been authenticated itself.
 - The aim of the IV is to protect information and ideally should not appear twice, otherwise a collision will occur (Carter & Shumway, 2002:135), but its short length (3 bytes) (Berghel & Uecker, 2004:16) means that it can only take 2^{24} (16 777 216), about 17 million values (Edney & Arbaugh, 2004:75), before it starts repeating. If a WLAN intruder captures a substantial number of packets the intruder will eventually find two packets of ciphertext that have been created using the same IV and the intruder can derive the plain text in a table attack. Increasing the key length will only exponentially increase the time it takes to crack the key and will do nothing to double the protection
 - The IV sent in plaintext means that the WLAN intruder could easily view the first 24 bits of each key sent.
 - If two messages are encrypted using the same IV and the same key, then XORing the two ciphertexts will cause the keystream to cancel out and the result will be the XOR of the two plaintexts (Borisov et al., 2001:4).
 - CRC computes a checksum that is included with every packet. The receiver decrypts the frame and re-computes the CRC, which is contrasted with the one computed with the original message. If the two CRC's are not equal, this denotes an error. Since CRC is a linear checksum (Sutton, 2002:9), it allows for controlled modification of the ciphertext. It is, therefore possible to flip bits and pass the CRC check successfully.
 - Many tools are available to facilitate the task of WEP Cracking, the most popular being Airsnort ("AirSnort Homepage", n.d.) and WEPCrack ("WEPCrack - An", n.d.). Both these tools run under the Linux operating system and passively observe WLAN traffic. When a substantial amount of data has been collected, repetitions can be observed and the encryption subsequently broken.

4.6.2.3 GENETIC HERITAGE

Literally, the term *genetic* means, "antecedents of something" ("Merriam-Webster", n.d.) and *heritage* means "something transmitted by or acquired from a predecessor" ("Merriam-Webster", n.d.). This part of the OODA cycle when mapped to a WLAN environment, is the default (inherited) configurations of these networks. 802.11 networks do not offer any security by default (Carter & Shumway, 2001:107) and are devoid of the most rudimentary security measures of "encryption, personalised Service Set Identifiers

(SSIDs) and MAC address filtering" ("Enterprise Approaches", 2003) which are discussed below.

4.6.2.3.1 WEP

WEP has two default configurations (Cam-Winget, Housley, Wagner & Walker, 2003:36):

- ▣ Users are not obliged to use WEP and are oblivious of the encryption features of WEP. In fact, only a quarter of corporate WLANs use WEP for encryption (Miller, 2003:24). Support for 40-bit encryption is only mandatory for WiFi certification by the Wireless Ethernet Compliancy Alliance (WECA). WECA is an organisation that ensures interoperability of WLAN products (Khan & Khwaja, 2003:123-124). Despite the fact that, WEP is severely flawed, it can prevent novice intruders (Carter, 2005:191) and postpone intrusion attacks (Bhagyavati, Summers & DeJoie, 2004:84).
- ▣ In the shared-key authentication mode, WEP keys used to authenticate wireless clients are by default shared between the AP and all of the wireless clients in a software-accessible storage. If a WLAN intruder manages to gain access to a wireless device, the intruder has total access to the WEP key and can authenticate to the AP. WEP does not have a key management protocol, therefore it would be a monumental task to create new WEP keys and distribute these keys to all the wireless clients.

4.6.2.3.2 Service Set Identifier (SSID)

WLAN SSIDs are typically announced in the broadcast beacon frames sent by APs. It is meant for client stations to easily identify available WLANs and the APs providing the service. Every AP has a default SSID allocated by the manufacturer, e.g. tsunami for Cisco equipment and Linksys for Linksys equipment. Many organisations neglect to change the default name of the AP and instead retain the default SSIDs. It is possible to obtain these SSIDs from the default wireless configurations web site ("Default Wireless", n.d.). Furthermore, the SSID is set to broadcast mode by default, which easily allows WLAN intruders to associate with an AP. War-drivers equipped with tools such as Netstumbler sometimes scan for the SSIDs broadcast by APs to discover potential targets. WLAN intruders can set the SSID on their client to attempt to join that WLAN.

Most wireless routers permit authentication if the wireless client simply has a blank entry for the SSID (Miller, 2003:199) from which the client can obtain an IP address from a Dynamic Host Configuration Protocol (DHCP) server and from there free access to the

WLAN. *DHCP* automates the assignment of IP address to wireless clients as they connect to the wireless LAN (McCullough, 2004:38).

4.6.2.3.3 Mac address filtering

MAC address filtering means wireless clients are restricted from authenticating and associating with an AP based on their MAC addresses. The MAC address of a WNIC provides access control. *Access control* is "a process that limits those than can use a system resource" (Housley & Arbaugh, 2003:33). MAC addresses, are however, broadcast in plain text by WEP during packet transfers (Park & Dicoi, 2003:63). This means that a WLAN intruder can capture a valid MAC address by eavesdropping using a sniffer such as Ethereal and then program his/her card to have the identical MAC address using a utility such as SMAC ("SMAC Official", n.d.) (figure 4-10) and successfully gain free rein entry to the WLAN as a legitimate user. A *packet sniffer* (network analyser) (protocol analyser) is "a program that captures or intercepts data from information packets as they travel over the network" (Khan & Khwaja, 2003:96).

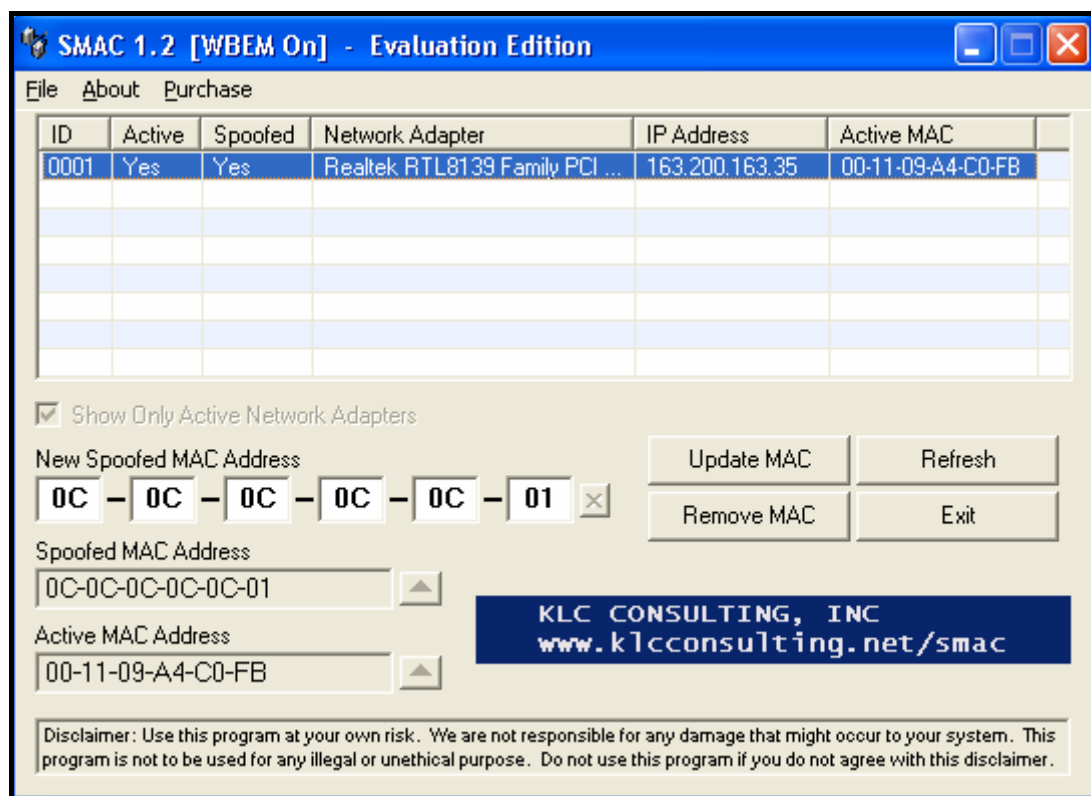


Figure 4-10: MAC address spoofing

In addition to the above, most network administrators neglect to change the following default settings:

4.6.2.3.4 AP passwords

It is possible to manage the AP through a web interface by typing in the IP address in the address field of the browser. This brings about a password-protected administrative interface. The default password for this interface as allotted by the manufacturer is always the same. It is a trivial task to determine the manufacturer by means of a sniffer program. Therefore the intruder can link the manufacturer to the default IP address and default password by searching for this vendor-specific information on the Internet and from there manipulate the AP settings successfully (Pandya & Frazin, n.d:1069).

4.6.2.3.5 Simple network management protocol (SNMP) parameters

Monitoring, controlling and managing network devices that use TCP/IP is accomplished by using SNMP (Lewis & Davis, 2004: 317). SNMP has three community strings. SNMPv1 and SNMPv2 agents use the commonly known community string "public", have assigned read and write privileges. If a WLAN intruder gains access to an AP that uses SNMP to monitor APs and wireless clients, the intruder can comfortably write information to the AP since the intruder has free read and write privileges (Karygiannis & Owens, 2002:3-27).

4.6.2.3.6 DHCP setup on wireless routers

Every computer connected to the Internet or a routed network must have a designated IP address, assigned by DHCP. If DHCP is not disabled, it distributes IP addresses to any wireless client that requests one and this includes unauthorised users as well.

4.6.2.3.7 Default subnet

Disabling DHCP means nothing if the default subnet is not changed too since most devices use the default subnet of 192.168.0.0 with a corresponding subnet mask of 255.255.255.0 (Pandya & Frazin, n.d:1070).

4.6.2.4 NEW INFORMATION

New information when mapped to a WLAN operating environment refers to the new standards and protocols developed, primarily to overcome the weaknesses in the WEP protocol. WLAN intruders must be abreast of this information so that they can discover which avenues of attack they can still exploit and what new security features can halt their attacks. The new standards include:

4.6.2.4.1 802.1x: Port-based network access control

802.1x describes a method of port authentication whereby the client (supplicant) sends Extensible Authentication Protocol (EAP) packets to an AP (authenticator) which in turn verifies the clients credentials from a central data source such as a RADIUS (Remote Dial-In user service) server. *Port-based authentication* essentially means that a *switch* (a switch is a device that routes a frame to the intended destination by recognising the destination address (Forouzan, 2003:136)) permits authorised users to connect to a network through a port (Ciampa, 2006:308). A *port* is an application-specific address on a particular receiving machine to which packets are directed (Hallberg, 2003:96). If the client's credentials match, the RADIUS server sends a WEP key to the client. The client and AP use this WEP session key to encrypt the data traffic. The word client is broadly used as opposed to wireless client because this mode of authentication applies to wired networks as well.

There are several implementations of EAP including Transport Layer Security (EAP-TLS), EAP-MD5, Lightweight EAP (LEAP), Protected EAP (PEAP) and Tunneled Transport Layer Security (EAP-TTLS) (Bhagyavati et al., 2004:85; Regan, 2003:8; Ciampa, 2006:310).

The mode of authentication used on the sample WLAN operating environment is EAP-FAST (Flexible Authentication via Secure Tunneling) (figure 4-11). The typical set-up of the EAP-FAST at the sample UNISA WLAN operating environment is as follows:

- ▣ EAP-FAST uses a symmetric key algorithm to achieve a tunnel authentication process that relies on manual Protected Access Credential (PAC) provisioning that is managed via an Authentication, Authorisation and Accounting server (AAA) such as Cisco's Secure Access Control Server (ACS).
- ▣ EAP-FAST authentication takes place between the wireless clients and the ACS server.
- ▣ The wireless clients and the AP are configured with WEP encryption.
- ▣ An external user database together with EAP-FAST provides user authentication.

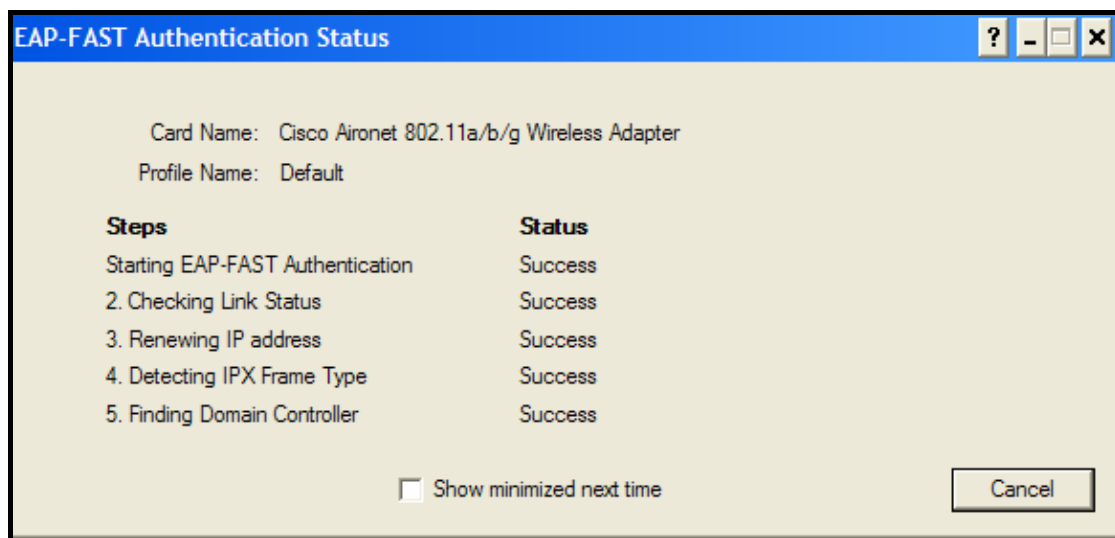


Figure 4-11: EAP-FAST Authentication at the sample UNISA WLAN operating environment

802.1x provides enhanced security by virtue of mutual authentication as well as by dynamic per user and per session encryption keys ("Give your network", 1995-2005:4).

A significant disadvantage of 802.1x is that it requires more back-end equipment and a dedicated RADIUS server with 802.1x capabilities (Maxim & Pollino, 2002:196). 802.1x is itself not the panacea for curing the problems with WEP, as it is prone to *man-in-the-middle attacks* as well as *session hijacking* attacks (Arbaugh & Mishra, 2002:7). The man-in-the-middle attack occurs primarily because 802.1x uses only one-way authentication. Once a client authenticates and a switch port opens, further communications between the supplicant and the switch are not authenticated. An intruder can thus capture the legitimate wireless client's MAC and IP addresses by sniffing and successfully authenticate with the RADIUS server. Upon successful authentication, it will be possible to take over the session of the legitimate client.

802.1x addresses authentication but not encryption and must therefore work as a component of both WiFi Protected Access (WPA) and 802.11i in order to address encryption (Williamson, 2004:10). The following section discusses this.

4.6.2.4.2 802.11 and WPA

802.11i overcomes most of WEP's inadequacies but because a large installed base of legacy systems will continue for some time (Adelstein et al., 2004:482) before 802.11i is fully

embraced, WLAN intruders can still exploit the vulnerabilities of WEP. For new systems, 802.11i and WPA are collective names for a host of security protocols.

The following table (table 4-1) outlines the marked differences between these two standards:

WPA	802.11i
<p>WPA is a standard proposed by the WiFi Alliance in November 2002 (Fung, 2005:198) as an intermediary standard before the ratification of 802.11i..</p>	<p>802.11i, also known as robust network security (RNS) ratified in June 2004 (Williams, 2004) is a standard proposed by the IEEE to replace WEP.</p>
<p>WPA uses the Temporal Key Integrity Protocol (TKIP) with the RC4 stream encryption algorithm. TKIP provides for better encryption by (Arora, 2003):</p> <ul style="list-style-type: none"> ▣ Preventing the use of static keys by generating a new encryption key for each 802.11 packet (Neoh, 2003:9). ▣ Larger IV values (Edney & Arbaugh, 2004:235) that are hashed which means that they are encrypted rendering them difficult to sniff (Peikari & Fogie, 2003:278). <i>Hashes</i> are a special use of one-way function that provides authentication and verification by virtue of encryption (Howlett, 2005:285). ▣ A Message Integrity Check (MIC) that prevents an intruder from modifying and resending packets (Peikari & Fogie, 2003:278). This is a bid to overcome the problems with the CRC function of WEP. 	<p>802.11i uses the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) with the Advanced Encryption Standard (AES) cipher for encryption. AES offers the following enhancements over WEP (Park & Dicoi, 2003:64):</p> <ul style="list-style-type: none"> ▣ Key sizes of 128, 192 or 256 bits. ▣ Eliminating the reuse of the 24-bit IV. <p>AES also suffers from the following drawbacks (Park & Dicoi, 2003:65; Wong, 2003:8):</p> <ul style="list-style-type: none"> ▣ An organisation has to replace all its APs in order to be compatible with this standard. ▣ Large key sizes mean that greater processing power is required by wireless clients for encryption and decryption. ▣ AES also requires greater power consumption which is not provided by current WNICs.

WPA	802.11i
<p>☐ Better key management.</p> <p>TKIP however, also relies on a pre-shared key and is therefore, also susceptible to <i>man-in-the-middle</i> attacks (Godber & Dasgupta, 2003). Both TKIP and WEP will eventually be replaced with the Advanced Encryption Standard (AES), which uses the more robust Rijndael algorithm (Cannon, 2006:143).</p> <p>WiFi Protected Access 2 (WPA2) ratified in September 2004 (Ciampa, 2006:299) is the newer generation of WPA security. WPA2 is based on the IEEE 802.11i standard. WPA2 uses AES for encryption and IEEE 802.1x for authentication. WPA2 allows both AES and TKIP clients to co-exist on the same WLAN.</p>	<p>AES is however one of the most concrete encryption schemes and to date has not been subjected to any attacks ("Give your network", 1995-2005:9).</p>

Table 4-1: Differences between 802.11i and WPA

4.6.2.4.3 Social environment of WLAN intruders

WLAN intruders typically obtain new information on intrusion techniques from dedicated WLAN hacking sites on the Internet ("Scanning and", 2004) as well as by socially interacting with other users on user groups on the Internet. Furthermore, there are certain hacking conventions such as DEFCON ("Welcome to DEF", 1992), Hackers on Planet Earth (HOPE) ("2600 The Hacker", 1995) and ToorCon ("ToorCon 7", n.d.) to discuss hacking techniques and tools. All this information equips WLAN intruders with a wealth of information and an arsenal of tools to launch potentially devastating intrusion attacks.

The orientation phase terminates at the point where WLAN intruders have an awareness of the security holes they can exploit in WLANs. The next step entails creating a hypothesis of

WLAN intrusion attacks. This is covered in the decision phase of the OODA cycle of the WLAN intruder discussed below.

4.7 DECISION

After discovering the presence of WLANs and creating a mental image of the security weaknesses of these networks, WLAN intruders can contrive on the various types of intrusion attacks to launch where an intrusion is defined as "violations of security policy, usually characterised as attempts to affect the confidentiality, integrity or availability of a computer or network" (Bace^b, 2002:37-2). These attacks could be simple innocuous attacks or potentially devastating ones.

Some of the types of intrusion attacks include (Sundaram, 1996:5; Karygiannis & Owens, 2002:20; Buzzard, 1999:323):

4.7.1 DENIAL-OF-SERVICE (DOS) ATTACKS

A DOS attack is specifically aimed at preventing legitimate users from using the WLAN. A common form of DOS attack is jamming which entails removing a wireless client off the air by superseding the APs signal with a stronger signal (Lewis & Davis, 2004:157). Jamming can occur in the following instances:

- ▣ By a malicious user who consciously emanates a signal from another wireless device in order to saturate the bandwidth thereby denying legitimate users the opportunity of using the WLAN.
- ▣ By inadvertent users who download large files, once again saturating the bandwidth.
- ▣ By electronic devices such as cordless phones (figure 4-12), baby monitors, elevator motors, photocopying machines, theft protection devices and microwave ovens (Maxim & Pollino, 2002:51; Ciampa, 2001:19) that use the same frequency range as 802.11b and 802.11g (Carter, 2005:29).

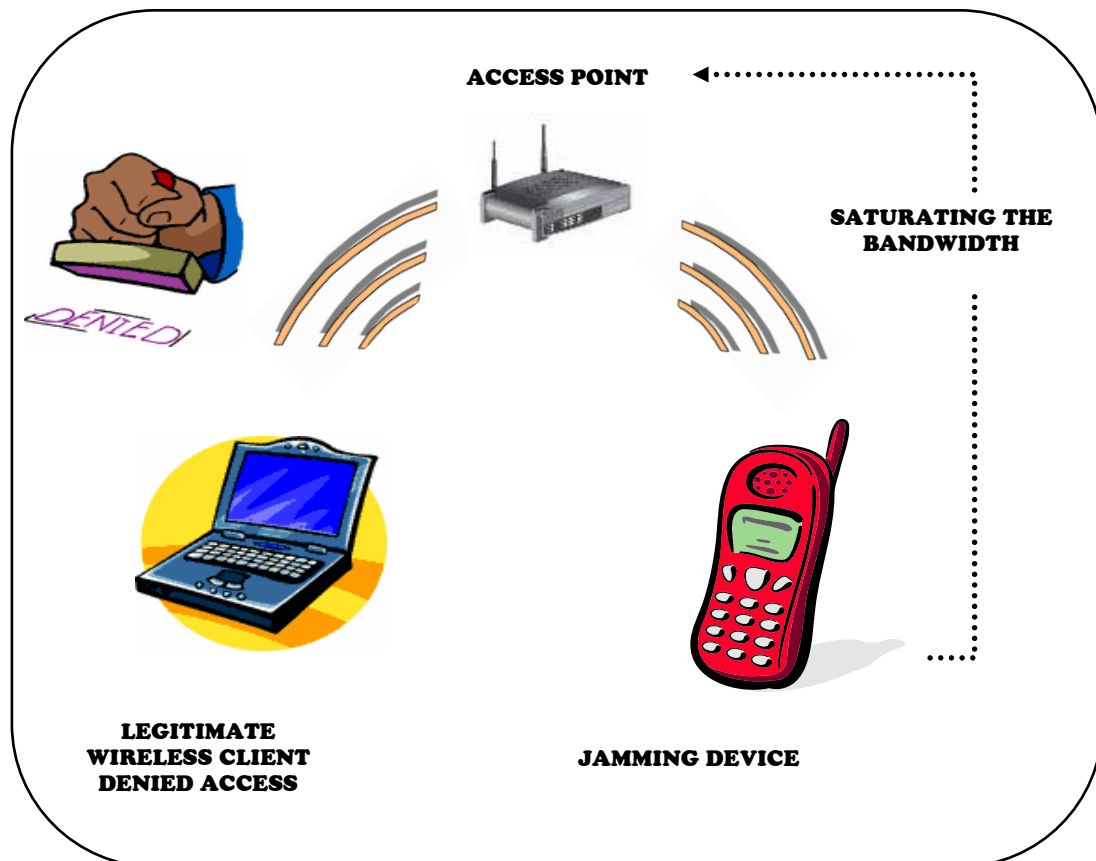


Figure 4-12: A Denial-of-service attack using jamming

Battery exhaustion is also a means of a denial-of-service attack (Stanley, 2002:12) where software placed in the wireless client can interfere with the power management function. This exhausts the battery more rapidly, forcing the wireless client off the network.

If the default AP settings are not changed and the WLAN intruder has free rein to manipulate the administrative console of the AP, the intruder can launch a DOS attack by changing certain settings on the AP, thereby denying legitimate wireless users access to the resources on the WLAN.

Another common type of DOS attack occurs with the 802.11 protocol, where a flood of 802.11 associate frames from an offending WLAN intruder renders it difficult for other legitimate wireless clients to associate with the AP because the WLAN intruder occupies the slots of other wireless clients. The WLAN intruder can also send a fleet of disassociate commands, forcing all wireless clients to disconnect from the WLAN.

4.7.2 MASQUERADE ATTACKS

A rogue AP deemed among the "greatest security threats in corporate America" (Chartoff & Boyland, 2004:41) can be successfully deployed in a WLAN environment by having the same SSID as the legitimate AP. If open authentication is used, a client can authenticate with the rogue AP if the rogue AP emanates a stronger signal than the legitimate AP (figure 4-13). Software tools such as FakeAP ("Projects - FakeAP", 2001-2002), render it possible to create virtual APs with a strong signal and MAC address to pose as legitimate APs.

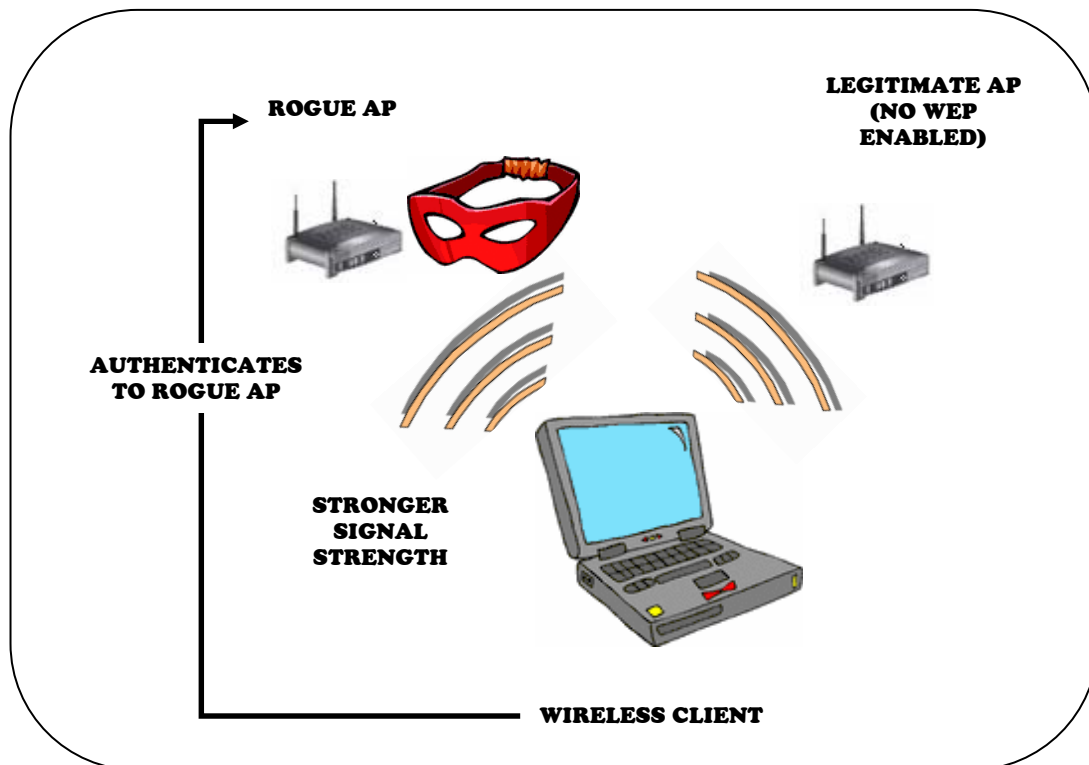


Figure 4-13: Rogue access point

In this mode, an AP can pose as a legitimate AP and force clients to associate with it thereby capturing the necessary credentials from the client. The WLAN intruder can then use the authentication requests of the legitimate user in an attempt to associate with a legitimate AP in order to gain access to the wired network. This is a classic case of the *man-in-the-middle* attack where the rogue AP acts as an AP to the wireless client and a user to the legitimate AP.

The WLAN intruder, now posing as a rogue AP, can also create a *DOS* attack by sending a constant stream of disassociate commands forcing the clients to detach themselves from the WLAN. The attacker can then use this opportunity to use the victim's MAC address to

hijack the user's session because in essence the user is not actually disconnected from the network.

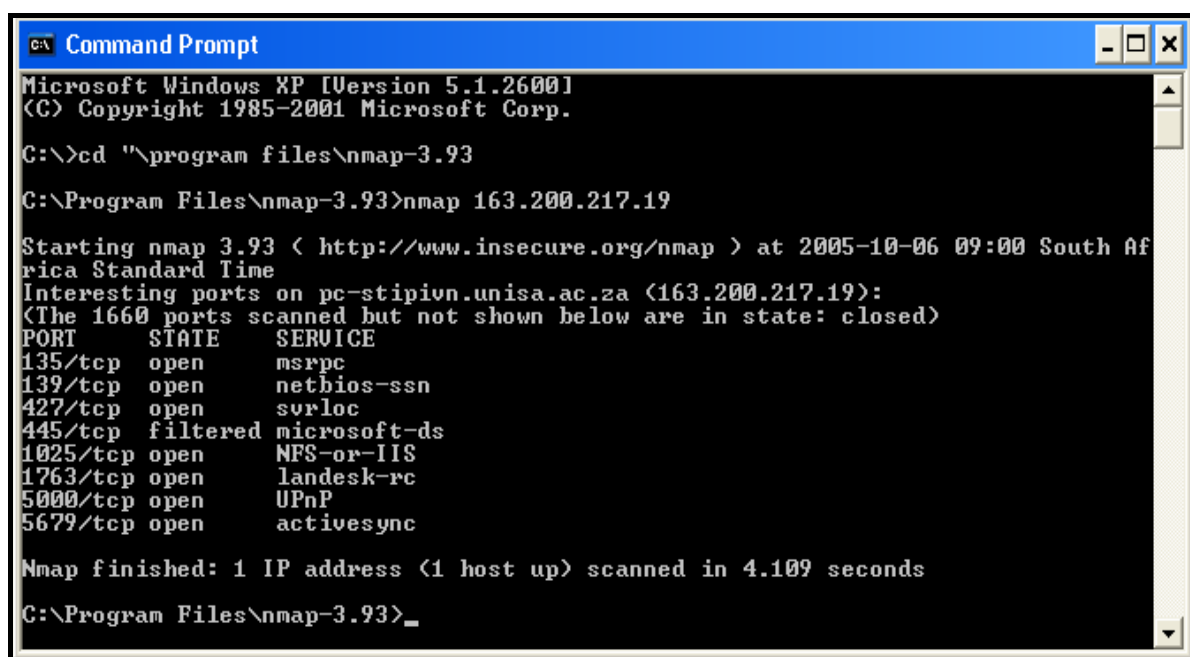
Rogue APs, can also be installed by well-meaning employees who wish to extend the range of the WLAN but do not have the necessary permission to do so. This opens up security windows that WLAN intruders can exploit (Chartoff & Boyland, 2004:88).

4.7.3 PENETRATION OF THE SECURITY CONTROL SYSTEM

Penetration of the security control system can occur by using a *port scanner* such as Superscan, SNScan, Look@Lan (Lewis & Davis, 2004:167) which an intruder can use to determine if a specific service is running on the victims computer (McCullough, 2004:79). One of the most popular port scanners is Network Mapper (NMap) and the prime advantages of this port scanner include (Howlett, 2005:96-97):

- ▣ NMap has a conglomerate of variations regarding how one can scan the network.
- ▣ NMap is easy to use.

The following figure (figure 4-14) depicts the output of a typical scan that was done on the sample UNISA WLAN operating environment using Nmap, Version 3.93. From this output it is possible to see the tcp ports that are open on the victim computer with an IP address of 163.200.217.19.



```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\>cd "\program files\nmap-3.93
C:\Program Files\nmap-3.93>nmap 163.200.217.19

Starting nmap 3.93 ( http://www.insecure.org/nmap ) at 2005-10-06 09:00 South Af
rica Standard Time
Interesting ports on pc-stipivn.unisa.ac.za (163.200.217.19):
(The 1660 ports scanned but not shown below are in state: closed)
PORT      STATE      SERVICE
135/tcp   open      msrpc
139/tcp   open      netbios-ssn
427/tcp   open      svrloc
445/tcp   filtered  microsoft-ds
1025/tcp  open      NFS-or-IIS
1763/tcp  open      landesk-rc
5000/tcp  open      UPnP
5679/tcp  open      activesync

Nmap finished: 1 IP address (1 host up) scanned in 4.109 seconds
C:\Program Files\nmap-3.93>_
```

Figure 4-14: NMap scanning at the sample UNISA WLAN operating environment

4.7.4 LEAKAGE

APs can broadcast signals ranging from about 150 feet to approximately 1 500 feet depending on their configuration ("Federal Agencies", 2005:10). Therefore, APs can broadcast signals outside the physical boundaries of a building. As a result of this, an AP that is in close proximity of another WLAN can emanate a powerful signal that filtrates into the air space of a neighbouring WLAN, causing the wireless clients of the neighbouring WLAN to associate with this AP and reveal sensitive information ("Wireless LAN - What", 2003:2).

4.7.5 MONITORING COMMUNICATIONS (EAVESDROPPING)

The open-air nature of wireless communication means information transmitted or received over a wireless network is prone to interception and eavesdropping. A WLAN intruder can capture messages between the AP and the wireless client by intercepting the radio transmission between the AP and the wireless client by using a wireless packet sniffer such as Ethereal. It is then possible to gather information such as "user logon credentials, networking information, e-mail or potentially anything else that traverses the segment" (Carter & Shumway, 2001:17).

The following diagram (figure 4-15) illustrates the output of an Ethereal scan conducted on the sample UNISA WLAN operating environment. Ethereal was used as it is one of the most popular and powerful sniffers available (Flickenger, 2003:94; Peikari & Fogie, 2003:167).

From this scan, it is possible to see how easy it can be to analyse the HTTP protocol and view the contents of the packet in plain ASCII.

The screenshot shows the Ethereal interface with a list of captured packets. The selected packet (No. 257) is expanded to show its details:

No.	Time	Source	Destination	Protocol	Info
253	75.809551	163.200.97.20	163.200.217.11	DNS	standard query response A 163.200.9.220
254	75.810541	163.200.217.11	163.200.9.220	TCP	32772 > 3128 [SYN] Seq=0 Ack=0 win=5840 Len=
255	75.810557	163.200.9.220	163.200.217.11	TCP	3128 > 32772 [SYN, ACK] Seq=0 Ack=1 win=5792
256	75.810671	163.200.217.11	163.200.9.220	TCP	32772 > 3128 [ACK] Seq=1 Ack=1 win=5840 Len=
257	75.811046	163.200.217.11	163.200.9.220	HTTP	GET http://fedora.redhat.com/images/favicon.
258	75.811256	163.200.9.220	163.200.217.11	TCP	3128 > 32772 [ACK] Seq=1 Ack=447 win=6864 Le
259	75.812633	163.200.9.220	163.200.217.11	HTTP	HTTP/1.0 403 Forbidden (text/html)
260	75.812305	163.200.217.11	163.200.9.220	TCP	32772 > 3128 [ACK] Seq=447 Ack=1118 win=8076

Expanded packet details for Frame 257 (512 bytes on wire, 512 bytes captured):

- Ethernet II, Src: 00:0b:cd:88:72:47, Dst: 00:00:0c:07:ac:d9
- Internet Protocol, Src Addr: 163.200.217.11 (163.200.217.11), Dst Addr: 163.200.9.220 (163.200.9.220)
- Transmission Control Protocol, Src Port: 32772 (32772), Dst Port: 3128 (3128), Seq: 1, Ack: 1, Len: 446
- Hypertext Transfer Protocol
 - GET http://fedora.redhat.com/images/favicon.ico HTTP/1.1\r\n
 - Host: fedora.redhat.com\r\n
 - User-Agent: Mozilla/5.0 (X11; U; Linux i686; rv:1.7.3) Gecko/20041020 Firefox/0.10.1\r\n
 - Accept: image/png, */*;q=0.5\r\n
 - Accept-Language: en-us,en;q=0.5\r\n
 - Accept-Encoding: gzip, deflate\r\n
 - Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7\r\n
 - Keep-Alive: 300\r\n
 - Proxy-Connection: keep-alive\r\n
 - If-Modified-Since: wed, 30 Mar 2005 17:47:23 GMT\r\n

Hex dump of the packet data:

```

0000 00 00 0c 07 ac d9 00 0b cd 88 72 47 08 00 45 00 .....rG..E.
0010 01 f2 60 9c 40 00 40 06 ad f1 a3 c8 d9 0b a3 c8 ..@. @.....
0020 09 dc 80 04 0c 38 71 f6 04 ba 9f aa 3b 6e 80 18 ....8q. ....;n..
0030 05 b4 9b 39 00 00 01 01 08 0a 00 23 64 22 03 f7 ...9....#d"...
0040 09 e2 47 45 54 20 68 74 74 70 3a 2f 2f 66 65 64 .RGET ht tp://fed
0050 6f 72 61 2e 72 65 64 68 61 74 2e 63 6f 6d 2f 69 ora.redh at.com/i
0060 6d 61 67 65 73 2f 66 61 76 69 63 6f 6e 2e 69 63 mages/fa vicon.ic
0070 6f 20 48 54 54 50 2f 31 2e 31 0d 0a 48 6f 73 74 n HTTP/1 1 Host

```

Figure 4-15: Ethereal scan at the sample UNISA WLAN operating environment

4.7.6 MALICIOUS USE

This can occur when a WLAN intruder physically steals a legitimate WNIC that has a MAC address pre-programmed as allowed on the AP and then uses this card to authenticate with the AP. A WLAN intruder can also maliciously use someone else's wireless Internet access. A reported incident of this has occurred, where David M. Kauchak was fined \$250 and a years court supervision for illegally surfing the Web from his laptop (Green, 2006).

In a similar incident, the first of its kind in U.K., Gregory Straszkiwicz, was fined 500 pounds and 12 months conditional discharge for hijacking a wireless broadband connection (Ilett, 2005).

4.7.7 REPLAY ATTACKS

Cyclic Redundancy Checks do not provide any means of ensuring the integrity of a data stream that a WLAN intruder has intentionally corrupted. If a WLAN intruder has knowledge of a certain data stream, it is possible to change the contents and successfully complete the transaction with a legitimate checksum. The receiver would have no knowledge of this because the checksum would match.

4.7.8 SOCIAL ENGINEERING

Social engineering is a "non-technical means" (McMahon, 2003:301) used by WLAN intruders to lure unsuspecting WLAN users to disclose their usernames and passwords in order to gain illicit entry into the network. Getting WLAN users to disclose this information can be a trivial task as most users are naïve and trusting. Kevin Mitnick, a famous reformed hacker illustrates how easy it is to exploit human trust with a study conducted in the U.K. This study revealed that seven out of 10 office workers readily disclosed their usernames and passwords in return for an Easter egg when approached at London's Waterloo station (Glazier, 2006).

4.7.9 BRUTE FORCE ATTACKS

As expounded previously, when a wireless client wishes to authenticate itself with an AP, it commonly sends a probe request packet out on all the channels (section 4.4.4). The AP receives this packet and sends a probe response packet back to the wireless client. The probe response packet contains vital information including the SSID, which the wireless client uses to ascertain with which AP it will associate. A *brute force probe* occurs when a wireless client has been sending probes of the AP with different SSIDs in them, in an attempt to guess the SSID of the AP.

A brute force attack can also occur when a persistent WLAN intruder uses all possible combinations of letters and numbers to guess the username/password of a legitimate user and then use this information to gain illicit entry to the WLAN.

Having created a hypothesis of the multitude of possible attacks, the next stage is to activate the WLAN intrusion attack plan. This action phase of the OODA cycle of the WLAN intruder discusses this.

4.8 ACTION

Having decided on the possible types of WLAN intrusion attacks, the final stage is to carry out these attacks in practice.

After observing the OODA cycle of the WLAN intruder, an organisation must observe itself to uncover any major security holes in its WLAN environment, which intruders can use as windows of opportunity to launch intrusion attacks.

4.9 OBSERVING ONESELF

To sense oneself, it is necessary for an organisation to determine whether its APs are freely open and accessible to WLAN intruders. This is a relatively simple task, accomplished by visiting the Wireless Geographic Logging Engine (Wigle) website. By entering the MAC address of the AP, obtainable by issuing an `ipconfig/all` command on a Windows XP operating system (figure 4-16), an organisation can ascertain whether its APs have been discovered. An organisation can also use NetStumbler to check that its WLANs are not freely open and accessible to anyone.

```
Ethernet adapter Wireless Network Connection 4:
    Media State . . . . . : Media disconnected
    Description . . . . . : Cisco Systems 350 Series PCMCIA 802.
11b Wireless LAN Adapter by AirMagnet
    Physical Address. . . . . : 00-0D-BD-8F-45-A9
```

Figure 4-16: Obtaining the MAC address of a WNIC

Having completed all three aspects of the observation phase, the risk analysis team can now begin enacting the remaining activities of the knowledge elicitation phase. Appendix C covers these activities.

4.10 CONCLUSION

This chapter concludes at a point of situational analysis, where the University is enriched with knowledge regarding the real and perceived type of intrusion attacks that could be launched on its WLAN operating environment. This was determined by studying how WLAN intruders mentally compose themselves to enter WLANs illicitly. Studying the WLAN operating environment rendered it possible to pinpoint the most important assets that require the greatest protection.

This chapter covered the WLAN intrusion security organisational view. The next chapter focuses on the continuation of the WLAN intrusion security risk analysis exercise by covering the analysis activities required for the orientation phase.



CHAPTER

5. ORIENTATION: TECHNICAL VULNERABILITY ASSESSMENT AND RISK IMPACT

5.1 INTRODUCTION

A risk analysis immediately conjures up the notion of a technological evaluation (Alberts & Dorofee, 2003:137). Security, however, is a "business or organisational problem", yet many organisations adopt only a "technology-centric" approach (Caralli & Wilson, 2004:8). Conducting a WLAN intrusion security risk analysis exercise encompasses both an organisational evaluation and a technological evaluation. Having completed the organisational evaluation, this chapter focuses on the technological evaluation.

The objective of this chapter is to illustrate how each critically identified asset is threatened, the technological weaknesses present in the WLAN infrastructure and how threats can affect the University's missions and aims.

5.2 STRUCTURE OF THIS CHAPTER

"When evaluating risks to organisational processes, analysts generally begin by performing an assessment to provide a snapshot of current risks" (Alberts & Dorofee, 2004:142). This is accord with the orientation phase of the OODA cycle. The orientation phase advocates creating a mental image or snapshot of the situation.

The orientation phase advocates commencing an initial assessment. This equates to the threat assessment, technological vulnerability assessment and risk impact assessment of the WLAN intrusion security risk analysis process to cover all the analysis activities. The analysis information is stored in the database.

The following diagram (figure 5-1) depicts the role of this chapter within the overall context of the dissertation.

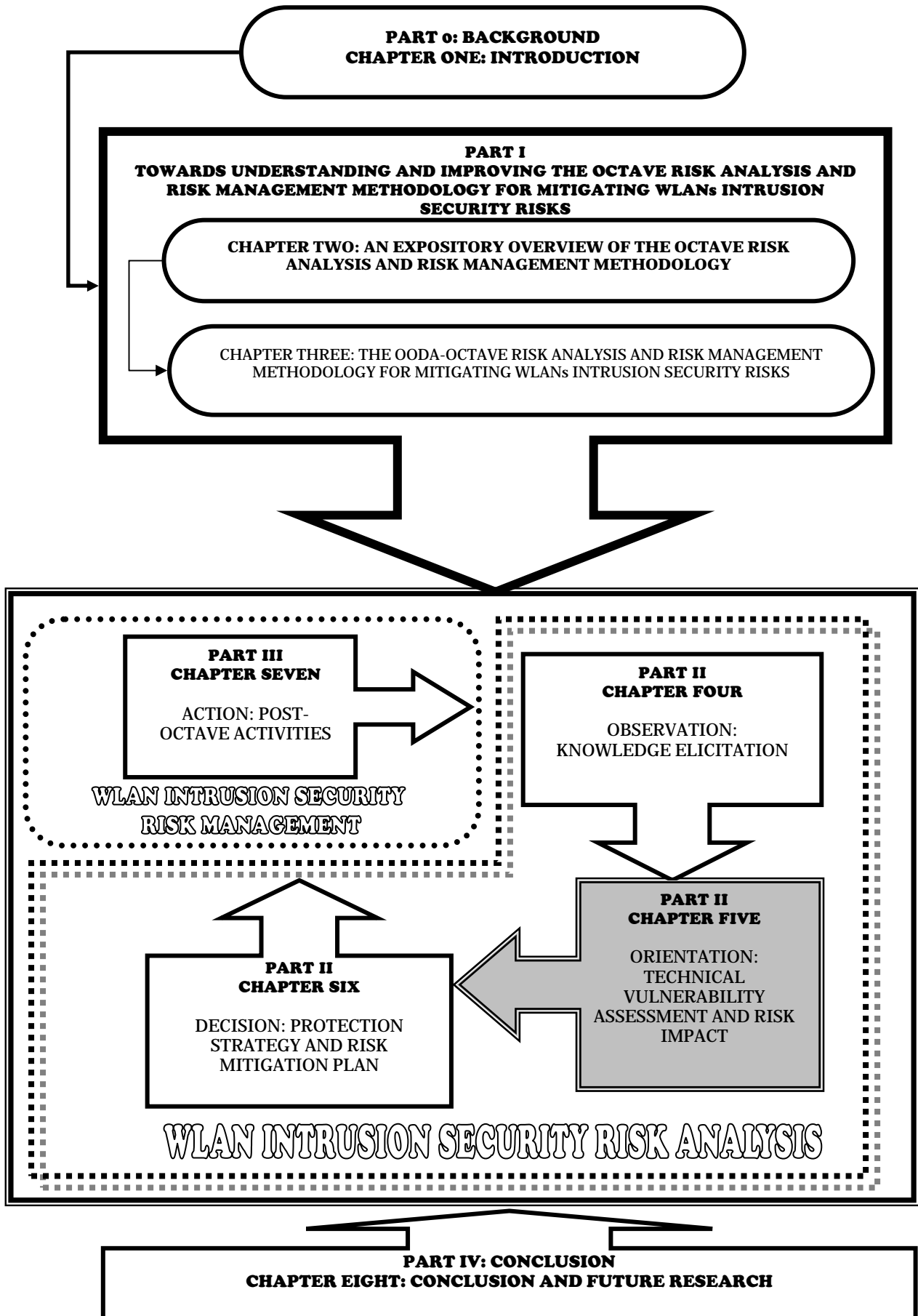


Figure 5-1: The role of chapter five within the overall context of the dissertation

5.3 THREAT ASSESSMENT

Conducting a threat assessment comprises the following activity (Alberts & Dorofee, 2003:48):

5.3.1 IDENTIFYING THREATS TO CRITICAL ASSETS

This step entails creating a threat profile for the critically identified asset (infrastructure BSS), by mapping the outcomes of the various areas of concern. The outcomes include disclosure, modification, loss/destruction and interruption (appendix C, figures 11-2 to 11-10). A *threat profile*, defines the range of threats than can affect an asset using the following properties (Alberts & Dorofee, 2003:112):

- ▣ Asset—something of value to the University.
- ▣ Actor—who or what may violate the security requirements (confidentiality, integrity, availability) of an asset.
- ▣ Motive (optional)—defines whether the actor’s intentions are deliberate or accidental.
- ▣ Access (optional)—how the asset is accessed by the actor (network access, physical access).
- ▣ Outcome—the immediate outcome (disclosure, modification, destruction, loss, interruption) of violating the security requirements of an asset.

Threat profiles contain categories grouped according to source. The main threat category is:

- ▣ Human actors using wireless network access-These are wireless network-based threats to the critical assets.

Figure 5-2 illustrates the asset-based threat profile for human actors using wireless network access. Since the origin or intent of the unauthorised individual are of no consequence (section 1.4), these properties are not considered. The next to the outcome indicates that particular outcome manifestation.

The screenshot displays a 'Threat' profile window. At the top right, the 'Asset Name' is 'Infrastructure BSS' and the 'Type of threat' is 'Human actors using wireless access'. Below this, there are four record sections, each with a 'Record: 1 of 1' indicator. Each record section contains two rows of options: 'Actor' with 'Insider' and 'Outsider' (both unchecked), and 'Motive' with 'Accidental' and 'Deliberate' (both unchecked). On the left side, under the 'Outcome' section, there are four checkboxes: 'Disclosure' (checked), 'Modification' (checked), 'Loss/Destruction' (checked), and 'Interruption' (checked).

Figure 5-2: Asset-based threat profile for human actors using wireless network access

5.4 TECHNOLOGICAL VULNERABILITY ASSESSMENT

The technological vulnerability assessment addresses the technological aspects of information security highlighting the technological vulnerabilities in relation to the assets, security requirements and threats of phase 1 (Alberts & Dorofee, 2003:37). The first step of this phase is the selection of infrastructure components which are examined for technological weaknesses and comprises the following two activities (Alberts & Dorofee, 2003:48):

5.4.1 IDENTIFY KEY CLASSES OF COMPONENTS

In order to identify key classes of components, it is necessary to have a network topology diagram. The network topology diagram (figure 5-3), is that of the UNISA WLAN operating environment as this environment has been sampled for the WLAN intrusion security risk analysis exercise.

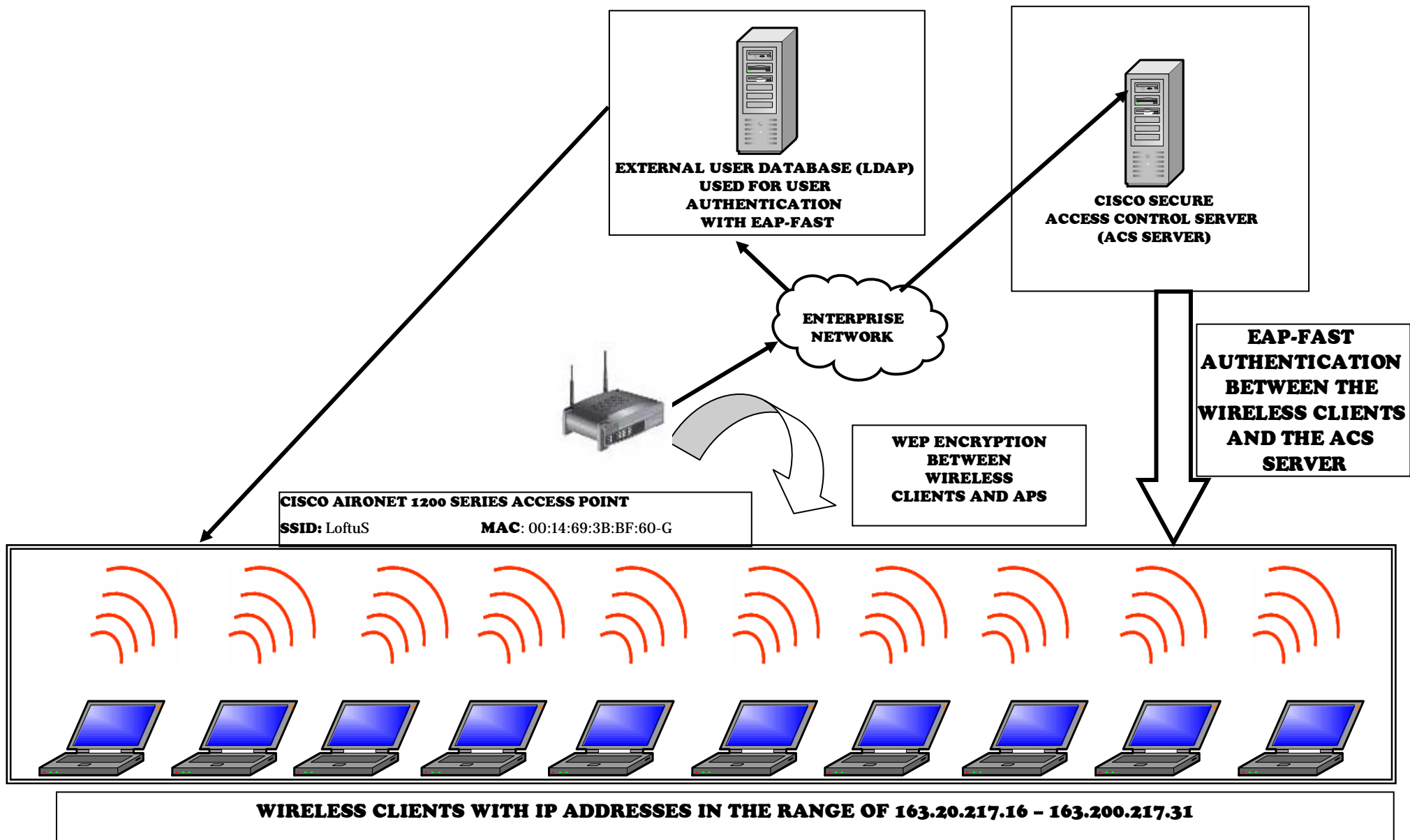


Figure 5-3: Topology diagram of the sample UNISA WLAN operating environment

For system assets, the system of interest is the asset itself (Alberts & Dorofee, 200:144). Therefore, the system of interest is the infrastructure-based network itself. Identifying key classes of components related to the system of interest entails examining the types of components that are part of the system of interest. By examining the topology diagram, the following important components are identified (figure 5-4).

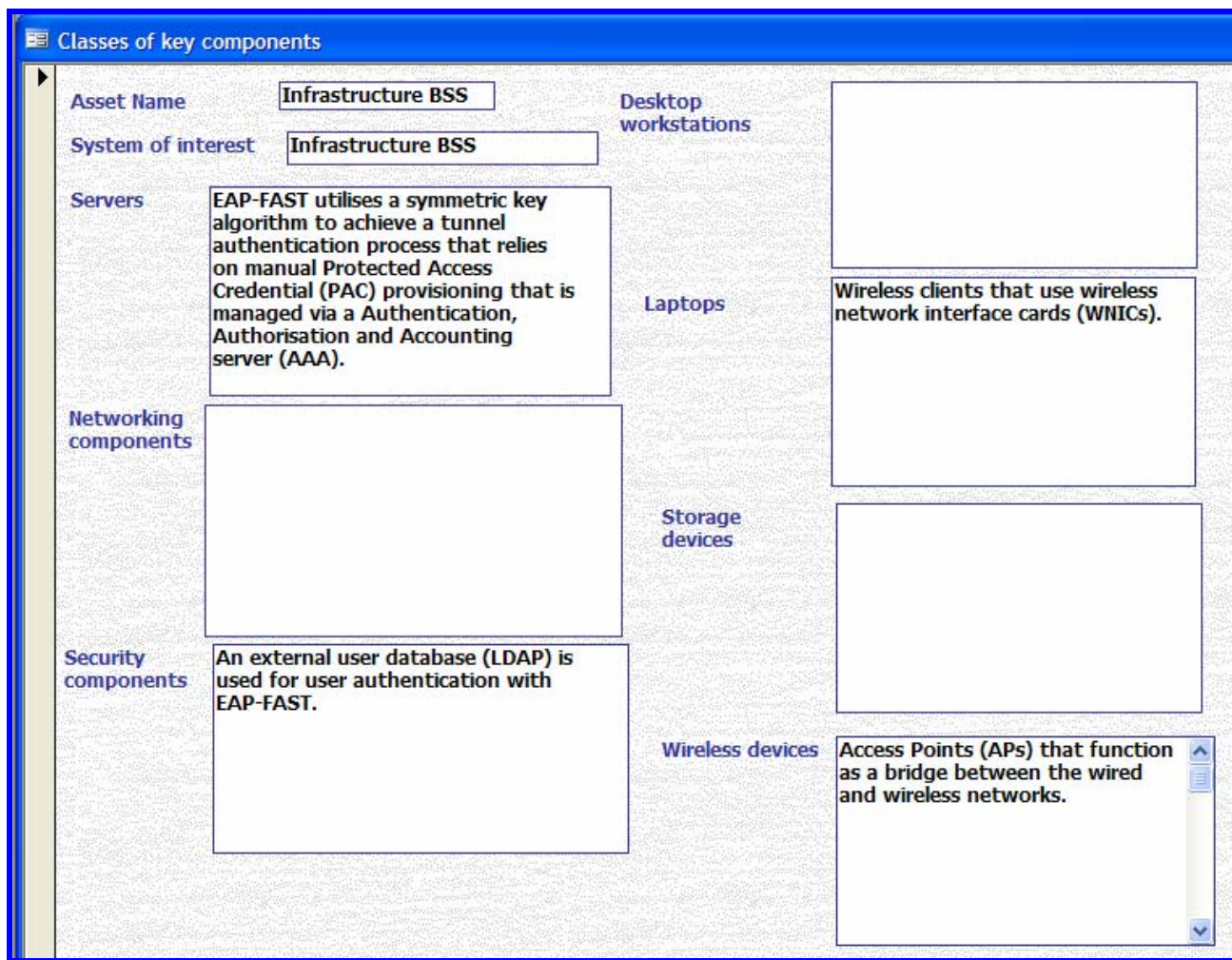


Figure 5-4: Identifying key classes of components

5.4.2 IDENTIFY INFRASTRUCTURE COMPONENTS TO EXAMINE

This entails pinpointing very specific components which are examined for technological vulnerabilities. Therefore drilling down the key classes of components reveals the wireless clients and the APs as the two most important infrastructure components. These are the two most important constituents of the WLAN operating environment (figures 5-5 and 5-6). A vulnerability analysis approach and the specific tools for conducting the vulnerability analysis exercise are selected.

The screenshot shows a web-based application window titled 'InfrastrutureComponents'. The main content area is divided into several sections:

- Component Name:** Wireless clients
- Description:** The wireless clients equipped with wireless network interface cards (WNICs) facilitate the task of sending and receiving data.
- Rationale for Component Selection:** A wireless client is one of the most important components of an infrastructure-based WLAN. It will be virtually impossible to send and receive data without a wireless client such as a laptop.
- IP Address:** 163.200.217.19
- DNS Name:** (Empty field)
- Name of Component Evaluator:** Hanifa Abdullah
- Evaluation Tools Used:** AirMagnet
- Date of Component Evaluation:** 11/10/2005
- Method of Assessment:** A vulnerability analysis tool to provide a point-in-time view of the security state of the wireless clients.
- Approval Authority:** Network administrator at UNISA
- Class of component:** Laptops (dropdown menu)
- System of interest:** Infrastructure BSS (dropdown menu)

At the bottom of the window, there is a record navigation bar showing 'Record: 1 of 2' with navigation icons.

Figure 5-5: Identifying wireless clients as an infrastructure component

The screenshot shows the same 'InfrastrutureComponents' application window, but with the entry for 'Access Points (APs)'. The main content area is divided into several sections:

- Component Name:** Access Points (APs)
- Description:** The AP is the central hub of a WLAN and is normally connected to a fixed-wired LAN.
- Rationale for Component Selection:** The AP functions as a bridge between the wired and wireless networks allowing WLAN users access to fixed-wired resources such as e-mail servers, application servers, the Internet and/or the University intranet.
- IP Address:** (Empty field)
- DNS Name:** (Empty field)
- Name of Component Evaluator:** Hanifa Abdullah
- Evaluation Tools Used:** AirMagnet
- Date of Component Evaluation:** 11/10/2005
- Method of Assessment:** Use of a vulnerability analysis tool to provide a point-in-time view of the security state of the APs.
- Approval Authority:** Network administrator at UNISA
- Class of component:** Wireless devices (dropdown menu)
- System of interest:** Infrastructure BSS (dropdown menu)

Figure 5-6: Identifying APs as an infrastructure component

The next step is to identify technological weaknesses with respect to the infrastructure components identified (wireless clients and APs) and comprises the following two activities (Alberts & Dorofee, 2003:49):

5.4.3 RUN VULNERABILITY EVALUATION TOOLS ON SELECTED INFRASTRUCTURE COMPONENTS

A *vulnerability assessment* is "a systematic, point-in-time examination of an organisation's technology base, policies and procedures" (Alberts & Dorofee, 2003:6).

AirMagnet ("Enterprise Wireless", n.d.), is used to conduct a point-in-time analysis of the sample UNISA WLAN operating environment. The aim of this vulnerability exercise is to pinpoint vulnerabilities related to the most important infrastructure components (wireless clients and APs) identified.

To ensure that the vulnerabilities are all current ones, these vulnerabilities can be checked, against the Wireless Vulnerabilities and Exploits Catalogue (WVE), a catalogue for wireless vulnerabilities and exploits ("Wireless Vulnerabilities", n.d.). However, this catalogue is not yet very comprehensive and currently lists only 50 results for WLANs exploits and vulnerabilities.

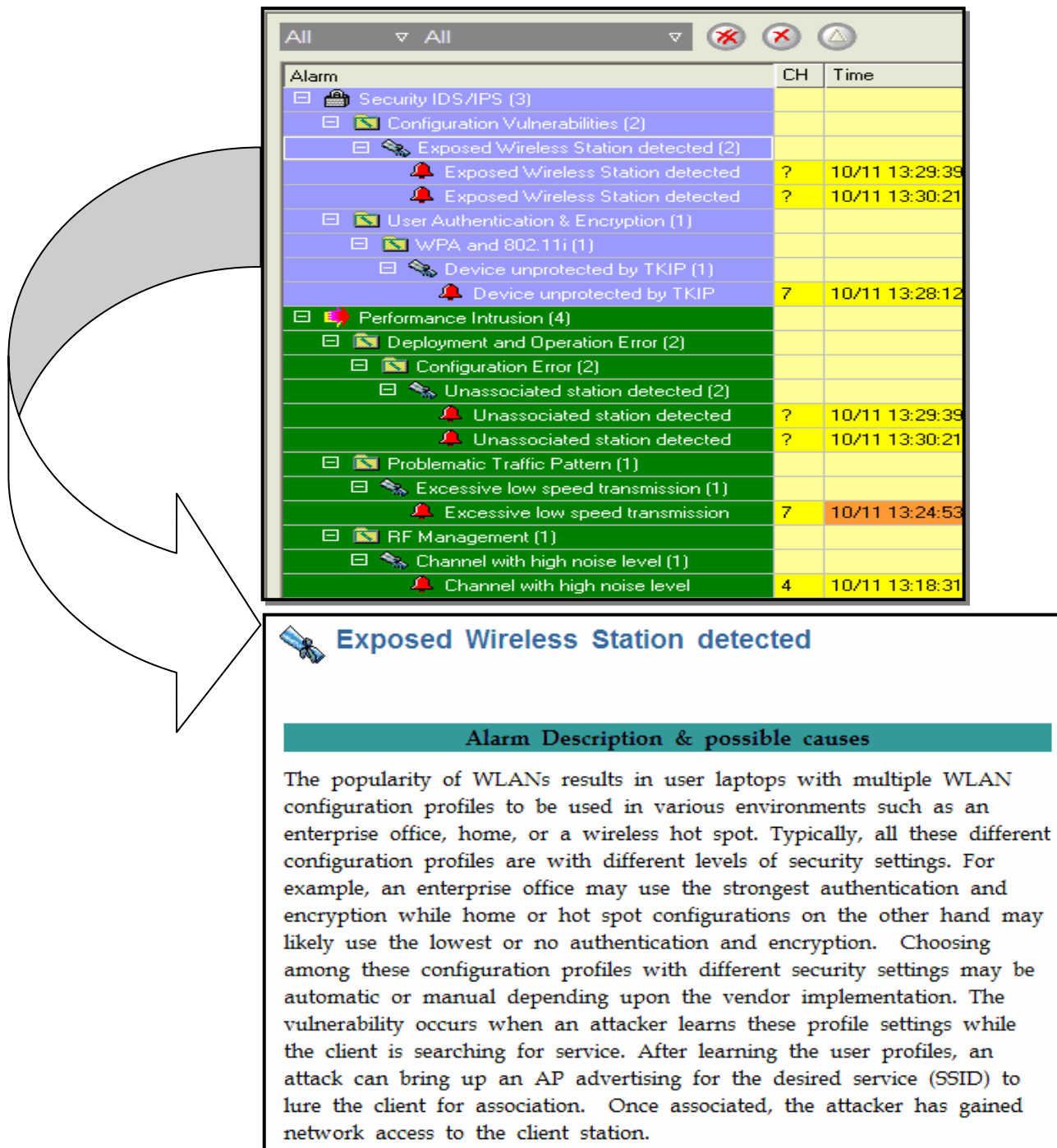
Figure 5-7 illustrates the APs that detected.

Device / MAC address	SSID
00:0E:35:72:E6:77	
00:12:79:3E:DD:2D	LoftuS
Aironet:AA:11:DE	
00:0C:F1:4F:6A:5A	Indabahotel, Smoke_Grill_Lo...
00:0E:35:58:07:D5	
00:0E:35:73:62:61	
00:0E:35:68:A8:B8	
00:0C:F1:09:B7:D3	CTech
Aironet:AA:11:DD	LoftuS2, LoftuS

Figure 5-7: APs that were detected on the sample UNISA WLAN operating environment.

LoftuS circled in the diagram indicates the SSID of the AP with a MAC address of 00:12:79:3E:DD:2D. Figure 5-8 illustrates one of the vulnerabilities relating to the wireless

client detected on the sample UNISA WLAN operating environment as well as an explanation of this particular vulnerability.



Alarm	CH	Time
Security IDS/IPS (3)		
Configuration Vulnerabilities (2)		
Exposed Wireless Station detected (2)		
Exposed Wireless Station detected	?	10/11 13:29:39
Exposed Wireless Station detected	?	10/11 13:30:21
User Authentication & Encryption (1)		
WPA and 802.11i (1)		
Device unprotected by TKIP (1)		
Device unprotected by TKIP	7	10/11 13:28:12
Performance Intrusion (4)		
Deployment and Operation Error (2)		
Configuration Error (2)		
Unassociated station detected (2)		
Unassociated station detected	?	10/11 13:29:39
Unassociated station detected	?	10/11 13:30:21
Problematic Traffic Pattern (1)		
Excessive low speed transmission (1)		
Excessive low speed transmission	7	10/11 13:24:53
RF Management (1)		
Channel with high noise level (1)		
Channel with high noise level	4	10/11 13:18:31

Exposed Wireless Station detected

Alarm Description & possible causes

The popularity of WLANs results in user laptops with multiple WLAN configuration profiles to be used in various environments such as an enterprise office, home, or a wireless hot spot. Typically, all these different configuration profiles are with different levels of security settings. For example, an enterprise office may use the strongest authentication and encryption while home or hot spot configurations on the other hand may likely use the lowest or no authentication and encryption. Choosing among these configuration profiles with different security settings may be automatic or manual depending upon the vendor implementation. The vulnerability occurs when an attacker learns these profile settings while the client is searching for service. After learning the user profiles, an attack can bring up an AP advertising for the desired service (SSID) to lure the client for association. Once associated, the attacker has gained network access to the client station.

Figure 5-8: Vulnerability detected on the sample UNISA WLAN operating environment

5.4.4 REVIEW TECHNOLOGICAL VULNERABILITIES AND SUMMARISE THE RESULTS

The vulnerability assessment generated the following report.

- ▣ Detailed information of policy violations (Security IDS/IPS and Performance Intrusion) (figure 5-9).

All Alarm Detail

Time Period: 13:30:28 Tuesday, October 11, 2005

Description: This report contains detailed information of policy violations (Security IDS/IPS and Performance Intrusion) that AirMagnet has detected in the 802.11 wireless network. An insecure network can usually be fixed by reconfiguring some of the network equipment, by using additional software or hardware and always being in the forefront of implementing the latest security standards to provide good security for sensitive data such as employee salary data or company financial information. A closely monitored and well tuned WLAN system can achieve a higher throughput than a poorly managed one. AirMagnet ensures WLAN performance and efficiency by monitoring the WLAN and alerting the wireless administrator on early warning signs for trouble. This includes reporting the devices which are vulnerable to violations/are violating and actions that can be performed to nullify such violations. With the comprehensive suite of security monitoring technologies, AirMagnet alerts the user on more than 120 different threat conditions.

Total Alarms: 7

Alarm: Device unprotected by TKIP

Category: Security	Severity: Warning	First Seen: 10/11/2005-13:18:11
MAC: 00:14:69:3B:BF:60	Channel: 7	Last Seen: 10/11/2005-13:28:12
AP: CVV-WiAP1-FI05-		

Alarm: Exposed Wireless Station detected

Category: Security	Severity: Warning	First Seen: 10/11/2005-13:18:51
MAC: 00:0C:F1:09:B7:D3	Channel:	Last Seen: 10/11/2005-13:29:39

Alarm: Exposed Wireless Station detected

Category: Security	Severity: Warning	First Seen: 10/11/2005-13:20:21
MAC: 00:0C:F1:4F:6A:5A	Channel:	Last Seen: 10/11/2005-13:30:21

Alarm: Channel with high noise level

Category: Performance	Severity: Warning	First Seen: 10/11/2005-13:18:31
MAC:	Channel: 4	Last Seen: 10/11/2005-13:18:31

Live Capture



Powered by AirMagnet

Chapter 7 - 1

Tuesday, October 11, 2005 1:30:28PM

Figure 5-9: Report on policy violations

The vulnerability scan reveals the following technological vulnerabilities detected on the wireless client, one of the most important infrastructure components identified:

- ▣ One of the wireless clients is not using TKIP for encryption. TKIP is a necessary mode of encryption protection. WLAN traffic encrypted with TKIP and MIC combats packet forgery and replay attacks. Additionally, TKIP overcomes the weakness of the static WEP key and key reuse problem.
- ▣ An exposed wireless client. Figure 5-8 explains this vulnerability.

5.5 RISK IMPACT ASSESSMENT

The objective of the risk impact assessment is to identify and analyse the risks to the mission-critical asset (infrastructure BSS) and comprises the following activities (Alberts & Dorofee, 2003:50):

5.5.1 CREATE NARRATIVE IMPACT DESCRIPTION

A narrative statement that describes how a threat affects the University for the threat outcomes (disclosure, modification, loss/destruction and interruption) is given (figures 5-10 to 5-14).

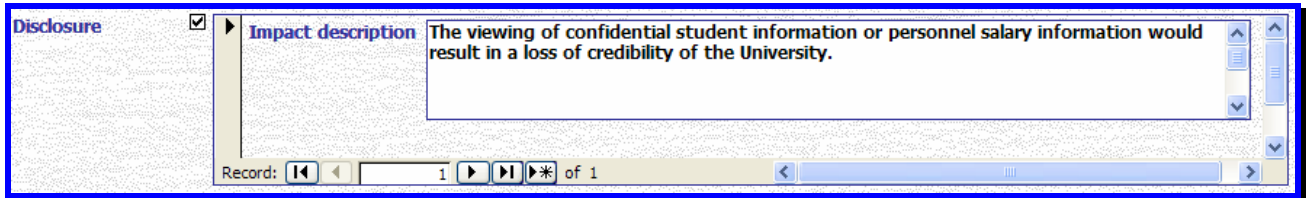


Figure 5-10: Impact description for the outcome disclosure

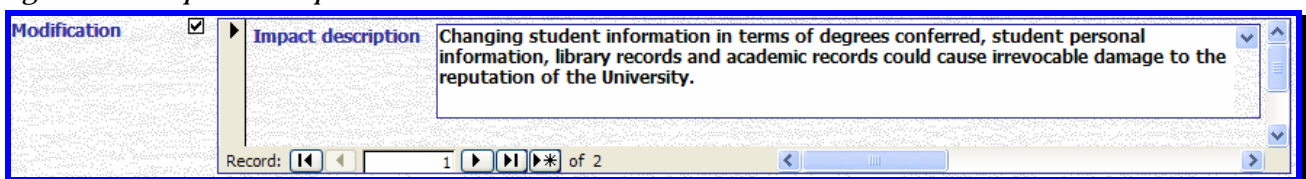


Figure 5-11: Impact description for the outcome modification

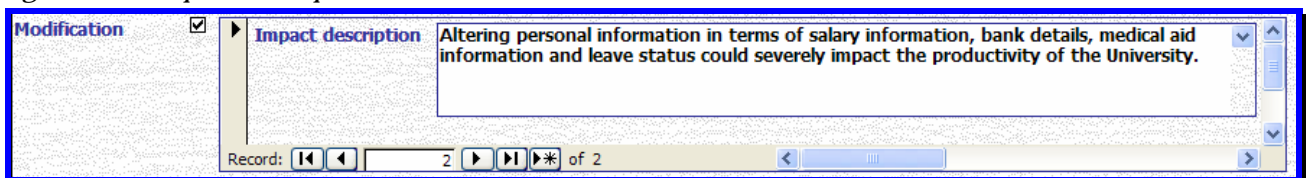


Figure 5-12: Impact description for the outcome modification

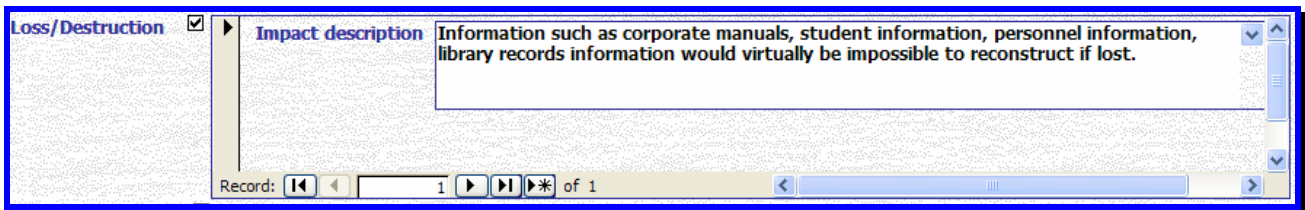


Figure 5-13: Impact description for the outcome loss/destruction

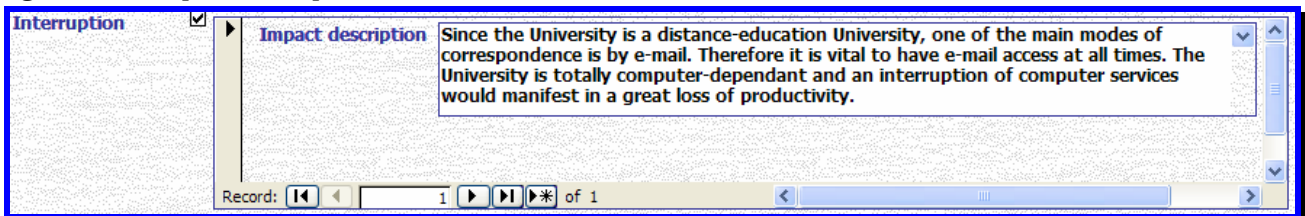


Figure 5-14: Impact description for the outcome interruption

5.5.2 CREATE RISK EVALUATION CRITERIA

An overall set of impact evaluation criteria are defined for the threats to the University's critical asset (infrastructure BSS) (figure 5-15). Definitions for three levels of qualitative evaluation, high, medium and low are defined for multiple aspects. The impact areas are all high impact areas meaning that it is absolutely crucial that the transitory information, student information, financial information, human resources information and the information products of the University be protected and preserved at all times. Any compromise thereof, will severely diminish the status of the University. There is no medium or low impact.

Area of impact	High	Medium	Low
Transitory information	The daily letters, memos, reports and e-mail communication are of great strategic value to the University.	None.	None.
Student information	Student information must be safeguarded at all times.	None.	None.
Financial information	Financial information in terms of student accounts and the salary of staff members must be kept strictly confidential and not be modified in any way.	None.	None.
Human resources informatio	Information files on personnel, contracting staff, pension, litigation, insurance and payroll must be preserved.	None.	None.
Information products	Tutorial letters, periodicals, books, computer programs (source code and object code) and the University logo that are required to be copyrighted by law cannot be tampered with in any way.	None.	None.

Figure 5-15: Risk Evaluation Criteria

5.5.3 EVALUATE THE IMPACT OF THREATS TO CRITICAL ASSETS

Each risk is reviewed and a corresponding impact measure assigned (figures 5-16 to 5-20).

Disclosure

Impact description

The viewing of confidential student information or personnel salary information would result in a loss of credibility of the University.

Impact measure

High

Record: 1 of 1

Figure 5-16: Impact value for disclosure

Modification

Impact description

Changing student information in terms of degrees conferred, student personal information, library records and academic records could cause irrevocable damage to the reputation of the University.

Impact measure

High

Record: 1 of 2

Figure 5-17: Impact value for modification

Modification <input checked="" type="checkbox"/>	<p>Impact description</p> <p>Altering personal information in terms of salary information, bank details, medical aid information and leave status could severely impact the productivity of the University.</p>	<p>Impact measure</p> <p>High</p>
Record: 2 of 2		

Figure 5-18: Impact value for modification

Loss/Destruction <input checked="" type="checkbox"/>	<p>Impact description</p> <p>Information such as corporate manuals, student information, personnel information, library records information would virtually be impossible to reconstruct if lost.</p>	<p>Impact measure</p> <p>High</p>
Record: 1 of 1		

Figure 5-19: Impact value for loss/destruction

Interruption <input checked="" type="checkbox"/>	<p>Impact description</p> <p>Since the University is a distance-education University, one of the main modes of correspondence is by e-mail. Therefore it is vital to have e-mail access at all times. The University is totally computer-dependant and an interruption of computer services would manifest in a great loss of productivity.</p>	<p>Impact measure</p> <p>High</p>
Record: 1 of 1		

Figure 5-20: Impact value for interruption

5.5.4 CREATE RISK PROFILE

Impact measures affixed to the asset-based threat profile trees result in the creation of an asset-based risk profile (figure 5-21).

Asset Name: Infrastructure BSS		Type of threat: Human actors using wireless access	
Record: 1 of 1			
Outcomes Disclosure <input checked="" type="checkbox"/> Modification <input checked="" type="checkbox"/> Loss/Destruction <input checked="" type="checkbox"/> Interruption <input checked="" type="checkbox"/>	Actor Insider <input type="checkbox"/> Outsider <input type="checkbox"/> Motive Accidental <input type="checkbox"/> Deliberate <input type="checkbox"/>		Impact High
	Record: 1 of 1		Record: High
	Actor Insider <input type="checkbox"/> Outsider <input type="checkbox"/> Motive Accidental <input type="checkbox"/> Deliberate <input type="checkbox"/>		High
	Record: 1 of 1		Record: High
Actor Insider <input type="checkbox"/> Outsider <input type="checkbox"/> Motive Accidental <input type="checkbox"/> Deliberate <input type="checkbox"/>		High	
Record: 1 of 1		Record: High	
Actor Insider <input type="checkbox"/> Outsider <input type="checkbox"/> Motive Accidental <input type="checkbox"/> Deliberate <input type="checkbox"/>		High	
Record: 1 of 1		Record: High	

Figure 5-21: Asset-based risk profile

5.6 CONCLUSION

All the analysis activities provide the University with a sense of knowledge regarding its unique WLAN intrusion security risks (situation awareness). The concluding process, decision: protection strategy and risk mitigation plan enables the organisation to address these risks in practice and develop a WLAN enterprise-wide protection strategy and WLAN intrusion security risk mitigation plan for the University. This is the focus of the subsequent chapter.



CHAPTER

6. DECISION: PROTECTION STRATEGY AND RISK MITIGATION PLAN

6.1 INTRODUCTION

The open nature of WLANs makes them a perfect target for itinerant hackers to execute intrusion attacks. The lack of protection rendered by recognised security countermeasures (Zhang et al., 2003:545) further aggravates this problem. However, if properly designed, certain countermeasures can detect an intrusion attack.

The desirable outcome of this exercise is the development of a WLAN enterprise-wide protection strategy and the recommendation of an appropriate risk mitigation plan capable of reducing WLANs intrusion security risks to an acceptable level.

6.2 STRUCTURE OF THIS CHAPTER

This chapter centres on the culmination of the WLAN intrusion security risk analysis process on the basis by which the organisation decides on what security measures to enforce. This therefore conforms to the decision: protection strategy and risk mitigation plan of the WLAN intrusion security risk analysis process.

The following diagram (figure 6-1) depicts the role of this chapter within the overall context of the dissertation.

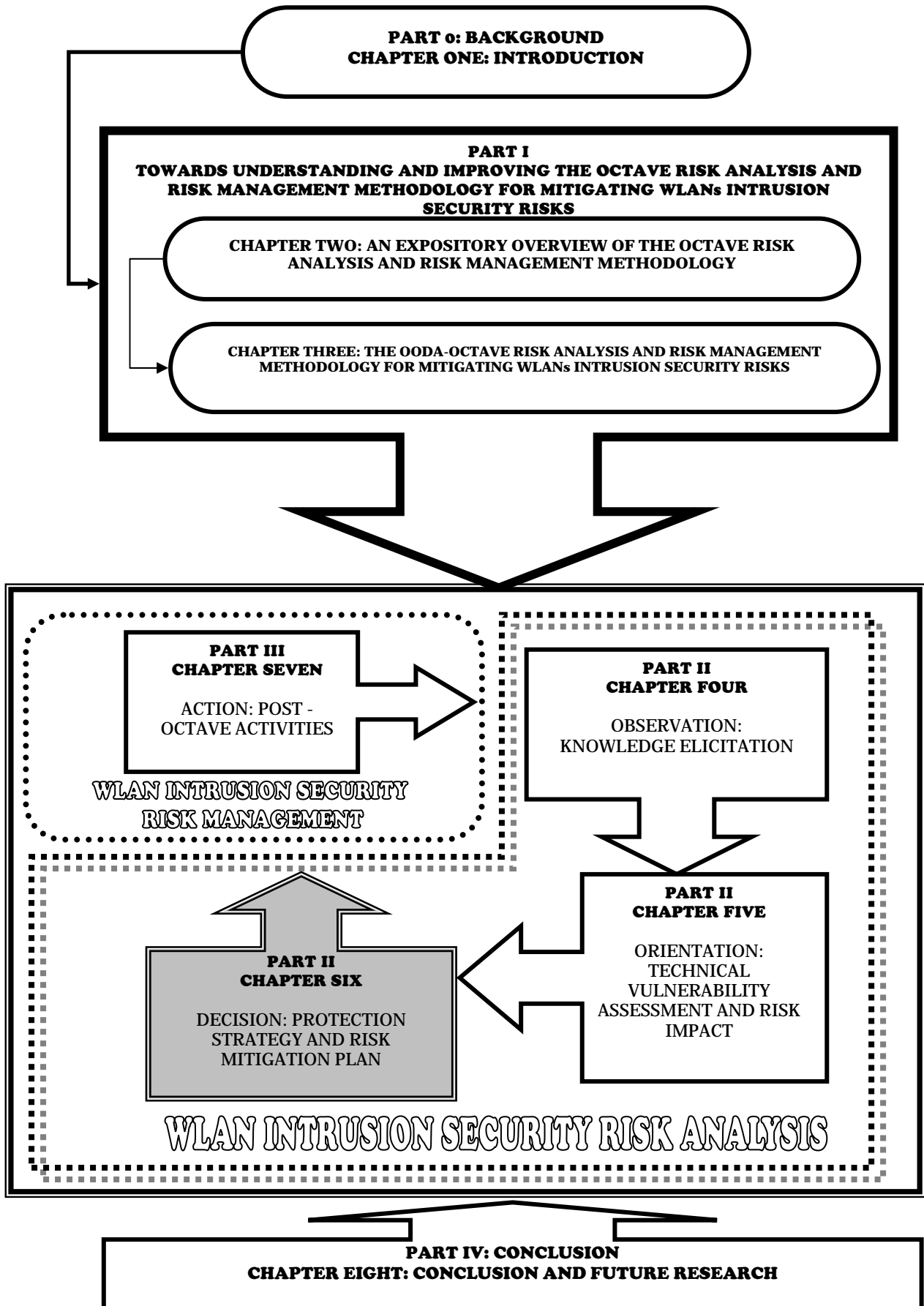


Figure 6-1: The role of chapter six within the overall context of the dissertation

6.3 WLAN ENTERPRISE-WIDE PROTECTION STRATEGY AND RISK MITIGATION PLAN

The risk impact criteria all connote a high degree impact (figure 5-21), signalling the importance of developing a WLAN enterprise-wide protection strategy and WLAN intrusion security risk mitigation plan. *Risk mitigation* planning involves the actions and activities performed prior to a risk, either to prevent a risk from occurring altogether or to reduce the impact or consequences of its occurrence to an acceptable level ("Microsoft Operations", 2004:31).

6.3.1 CREATION OF A WLAN ENTERPRISE-WIDE PROTECTION STRATEGY

This activity entails the development of a long-term WLAN protection strategy for enterprise-wide improvement for the University. This strategy is structured against the backdrop of the catalogue of practices. The WLAN enterprise-wide protection strategy appears in appendix D.

6.3.2 CREATION OF A WLAN RISK MITIGATION PLAN

The focus of this activity is a more tactical view to reduce intrusion security risks to the University's most crucial asset (infrastructure BSS) by means of action plans or countermeasures (Alberts & Dorofee, 2003:208).

One particular countermeasure, a wireless intrusion detection system (*wireless IDS*), is particularly apt at shielding a network against intruders (Kachirski & Guha, 2002:153) and should be included as a fundamental security countermeasure in the organisation's WLAN computing infrastructure. The following in-depth section provides a justification for the deployment and consolidation of a wireless IDS in the University's WLAN computing infrastructure.

6.4 JUSTIFICATION OF A WIRELESS IDS FOR MITIGATING WLANS INTRUSION SECURITY RISKS

The rapid adoption of WLANs has dramatically changed the entire outlook of network security rendering these networks more vulnerable to "malicious attacks" (Yang^c et al., 2004:1949). There is an immediate need for a mechanism to protect WLANs from intrusion attacks. The most widespread and common vulnerabilities of WLANs were explored and it was demonstrated that the exploitation of these vulnerabilities can

manifest in real risks that can affect the confidentiality, integrity and availability of information. It can, therefore be argued that a wireless IDS should form a salient component as a "second wall of defense" (Zhang et al., 2003:546; Yang^b, Hu & Chen, 2004:150) or an additional layer of protection (Adelstein et al., 2004:482) in the WLAN computing infrastructure.

It should be emphasised that a wireless IDS is only "part of the security puzzle" (Potter, 2004:5) and should not function in solitude as the only mode of protection (McHugh, Christie & Allen, 2000:42). At present, innumerable security technologies such as "firewalls, encryption technology, authentication devices, vulnerability checking tools" (Goan, 1999:46), are capable of counteracting various security breaches. Security measures such as encryption technology and authentication devices which usually form the first layer of defense (Zhang et al., 2003:546) in WLAN security have already been discussed in the observation: knowledge elicitation phase (chapter 4).

Additional security countermeasures may include a virtual private network (VPN) and a firewall. A *VPN* uses encryption to create a tunnel, a secure means of communication across an untrusted network such as the Internet between the user's device and the destination (McCullough, 2004:65; Park & Dicoi, 2003:64). A *firewall* is any device used to impede or selectively allow network traffic (Carter & Shumway, 2002:53). Ideally, a firewall should be placed near the AP between the fixed-wired network and the wireless network (Miller, 2003:224).

The following section provides an overview of wireless intrusion detection systems stemming from the historical emanation of these systems.

6.4.1 BACKGROUND: A SYNOPSIS OF INTRUSION DETECTION SYSTEMS (IDSs)

IDSs can be classified as the tools and methods that monitor computer systems and network traffic to identify and report possible hostile attacks originating from outside the organisation and also for system misuse or attacks originating from within the organisation (Iheagwara, 2004:213; Endorf, Schultz & Mellander, 2004:4).

The genesis of intrusion detection dates from 1980 commencing with James Anderson's (Anderson, 1980) technical report, Computer Security Threat Monitoring and Surveillance

for the U.S. Air Force. In 1985, Stanford Research Institute (SRI) was funded by the U.S. Navy to build the initial type of Intrusion Detection Expert System (IDES). Dr. Dorothy Denning assisted in leading this team and a year later published a paper entitled, An Intrusion Detection Model (Denning, 1986) for the 1986 IEEE Symposium on Security and Privacy. This paper is regarded as being the seminal work on intrusion detection.

Conceptually a wireless IDS is similar to wired IDS (Yang^c et al., 2004:1949) but marked differences between wireless and wired-line networks, particularly the "structural and behavioural differences" (Kachirski & Guha, 2002:154) render current IDS designs unsuitable for wireless networks. Wired intrusion detection systems operate at layer 3 (IP layer) and above of the OSI model ("Wireless LANs:Defending", 2004:2) whereas WLANs generally refer to the Physical and Data Link layers of the OSI model. A wireless IDS must therefore function at the Data Link layer or even possibly the Physical layer if optimal security is required (Lim & Schmoyer, 2003:68).

The following section provides an overview of the functions that a wireless IDS must possess.

6.4.2 FUNCTIONS OF A WIRELESS IDS SYSTEM



The functionality that a wired-line IDS must possess can well be extended to a wireless IDS. Therefore, a wireless IDS must be capable of (Yang^c et al., 2004:1949, Bace^a, 2002:11):

- Monitoring and analysing both user and system activities.
- Recognising patterns of known attack.
- Identifying abnormal network activity.
- Detecting policy violations.
- Providing an audit trail to ascertain how far the intruder got and the origin of the attack.
- Assessing the integrity of crucial system and data files.
- Auditing system configurations and vulnerabilities.

The next section provides an overview of the operational design of a wireless IDS.

6.5 OPERATIONAL DESIGN OF A WIRELESS IDS

To study the operational design of a wireless IDS, it is necessary to exploit the literature in order to uncover what has generally been included in this area as well as study a few notable wireless IDSs. The aim of this exercise is to propose the inclusion of a wireless IDS in the University's WLAN computing infrastructure by demonstrating the effectiveness of this system. At present a large number of commercial and open-source wireless IDSs are available, including AirDefense ("Enterprise Wireless Intrusion", 2001-2005), AirMagnet ("Enterprise Wireless", n.d.), Network Chemistry ("Network Chemistry-The", 2005), AirTight Networks ("AirTight Networks,", 2005), Highwall Technologies ("Highwall Technologies", 2005), Red-M ("Red-M-Home", 2005), Snort-Wireless (Lockhart, 2003-2005) and WIDZ ("Loud-Fat-Blokes-World-Of-Weird", n.d.).

Of these systems, two notable commercial wireless intrusion detection system (IDSs)/intrusion prevention systems (IPSs),  AirDefense Enterprise and  AirMagnet Enterprise were considered as these systems have been labelled the "industry veterans" (Bulk, 2005:2) and an "interesting pair of competitors" (Turvey, 2005:2). These systems are wireless IDSs/IPSs meaning they are able to detect and prevent intrusion attacks. The detection part of the wireless IDS/IPS is reactive in nature, in a sense that corrective action can only take place after a breach of security. The prevention part entails a "programmatic approach to vulnerability assessment to identify any potential weaknesses in the security deployment before they can be exploited ("AirMagnet Enterprise", 2005:ii).

Open-source wireless IDS systems such as Snort-Wireless were also investigated as Snort is one of the most widely deployed IDS available today (Potter, 2004:5). Snort-Wireless is currently capable of detecting rogue APs, ad hoc networks, DOS attacks, MAC spoofing and Netstumpers (Lockhart, 2003-2005). The reason why Snort-Wireless was considered is that it is a viable solution since it is an open-source wireless IDS. However, the researcher concluded that this tool would not be suitable for the University WLAN operating environment because the operational and deployment requirements of Snort would require a great deal of investment in time and expert human resources. If these systems are not succinctly pre-configured to look exactly for what they should, they will fail to function optimally.

AirMagnet Enterprise and AirDefense Enterprise have a very similar architectural design, hence they have been labelled as being an "interesting pair of competitors". The operational design of the wireless IDS/IPS, is examined by virtue of studying AirMagnet Enterprise 6.0, since it was the overall category winner for the Best Wireless Security ("SC Magazine", 2006). However, features of AirDefense that are lacking or better than those in AirMagnet are discussed. The aim of this exercise is to illustrate the effectiveness of a wireless IDS to senior management.

The operational design of a wireless IDS/IPS using AirMagnet Enterprise 6.0 is examined within the framework of the OODA cycle since the design of this system is dynamic, constantly requiring refinements and updating for a non-static environment.

6.5.1 OBSERVATION

A wireless IDS observes functions by using information sources such as IDS sensors. There are two types of sensors, network-based sensors and host-based sensors (Endorf et al., 2004:19, Kachirski & Guha, 2002:154).

- ▣ Network-based sensors can monitor traffic as it flows through a network to other hosts on the network (Koziol, 2003:2). In the AirMagnet Enterprise System, the AirMagnet SmartEdge sensors, which are network-based sensors capture and analyse wireless packets. These SmartEdge sensors can typically be AirMagnet handheld devices or laptop devices. The AirMagnet console governs the user interface to the SmartEdge sensors by providing an insightful interface. The following diagram (figure 6-2), illustrates a SmartEdge sensor observing the sample UNISA WLAN operating environment.

The consensus is to deploy sensors (network-based sensors) wherever an AP is located (Carter & Shumway, 2002:72, Poblete, 2005). This has a number of advantages (Yang^c et al., 2004:1950):

- ▣ By covering the APs with a blanket of sensors, attacks and misuse can be detected.
- ▣ It is possible to ascertain the location of the intruder physically.

For the AirMagnet Enterprise System, the general rule is to deploy one sensor for every 6 APs ("Enterprise Quick", 2005). AirMagnet can support approximately 1 500 sensors with a single server ("Enterprise-hardened", 2005). Since the University already has a Cisco

Aironet 1200 AP (section 4.4.4.2), this AP can be used as a sensor to provide information to the enterprise server (Turvey, 2005:3). This can significantly reduce costs, precluding the need to invest in a dedicated sensor.

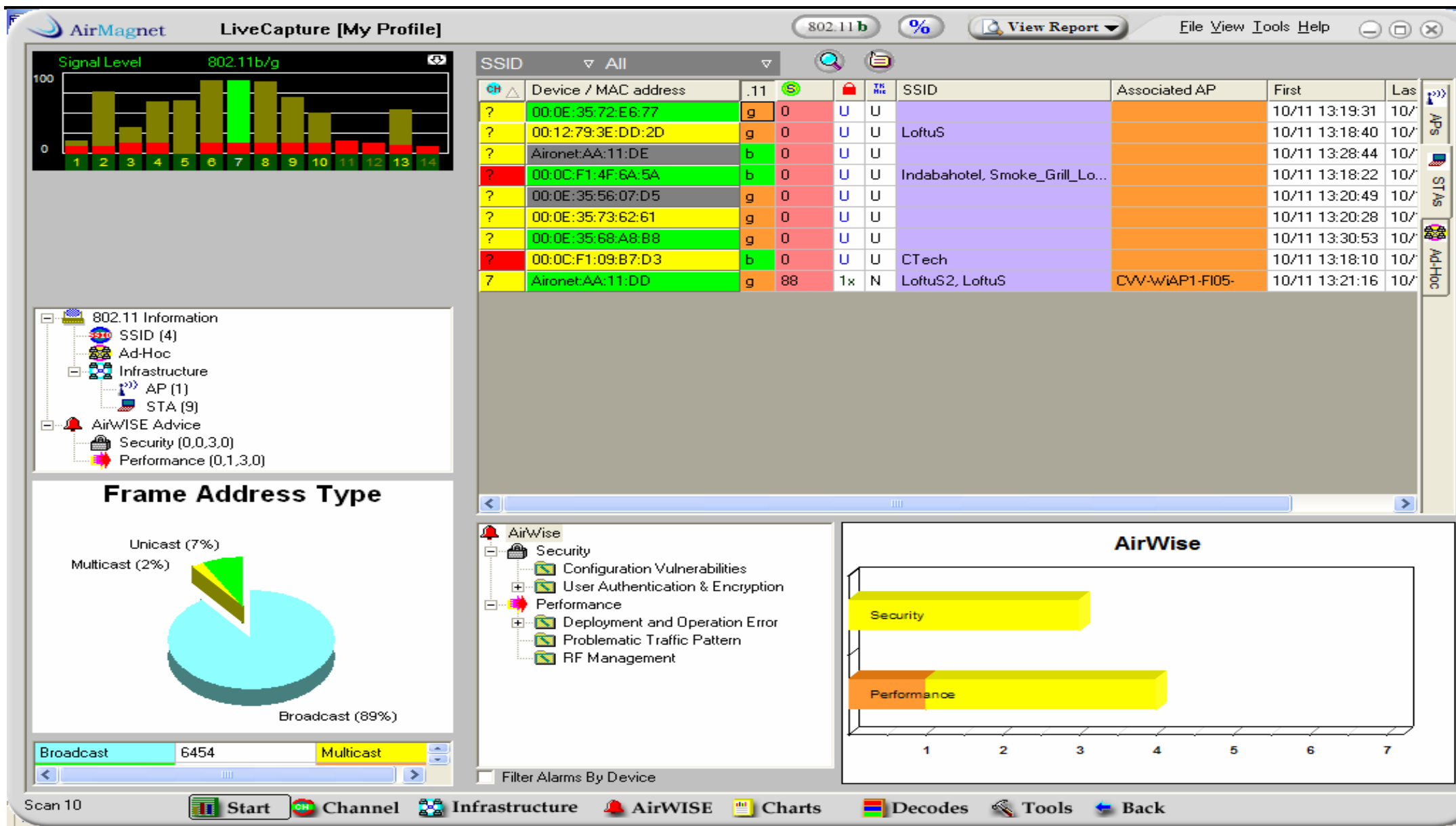


Figure 6-2: SmartEdge sensor monitoring the sample UNISA WLAN operating environment

- Host-based sensors operate on a single protected host and inspect audit or log data for any activity deemed intrusive (McHugh et al., 2000:45). AirDefense Personal



, is a host-based sensor designed for complete wireless end-point security (WEPS) that may work as stand-alone host-based sensor or in concert with the AirDefense Enterprise 7.0 server to prevent wireless security vulnerabilities from affecting wireless clients. The AirDefense Personal agent constantly monitors the activity and configuration of the wireless client to prevent policy violations or malicious attacks such as *redirection attacks*, *man-in-the-middle attacks*, *deauthentication attacks* and secures the network from probing laptop problems ("Wireless Protection", 2002-2005:4). Figure 6-3 illustrates AirDefense personal running on a wireless client in the sample UNISA WLAN operating environment. It is also possible to enforce a wireless policy by using AirDefense Personal (figure 6-4).



Users are warned of the attack and AirDefense Personal takes the necessary action to halt the attack before it is successful.

In the stand-alone mode users can enforce individual policies. AirDefense Personal agents can also report to the Enterprise 7.0 server for centralised management of security events and the enforcement of new or updated agent policies (figure 6-5) ("AirDefense Enterprise 6.0", 2005).

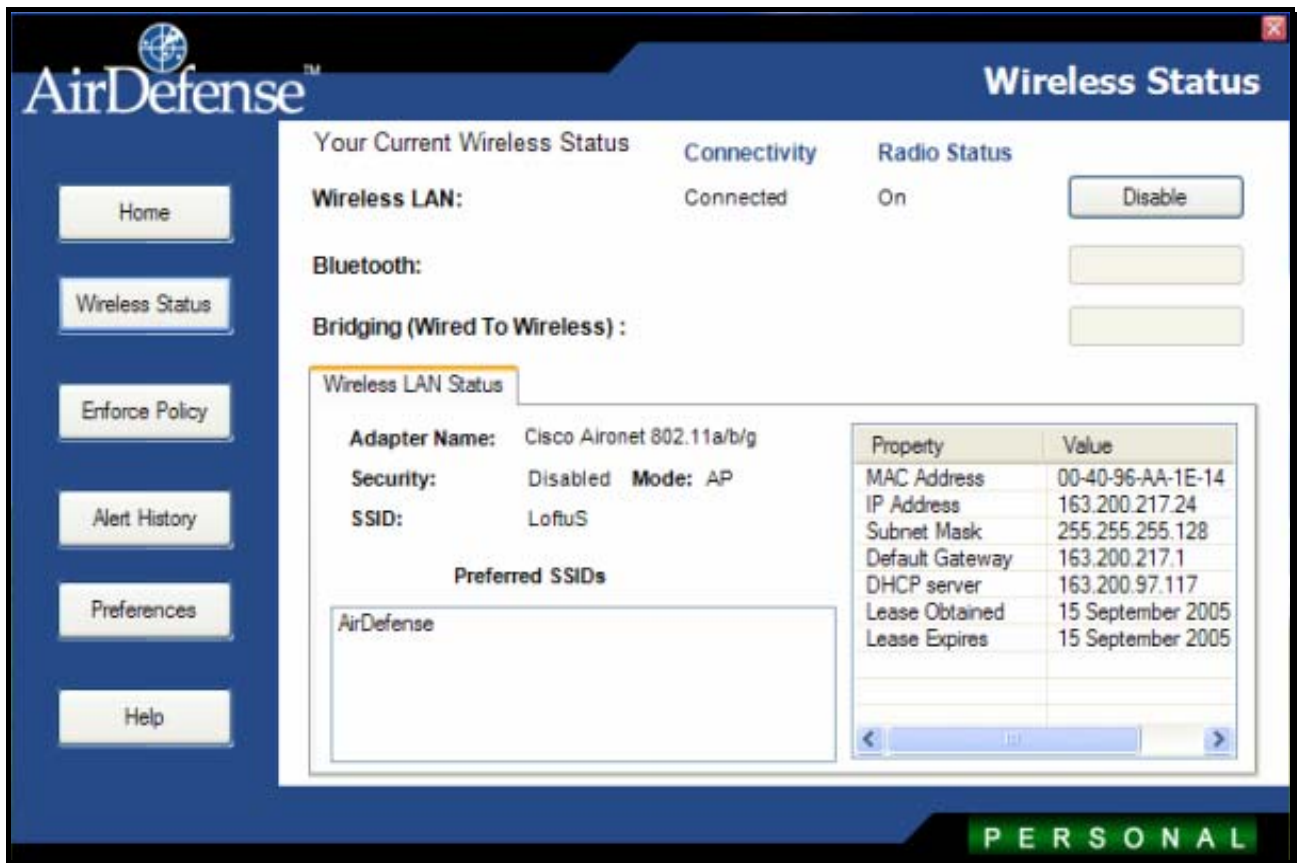


Figure 6-3: AirDefense personal on the sample UNISA WLAN operating environment

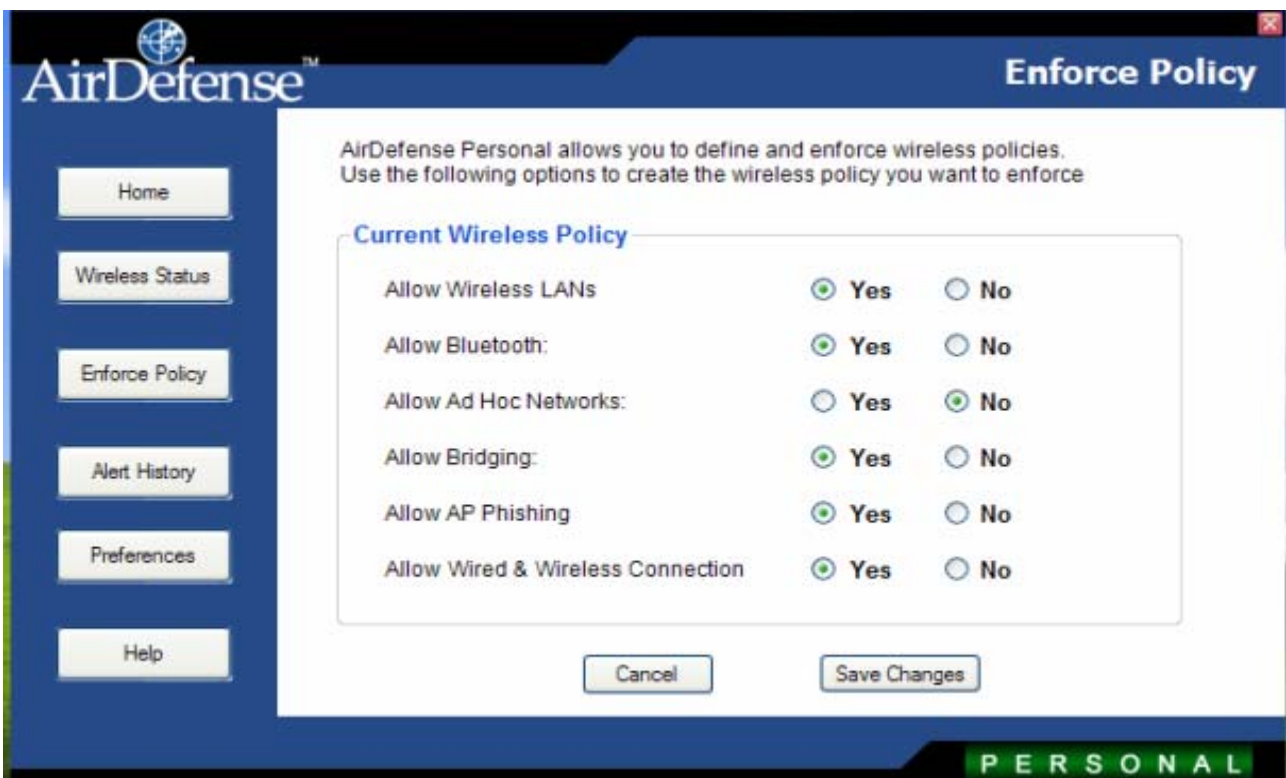


Figure 6-4: Using AirDefense personal to enforce a policy

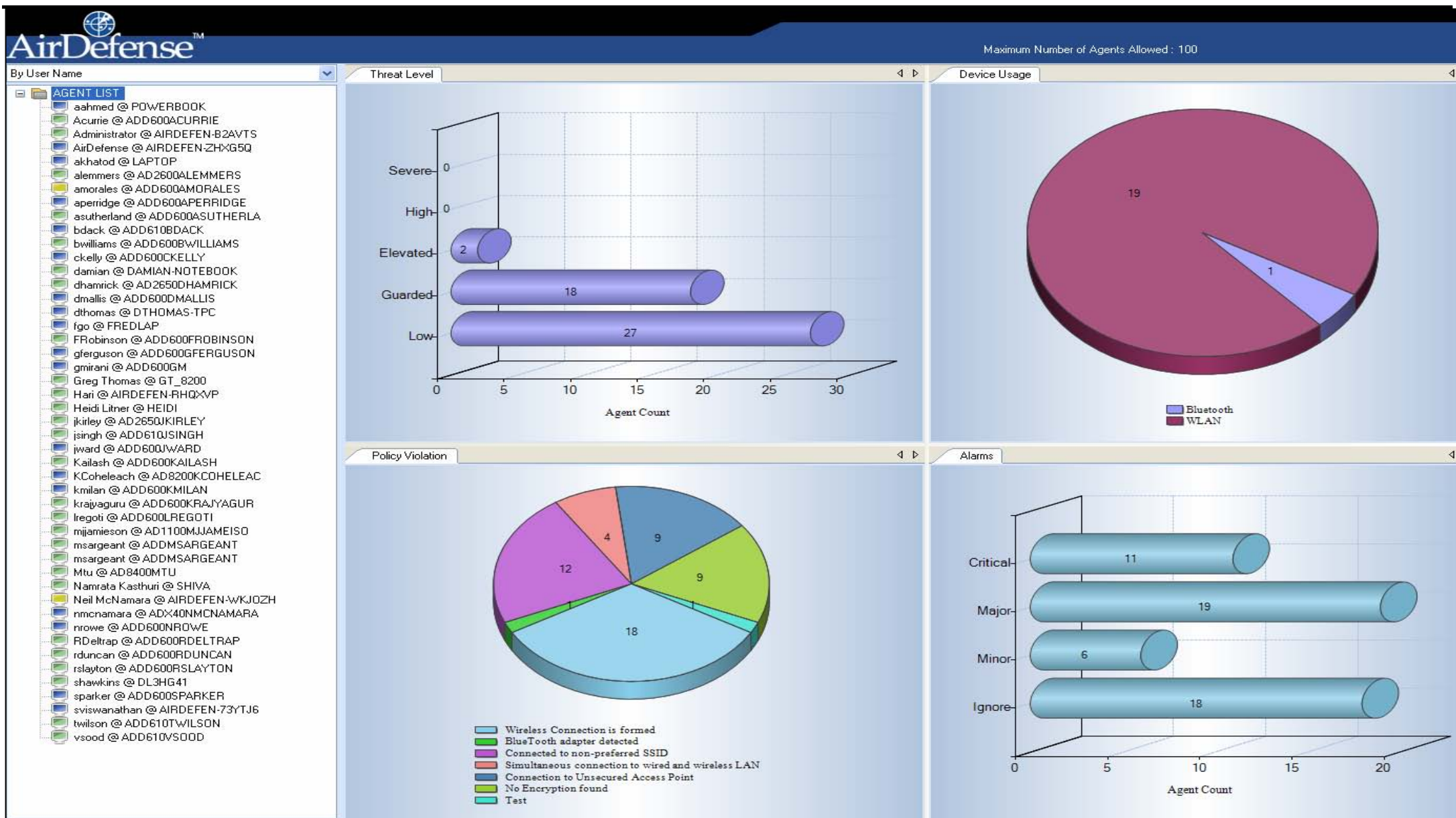


Figure 6-5: Managing multiple AirDefense personal agents using the personal manager

6.5.2 ORIENTATION

Analysis of the wireless packets takes place in the orientation phase. Intrusion detection techniques are broadly classified as misuse detection and anomaly detection (Zhang et al., 2003:546):

- ▣ Anomaly detection techniques have been applied to the problem of detecting intrusion since the research field of intrusion detection was first formalised with the publication of Anderson's seminal report in 1980 (Anderson, 1980). Anomaly detection builds profiles of normal user and system behaviour and any activity that deviates drastically from this accepted normal usage profile is labelled intrusive (Campbell, 2003:337) Anomaly detection modules can be constructed by enabling a logging system and studying the log files to note deviations in certain behaviour (Sharma, 2004:118). AirMagnet enterprise can study these patterns and generate an alarm upon detection of a specific abnormality ("AirMagnet Enterprise 6.0", 2005:84).
- ▣ Signature detection, also referred to as rules-based detection, pattern matching and misuse detection uses pattern matching to detect known attack patterns (Endorf et al., 2004:16). Signature detection entails recording unique activity patterns into a signature. The user's activity is compared with this signature. Pending a match, an alert indicates that an intrusion has taken place.

The SmartEdge sensors capture 802.11 packets using the 802.11b, 802.11g or 802.11a band ("AirMagnet Enterprise 6.0 User", 2005:66) and can perform a total local analysis of the packets without having to send them through to the centralised server. The sensor is able to identify more than 120 classes of threats and a large number of specific attack tools ("Enterprise-hardened", 2005) in real time. At the crux of this solution is the industry's most advanced analysis engine, called AirWISE. AirWISE automatically analyses any wireless network to identify security and performance threats proactively. AirMagnet's AirWISE engine (zero-day analysis) provides alerts on devices that are repeatedly committing security and performance violations.

The SmartEdge sensors are capable of conducting a continuous vulnerability assessment of the network (figures 5-7 to 5-9). The continuous scanning means that it is not necessary to enlist the assistance of a large number of personnel to survey the area frequently (Lindstrom, 2003:3) which may very well be a large geographically dispersed area in the case of an enterprise WLAN (Henning, 2003:56). Owing to the open nature of wireless

networks, new vulnerabilities can come into being as soon as the vulnerability analysis has been done rendering this labour and capital exercise (Chartoff & Boyland, 2004:41) an exercise in futility ("Wireless LANs:Risks", 2003:9).

The following section provides an overview on how AirMagnet's intelligent SmartEdge sensors are able to detect some of the possible type of intrusion attacks identified in the observation: knowledge elicitation phase (figures 6-6 to 6-9) ("AirMagnet Handheld", n.d.).

6.5.2.1 AIRMAGNET SMARTEDGE SENSORS DETECTION OF WLAN INTRUSION ATTACKS AND POLICY VIOLATION



Figure 6-6: Unauthorised AP detected

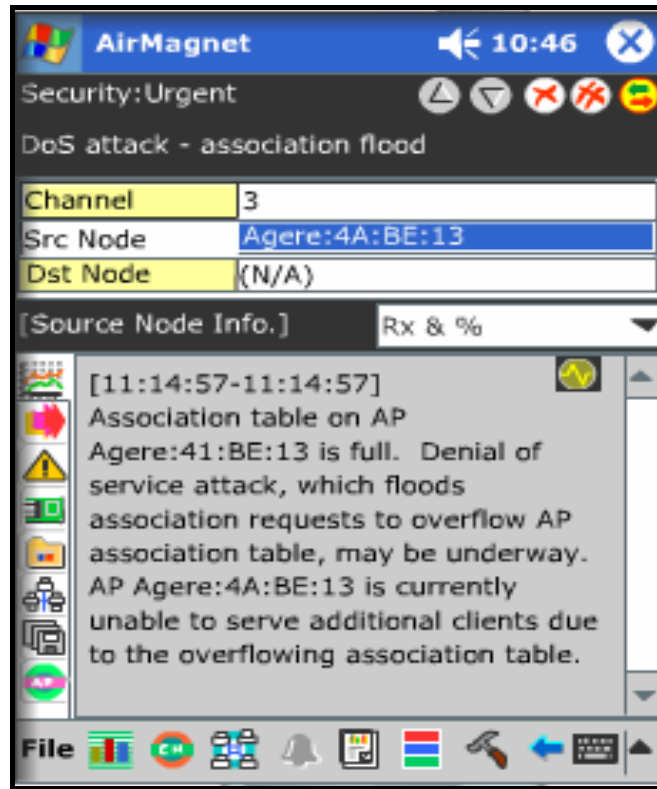


Figure 6-7: DOS (flood association request) attack detected

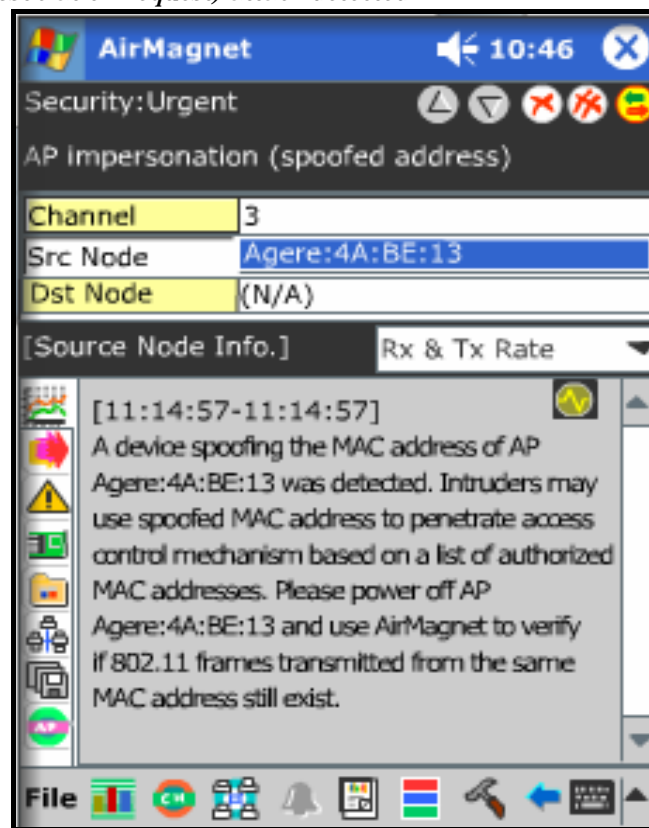


Figure 6-8: MAC address masquerading detected

Figure 6-9 illustrates how SmartEdge sensors are capable of detecting a policy violation; unconfigured AP. AirMagnet SmartEdge sensors scan the WLAN for unconfigured APs by matching factory default settings against an internal database of well-known default configurations such as default configurations for the SSID ("AirMagnet Enterprise 6.0", 2005:15).

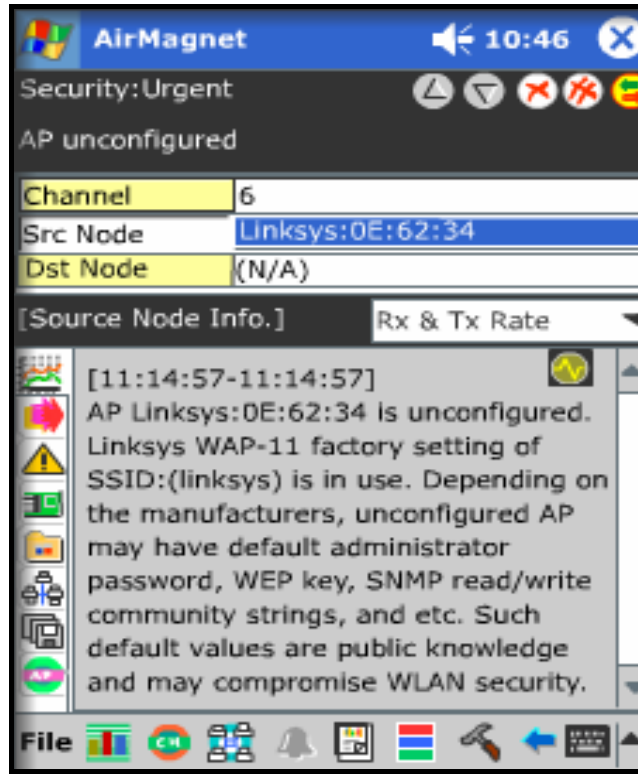


Figure 6-9: Unconfigured AP detected

It is possible to customise the SmartEdge sensors policy management to detect a range of intrusion attacks, configuration vulnerabilities and user authentication and encryption configurations (figure 6-10).




Figure 6-10: SmartEdge sensors policy management

The SmartEdge sensors are capable of detecting configuration vulnerabilities such as ad-hoc stations, APs broadcasting their SSIDs, an AP with a configuration that has changed and APs using default configuration. A comprehensive explanation of these vulnerabilities is provided. Figure 6-11 illustrates some of the configuration vulnerabilities detected by the researcher when doing a sample scan of an area in Centurion, South Africa on 10th October 2005 together with an explanation of one of these vulnerabilities (figure 6-12).

Alarm	CH	Time	Source Device
Security IDS/IPS (34)			
Configuration Vulnerabilities (17)			
AP broadcasting SSID (8)			
AP broadcasting SSID	6	10/6 15:52:51	GemTek:63:43:
AP broadcasting SSID	1	10/6 15:53:59	00:0F:EA:8E:9F
AP broadcasting SSID	6	10/6 15:55:01	GemTek:75:11:
AP broadcasting SSID	6	10/6 15:56:09	00:11:95:C2:89:
AP broadcasting SSID	11	10/6 15:56:09	00:02:6F:09:D9
AP broadcasting SSID	11	10/6 15:58:20	00:0F:B5:0E:DF
AP broadcasting SSID	11	10/6 15:58:20	00:0F:B5:0E:E1
AP broadcasting SSID	10	10/6 16:00:30	00:E0:98:51:2B
AP configuration changed (1)			
AP configuration changed	?	10/6 15:36:22	00:0F:B5:0E:DF
AP operating in bridged mode detected (4)			
AP operating in bridged mode detected	11	10/6 15:36:08	00:0F:B5:0E:E1
AP operating in bridged mode detected	11	10/6 15:36:22	00:0F:B5:0E:DF
AP operating in bridged mode detected	6	10/6 15:41:44	GemTek:63:43:
AP operating in bridged mode detected	6	10/6 15:43:16	GemTek:75:11:
Ad-hoc station detected (3)			
Ad-hoc station detected	?	10/6 15:36:58	00:02:6F:39:D6
Ad-hoc station detected	?	10/6 15:41:41	00:00:9D:21:21
Ad-hoc station detected	?	10/6 15:41:41	00:00:9D:24:E3
Exposed Wireless Station detected (1)			
Exposed Wireless Station detected	?	10/6 15:57:11	00:0C:F1:09:87
User Authentication & Encryption (17)			
Static WEP encryption (15)			
AP with encryption disabled (10)			
AP with encryption disabled	11	10/6 15:35:34	00:0F:B5:0E:E1
AP with encryption disabled	11	10/6 15:35:47	00:0F:B5:0E:DF

Figure 6-11: Configuration vulnerabilities detected

 **AP broadcasting SSID**

AP GemTek:63:43:B5 (SSID : Zenex) is currently broadcasting its SSID (Zenex) in clear text. For security reasons, it is generally recommended that the SSID broadcast be turned off in the AP configuration. For Cisco Aironet AP, this configuration is called "Broadcast SSID in beacon." Even though turning off SSID broadcast does not secure your WLAN by any definition, it does prevent your AP from being discovered by war-driving tools such as NetStumbler. Turning off SSID broadcast also blocks out casual WLAN hackers who do not have sophisticated tools and knowledge. Please note that AirMagnet can discover un-broadcasted SSID and APs.

Figure 6-12: Explanation of one of the configuration vulnerabilities

It is possible to create new policy profiles without using any of AirMagnet's pre-configured policy profiles ("AirMagnet Enterprise 6.0 User", 2005:215). Thus it will be possible to create a new policy or edit an existing policy to take into account the operational policies outlined in appendix D (section 12.2).

The AirMagnet SmartEdge sensors can detect an intruding device using the AirMagnet find tool located on the laptop analyser (figure 6-13).

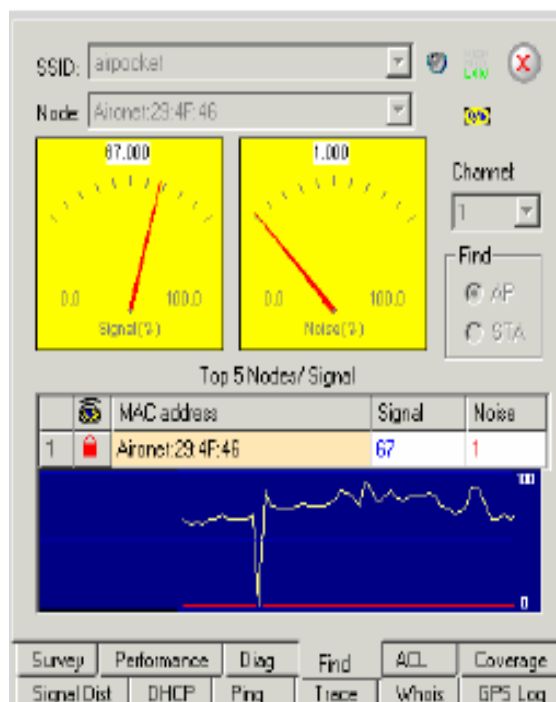


Figure 6-13: AirMagnet find tool locating an intruding device

All events, such as traffic statistics, identified APs and wireless clients, performance and security anomalies are periodically passed from the AirMagnet SmartEdge sensors to a centralised enterprise server ("AirMagnet SmartEdge", 2005:5). Communications between all AirMagnet components use SSL/TLS, ensuring all traffic is secure and VPN/firewall friendly ("Enterprise Quick", 2005). If the LAN or WAN link between the sensor and the centralised enterprise server goes down, AirMagnet is able to retrieve all the alarms and events that occurred during this missed period (Bulk, 2005:5). The centralised enterprise server integrates with other systems and does correlation, reporting, notification and alerting of all the WLAN events from the different sensors.

In the AirDefense Wireless IDS/IPS, the centralised server correlates events and statistics from all the sensors and agents. The centralised server runs a multi-dimensional engine

(figure 6-14) that amalgamates several detection technologies. The server is responsible for centrally managing and monitoring the policies.

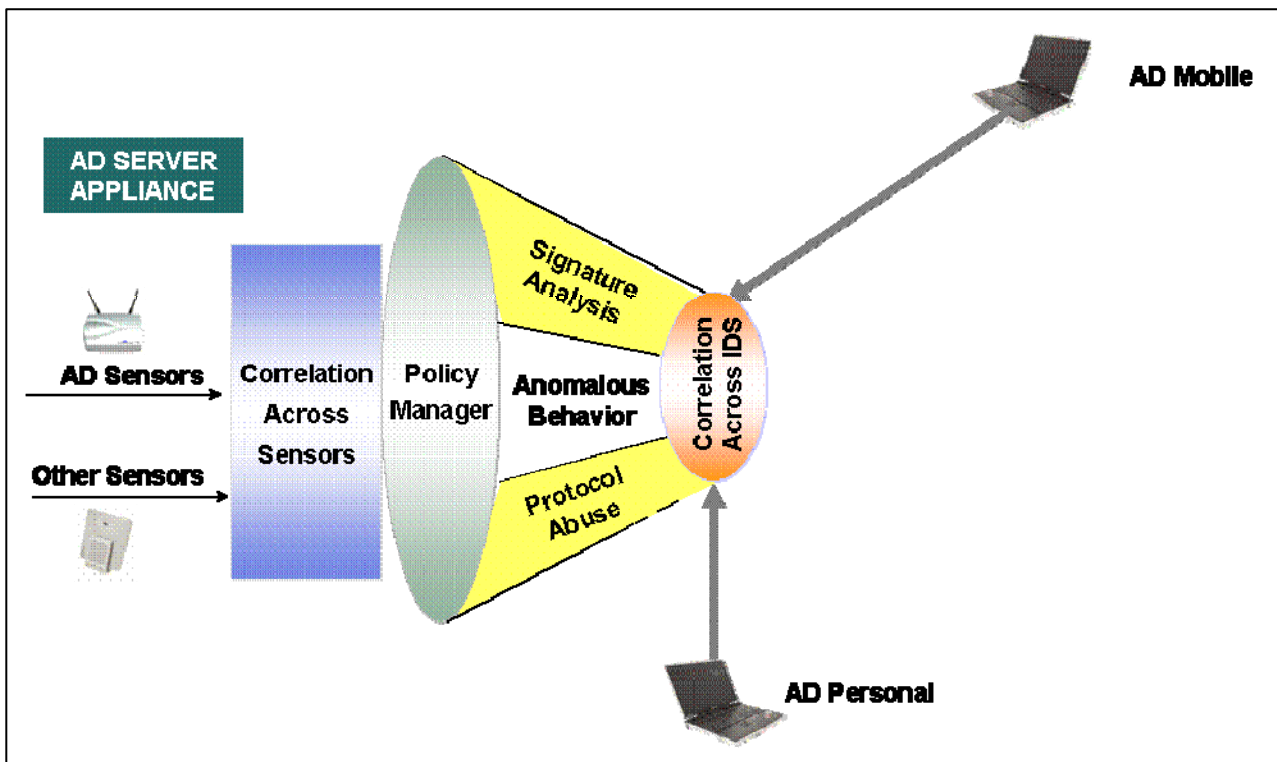


Figure 6-14: AirDefense multidimensional correlation engine

The following section provides an overview of how the centralised enterprise server is able to detect and prevent some of the possible types of intrusion attacks and policy violations identified in the observation: knowledge elicitation phase. The SmartEdge sensors are also capable of detecting some of these attacks.

6.5.2.2 AIRMAGNET CENTRALISED ENTERPRISE DETECTION OF WLAN INTRUSION ATTACKS AND POLICY VIOLATIONS

- ▣ The centralised enterprise server, governed by the AirMagnet Enterprise Console provides detailed information on the security and performance events that have occurred in the last 24 hours, plus full custom reporting for any time period (figure 6-15) ("Enterprise Quick", 2005:8). The AirMagnet Enterprise Console allows users to view network activities by location or sensor throughout the network. When more detailed information is required, the Enterprise Console can directly connect to any individual sensor for real-time analysis and remote troubleshooting, using the AirMagnet Remote Analyser. The remote analyser can be launched by double-clicking a particular sensor.

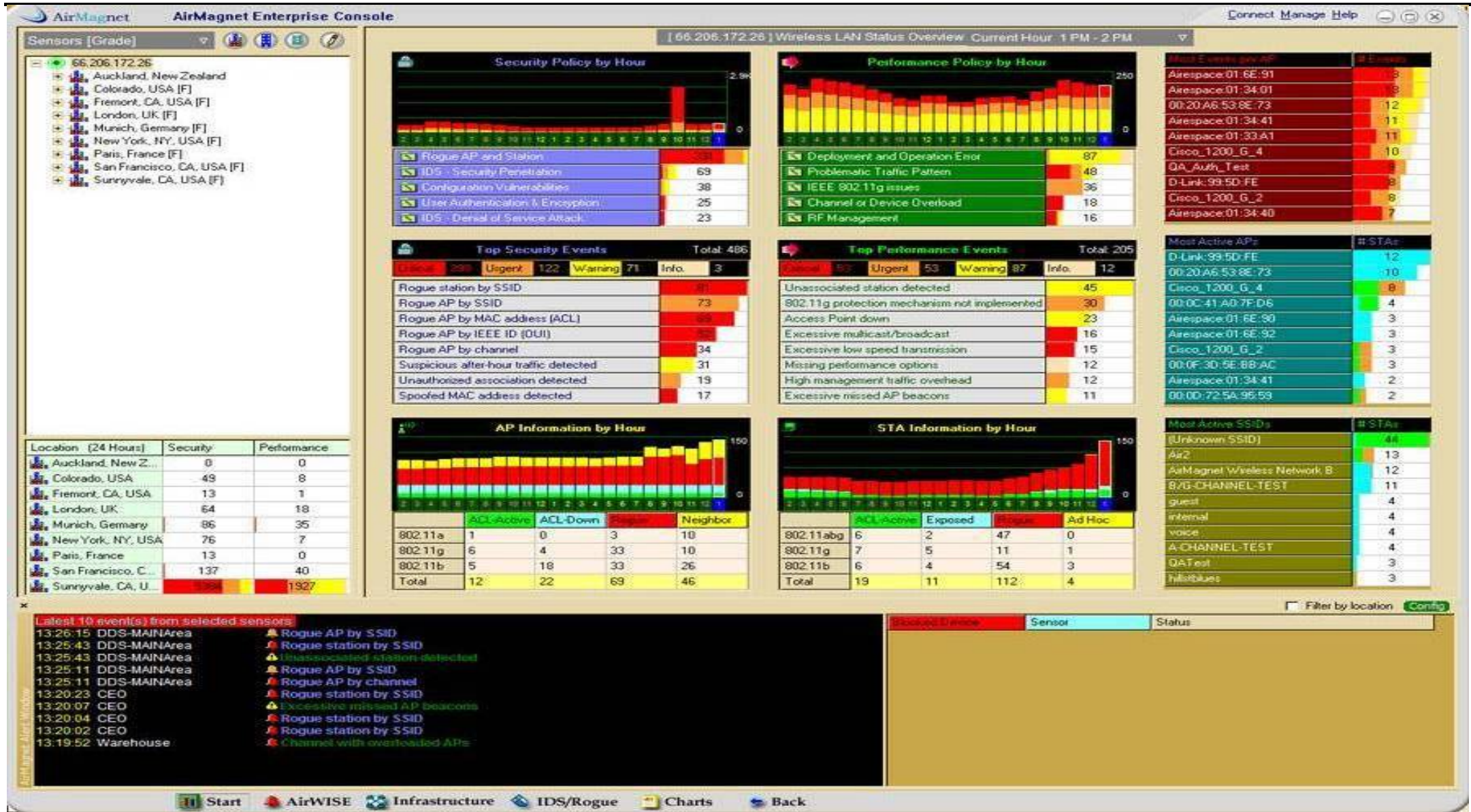


Figure 6-15: AirMagnet Enterprise Console

AirDefense Enterprise 7.0 includes multiple dashboards based on administrative roles such as the Manager Dashboard (figure 6-16) ("AirDefense Enterprise", 2005) that presents valuable information about the operation of the network.



Figure 6-16: AirDefense manager dashboard

- The centralised enterprise server provides a separate *Rogue/IDS* page (figure 6-17) ("Enterprise Quick", 2005:11) that allows for simple start/stop of wired/wireless blocking and provides all the historical blocking information.

The screenshot displays the AirMagnet Enterprise Console interface. On the left, a tree view shows the sensor hierarchy, including locations like Auckland, Colorado, Fremont, London, Munich, New York, Paris, San Francisco, and Sunnyvale, with sub-locations like CEO, Kitchen, Reception, etc. Below this is a summary table:

Location [24 Hours]	Security	Performance
Auckland, New Z...	0	0
Colorado, USA	49	8
Fremont, CA, USA	13	1
London, UK	64	18
Munich, Germany	87	35
New York, NY, USA	76	7
Paris, France	13	0
San Francisco, C...	137	40
Sunnyvale, CA, U...	541	1949

The main area shows the 'IDS AP List' with columns for Display Name, MAC Address, Owner, and Signal Status. A table of active IDS APs is displayed:

Display Name	MAC Address	Owner	Signal Status	First Seen
D-Link:99:5D:FE	B/G-CHANNEL-TEST		g 6 N	09/21 13:06:29
Allen-cube	QA_Test		b 6 Y	01/20 13:36:09
QA_Auth_Test	rogue Wireless		e 36 Y	
QA_Auth_Test	QA_Test		b 7 Y	
SMC:A6:92:C7	smc-rogue		g 11 Y	
Linksys:88:91:D1	hall75		b 6 N	
Netgear:B7:DA:00	t33r		g 9 N	
00:0F:66:42:8F:14	Niis		g 6 Y	
00:0F:66:2C:45:C2	linksys		g 6 Y	
Airspace:01:E4:60	linksys		b 6 N	
00:0F:66:C9:DC:23	MPL Broadcast		g 1 Y	
00:11:24:09:1B:C7	Machone Music		g 5 Y	
SMC:A8:9A:D6	SMC		g 11 Y	
00:03:93:EA:BF:A8	Mach One		g 5 Y	
Airspace:03:18:F0	linksys		b 6 N	

Control buttons include 'Disable Switch Port', 'Start Wireless Block', and 'Rogue Triangulation'. A configuration panel shows details for the selected device (QA_Auth_Test):

Switch IP	10.1.1.252
Switch Port	5
Rogue MAC	QA_Auth_Test
Status	Traced [01/12 03:14:01]

A history table shows the following entry:

Time	Rogue History Description	User-Sensor
10/22 16:09:39	Switch port disable pending	admin-Engineering-Office

At the bottom, a detailed view of the selected device (QA_Auth_Test) shows its MAC Address (00:07:85:B3:8A:E3), SSID (QA_Test), Channel (7), and other details. The 'IDS/Rogue' tab is highlighted with a blue circle.

Figure 6-17: Rogue IDS screen

Upon detecting a rogue device, it is possible to use the triangulation feature to pinpoint the location of the rogue device (figure 6-18) ("Enterprise Quick", 2005:13).

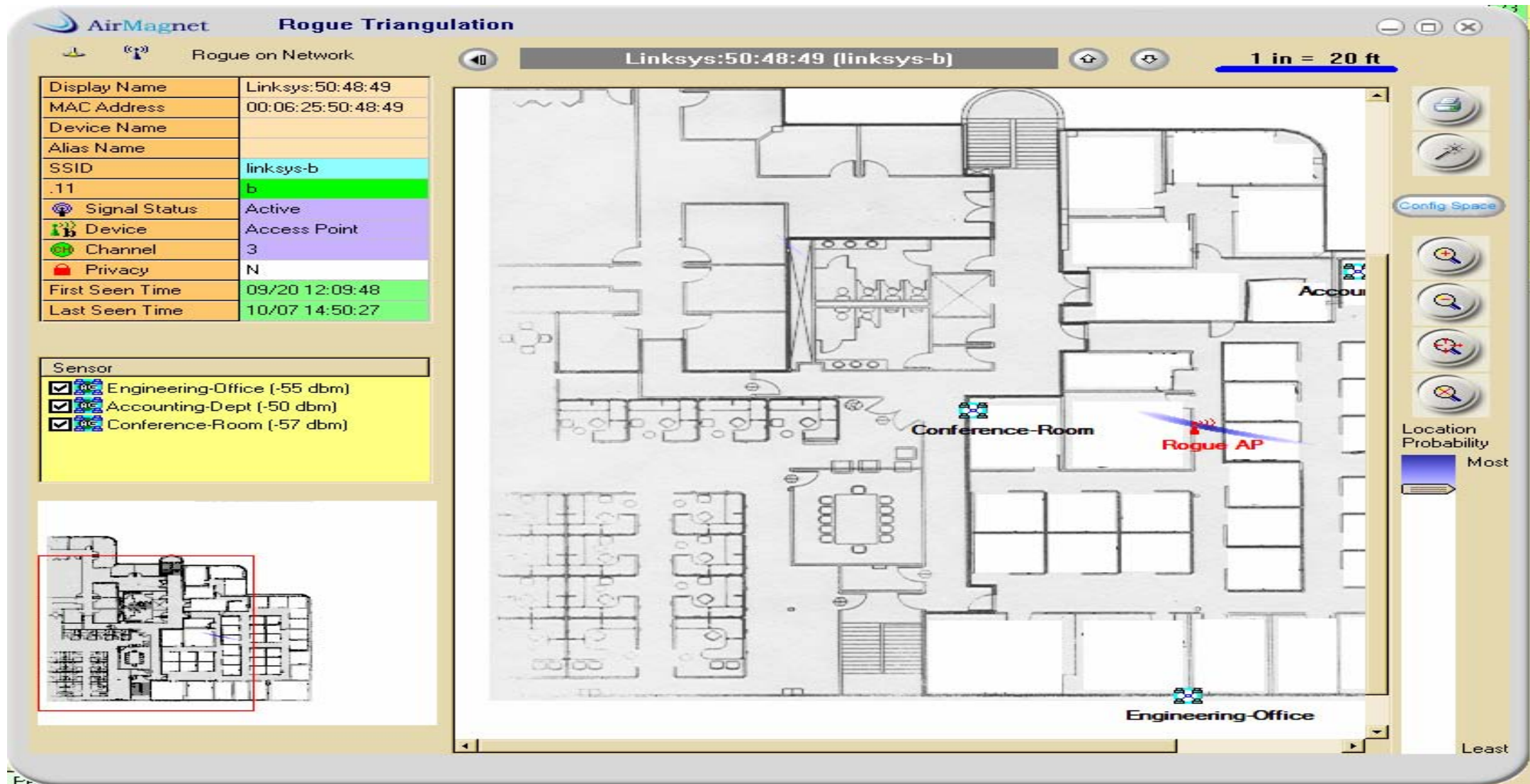


Figure 6-18: Rogue triangulation

- Both the AirMagnet centralised enterprise server and the SmartEdge sensors detect *MAC address spoofing* by studying the IEEE-authorized OUI and 802.11 frame sequence number signature ("AirMagnet Enterprise 6.0", 2005:83). The 2-byte sequence control field of an 802.11 frame (figure 4-4), collates fragments of 802.11 frames. The initial 4 bits denote a fragment number and the remaining 12 bits a sequence number progressively incremented by one if the frame is not fragmented which is always 0 for AirMagnet (Wright, 2005:14). WLAN intruders cannot alter this sequence number. As a result, it is possible to identify a spoofed MAC frame by scrutinising the pattern of successive sequence numbers for any deviation thereof (Wright, 2003:6). Furthermore, a specific manufacturer should allocate MAC addresses. Therefore, by monitoring the first 3 bytes exclusive to that specific manufacturer, it will be possible to determine spoofed MAC addresses (Wright, 2003:4).
- Both the AirMagnet centralised enterprise server and the SmartEdge sensors monitors the wireless client authentication process and identifies *DOS attack signatures* against the AP. An incomplete authentication and association process activates the AirMagnet Enterprise attack detection and statistical signature matching process. The DOS detection module uses statistical methods on the signal strengths and noise levels in which a time differential between beacons is the focus of statistical analysis (Lackey, Roths & Goddard, 2003:9). AirMagnet detects MAC address masquerading pending a successful client association to detect this form of DOS attack.
- Like the SmartEdge sensors, the AirMagnet centralised enterprise server is also able to check for policy violations. Therefore, the AirMagnet centralised enterprise server can detect a violation of some of the policies documented in appendix D. The AirMagnet centralised enterprise is able to validate an organisation's WLAN security deployment by monitoring on the authentication transactions and traffic encryption methods against the specified security deployment policy, which AirMagnet Enterprise learns from the AirMagnet policy configuration. AirMagnet Enterprise alerts the administrator on any AP operating without any layer 2 data encryption mechanisms such as WEP, TKIP or AES ("AirMagnet Enterprise 6.0", 2005:128). The AirMagnet centralised enterprise server is capable of detecting configuration vulnerabilities such as ad-hoc stations, APs broadcasting their SSIDs, an AP with a

configuration that has changed and APs using default configuration ("AirMagnet Enterprise", 2005:7-14).

- The AirMagnet Spectrum analyser included in AirMagnet Enterprise 7.0 caters for the identification of *RF jamming devices* in real time by using spectral fingerprinting techniques (figure 6-19) ("AirMagnet Spectrum", 2006:2). Figure 6-19 illustrates the identification of a microwave jamming device.

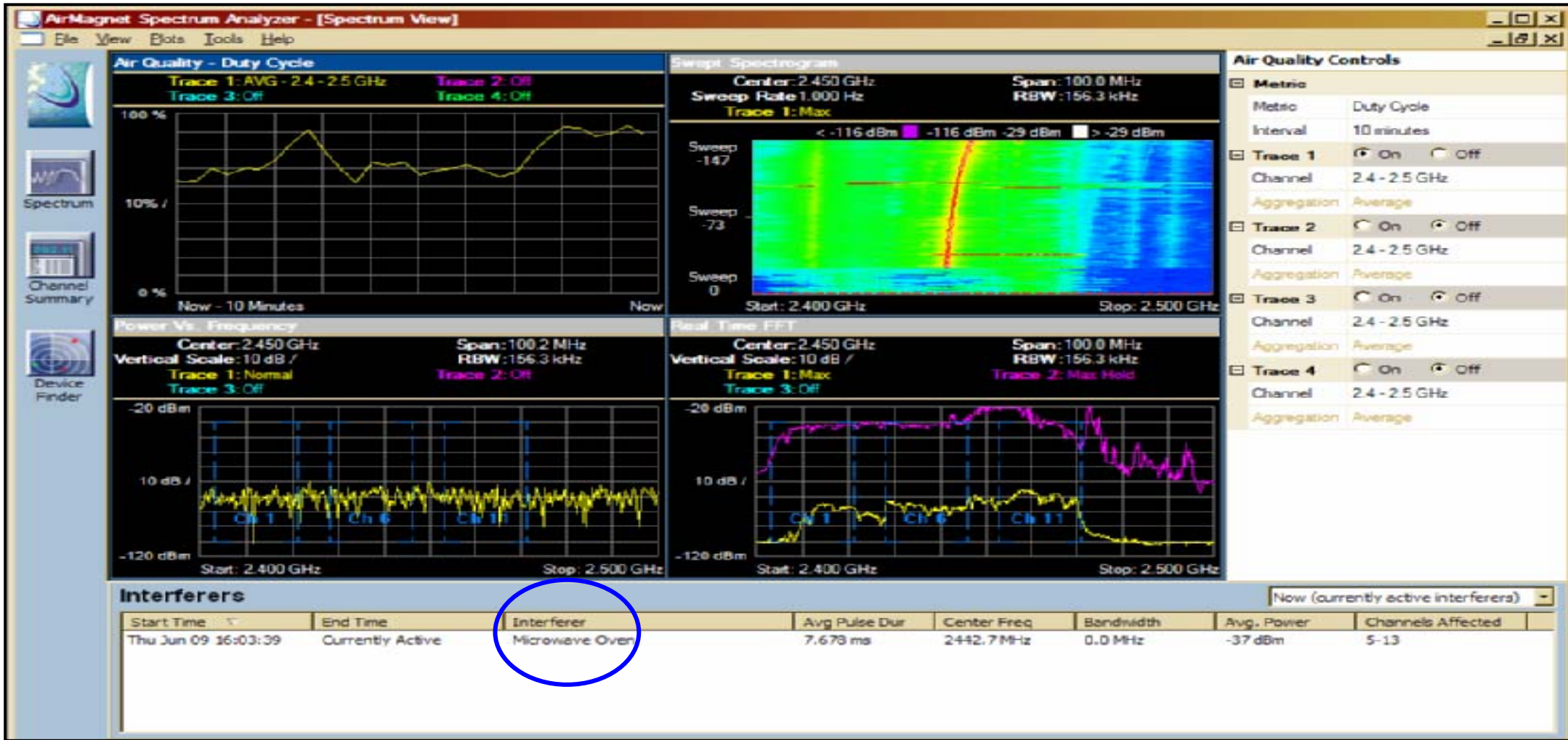


Figure 6-19: Spectrum analyser identifying RF jamming devices

- ▣ Both the AirMagnet centralised enterprise server and the SmartEdge sensors generate a *device probing for AP* alarm when WLAN intruders probe the WLAN using WLAN discovery or war driving tools such as NetStumbler ("AirMagnet Enterprise", 2005:62).
- ▣ Both the AirMagnet centralised enterprise server and the SmartEdge sensors generate an alert on weak key implementations and recommends a device firmware upgrade ("AirMagnet Enterprise", 2005:89). *Firmware* is programming that is inserted into programmable read-only memory (programmable ROM), to become a permanent part of a computing device ("Define firmware": 2000-2006).
- ▣ AirDefense Enterprise 7.0 provides administrators with the ability to review and rewind detailed records of wireless activity to assist in a forensic investigation (figure 6-20) ("AirDefense Enterprise", 2005). This is possible by virtue of a special console, the AirDefense IntelliCenter, incorporated into the AirDefense server. Using this console makes it is possible to ("AirDefense Enterprise", 2005) ("Enterprise Class", 2002-2005:3):
 - ▣ Rewind and review all device, network, connectivity, traffic and location information for any period with granularity (device, AP, location, group, enterprise).
 - ▣ Have forensic records that ensure compliance with regulations can be audited.
 - ▣ Store, analyse and mine data efficiently over extended periods..



Figure 6-20: AirDefense forensic engine

6.5.3 DECISION

Having decided that an intrusion has indeed taken place, necessary notification must take place. AirMagnets notification methods include ("Enterprise-hardened", 2005) SNMP versions 1, 2 and 3, sysLog, eventLog, e-mail, Page over Internet, instant messaging and short messenger service (SMS).

6.5.4 ACTION

AirMagnet Enterprise takes action in the following manner ("AirMagnet Enterprise 6.0 User", 2005:4):

- ▣ The AirMagnet Enterprise wired trace and block rogue device feature (figure 6-17) tracks down the wired-side IP address of the rogue AP and manually blocks it. The results will include the switch IP address and the port to which the rogue AP is connected. AirMagnet Enterprise also provides the feature of wired auto-trace and auto-blocking, in which the rogue AP is traced and automatically blocked on detection.
- ▣ The wireless trace and block rogue feature (figure 6-17) allows the SmartEdge Sensor to associate with the rogue AP and discovers the IP address used by or through the rogue AP to connect to the enterprise wired network. The sensor can suspend wireless communication from the rogue AP. AirMagnet Enterprise also provides the feature of wireless auto-trace and auto-blocking, in which the rogue AP is traced and automatically blocked as soon as it is detected. Figure 6-21 illustrates the wired port lookup and suppression feature of AirDefense 7.0.

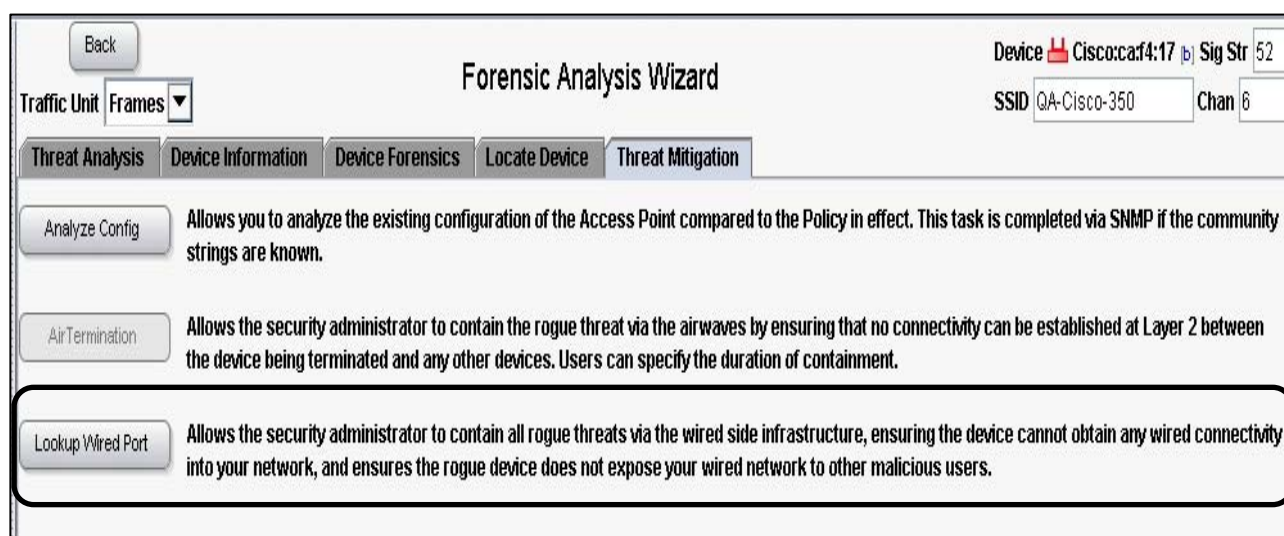


Figure 6-21: Wired port lookup feature of AirDefense Enterprise 7.0

In this regard, AirMagnet Enterprise and AirDefense Enterprise are not only intrusion detection systems but also intrusion prevention systems because they prevent unauthorised access to the WLAN.

The link from the action phase again to observation phase entails conducting maintenance activities on the wireless IDS/IPS. This includes updating new signatures, installing IDS upgrades and re-evaluating the placement of IDS sensors. Figure 6-18 depicts the architectural design of a wireless IDS/IPS using the AirMagnet Enterprise 6.0 system.

The degree to which WLAN intrusion security risks are capable of been mitigated can be determined by studying the operational features of the wireless IDS/IPS. It is necessary to revisit the nine areas of concern (figures 11-2 to 11-10) to determine the extent to which these intrusion security risks are capable of been mitigated by preventing a risk from occurring altogether or to reduce the impact or consequences of its occurrence to an acceptable level by taking corrective action.

- ☑ First area of concern: The first area of concern is rogue APs (figure 11-2). The AirMagnet Enterprise Block Rogue feature (figure 6-17, section 6.5.4) is an immediate solution to prevent a rogue AP from further risking WLAN security.
- ☑ Second area of concern: War-driving and wireless client probing for association with an AP with any SSID using NetStumbler can be reduced to an acceptable level by configuring APs not to broadcast their APs. The enterprise-wide protection strategy (appendix D, table 12-15) documents this information. Furthermore, the 24x7 network-monitoring feature of the AirMagnet policy management can detect APs that broadcast their SSIDs (figures 6-11 to 6-12). AirMagnet also generates the device probing for an AP alarm.
- ☑ Third area of concern: WLAN traffic encrypted with TKIP and MIC defeats packet forgery and replay attacks. AirMagnet can issue an alarm if the AP is unprotected by TKIP (figure 5-9). The WLAN enterprise-wide protection strategy (appendix D) also stipulates the use of TKIP to provide message integrity verification (table 12-11).
- ☑ Fourth area of concern: Table 12-14 of the WLAN enterprise-wide protection strategy advocates that users should not divulge any sensitive information.
- ☑ Fifth area of concern: AirMagnet Enterprise detects continuous RF noise over a certain threshold for a potential RF jamming attack (figure 6-19). A reported RF

jamming attack can be further investigated by tracking down the noise source using the AirMagnet find tool (figure 6-10) on the laptop and handheld analysers. As far as DOS association floods are concerned, AirMagnet can detect this type of DOS attack (figure 6-7). The WLAN security officer can log on to the AP to check the current association table status or use the active Tools (Diagnostics, DHCP, Ping) (figure 6-10) to test the wireless service provided by this AP. These tools are available via the remote analyser on the Enterprise system (figure 6-15) as well as on the laptop and handheld analysers.

- ☑ Sixth area of concern: In order to mitigate the security risk of MAC address spoofing, (figure 6-8), it is essential to ensure that all APs deploy a strong form of authentication. EAP-FAST, which is currently the mode of encryption (figure 11-14), alleviates the problem of MAC addresses been broadcast in plain text by WEP.
- ☑ Seventh area of concern: In EAP-FAST, a tunnel is created between the client and the server using a PAC (Protected Access Credential) to authenticate each other. After the tunnel establishment process, the client is authenticated using the user-name and password credentials. Thus even though, the client has stolen the WNIC, the client will not be able to gain access to the WLAN because of the need of knowing the user-name and password credentials.
- ☑ Eighth area of concern: 802.11i with AES and WPA with TKIP can overcome the IV problems. The WLAN enterprise-wide protection strategy (appendix D, table 12-11) documents the use of these two modes of encryption.
- ☑ Ninth area of concern: Retaining the default settings of APs, SSIDs, SNMP and DHCP can cause AirMagnet to signal an alarm regarding this (figure 6-9). Care should be taken to ensure these default settings are disabled. The WLAN enterprise-wide protection strategy (appendix D, table 12-15) advocates the disabling of these default settings.
- ☑ The current organisational vulnerability of the University (figure 11-15), indicates that wireless clients do not have personal firewalls installed. This prevents a port scanner from communicating with open ports. Installing a stand-alone wireless personal intrusion detection system such as AirDefense personal makes it possible to detect eavesdropping attacks. The AirDefense Personal agent can also prevent policy violations or malicious attacks such as redirection attacks, man-in-the-middle attacks, deauthentication attacks and secure the network from probing laptop

problems. The WLAN enterprise-wide protection strategy (appendix D, table 12-15) advocates the deployment of personal firewalls on the wireless clients.

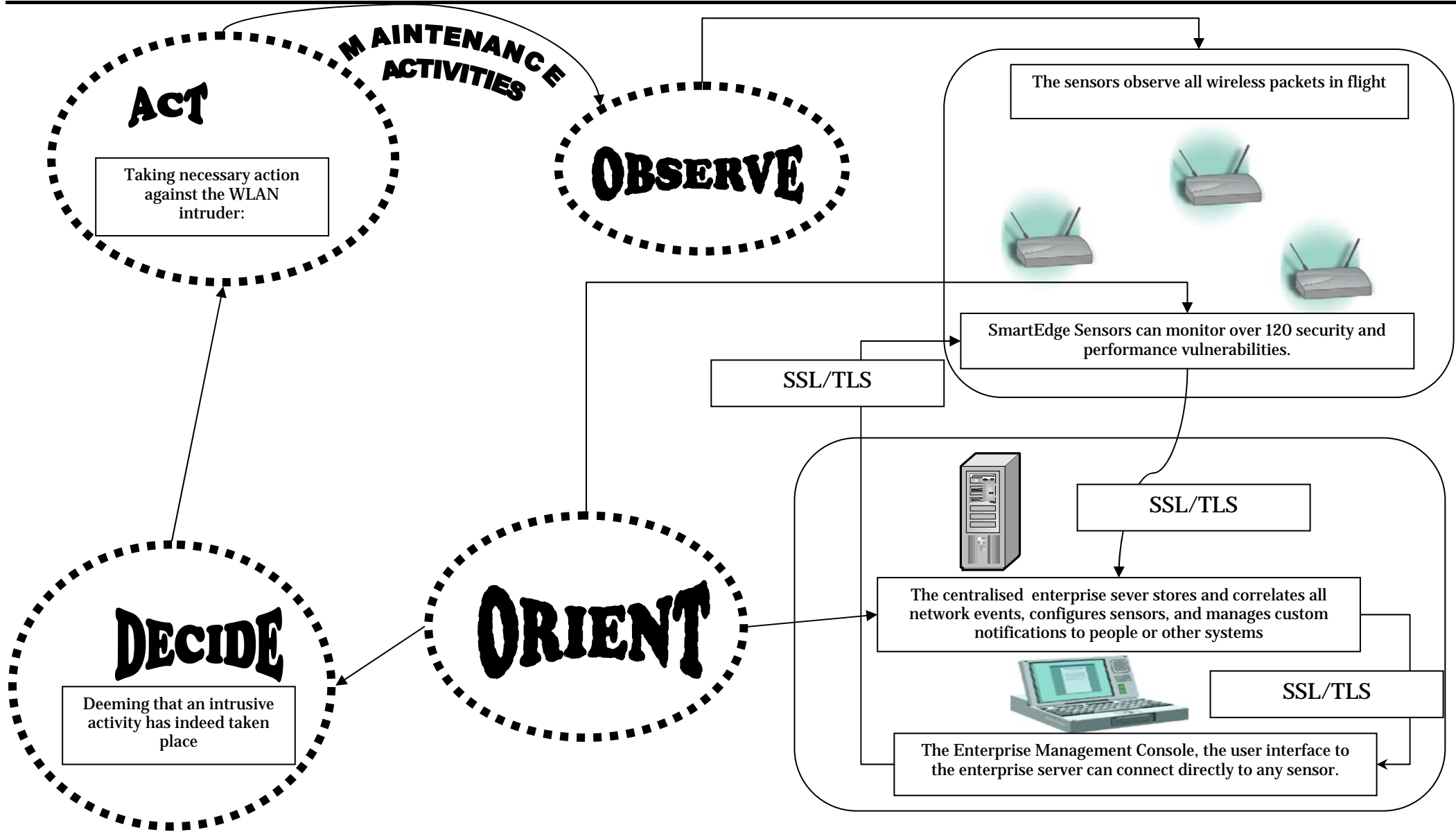


Figure 6-22: Operational design of a wireless IDS/IPS using AirMagnet

The above theoretical description of a wireless IDS/IPS has been designed to detect and mitigate WLAN intrusion attacks to an acceptable level, but no matter how much forethought goes into the planning of such a system, "developing systems that are absolutely secure is extremely difficult, if not generally impossible" (Denning, 1986:118).

6.6 WLAN INTRUSION SECURITY RISK ANALYSIS CONCLUDING ACTIVITIES

The following activities are the concluding activities of the WLAN intrusion security risk analysis process (Alberts & Dorofee, 2003:51):

6.6.1 PREPARATION TO MEET WITH SENIOR MANAGEMENT

Senior management should receive the WLAN intrusion security risk analysis results.

6.6.2 PRESENTATION OF RISK INFORMATION

Senior management should receive the following risk information:

Information regarding the most important assets, the security requirements for these assets as well as the areas of concern. The database can generate these reports. As far as the technological vulnerability assessment is concerned, a live demonstration using a tool such as the AirMagnet handheld analyser should be performed. It would also be advisable to discuss the impact of a WLAN intrusion attack verbally with senior management using the information from the risk impact assessment instead of presenting them with reports. This serves to heighten the severity of a WLAN intrusion attack.

6.6.3 REVIEW AND REFINEMENT OF WLAN ENTERPRISE-WIDE PROTECTION STRATEGY AND WLAN INTRUSION SECURITY MITIGATION PLAN

Senior management should receive the WLAN enterprise-wide protection strategy and WLAN intrusion security risk mitigation plan for review and modification. The WLAN intrusion security risk mitigation plan should be a condensed plan outlining the features of a wireless IDS/IPS as senior management may not read a voluminous report. These reports can be generated from the database.

6.6.4 CREATION OF SUBSEQUENT STEPS

This milestone marks the termination of the WLAN intrusion security risk analysis process. The ensuing chapter addresses the follow-up activities of the WLAN intrusion security risk analysis process.

It is at this stage fitting to review the objective of risk analysis as outlined in chapter two, section 2.5.4 to see whether this objective has been realised. The objective of risk analysis is to identify risks from potential or inadvertent events (these real and perceived threat scenarios were identified by virtue of studying the OODA cycle of the WLAN intruder) with a view to reducing the level of risk to an acceptable level (the risk profile indicated a high risk impact degree meaning that the risks should be mitigated. A WLAN enterprise-wide protection strategy and WLAN intrusion security risk mitigation plan was proposed to reduce the risks to an acceptable level). A report on the justification for the implementation of countermeasures to reduce the risk to an acceptable level should be submitted to senior management for approval (a report on the proposition of a wireless IDS is presented to senior management).

6.7 CONCLUSION

This chapter concludes the WLAN intrusion security risk analysis process. However, the entire exercise could be an exercise in futility if there is no follow-up and implementation of the results that were proposed. The next chapter therefore addresses the post-OCTAVE activities.



PART

WLAN INTRUSION SECURITY RISK MANAGEMENT

CHAPTER SEVEN

ACTION: POST-OCTAVE ACTIVITIES

Words are nothing but words; Power lies in deeds. Be a person of action.

- Mali Oriot Mamudu Konyate

A square graphic with a grey background. In the center is a large, stylized white number '7'. The word 'CHAPTER' is written in a bold, black, sans-serif font across the middle of the '7'. The background of the square is filled with a repeating pattern of small, light grey icons: a circle with a dot, a square with a dot, and a triangle with a dot, arranged in a grid.

CHAPTER

7. ACTION: POST-OCTAVE ACTIVITIES

7.1 INTRODUCTION

Subject to senior management approval, the next step is implementing the results of the WLAN intrusion security risk analysis process. This entails conducting typical risk management activities. Risk management is a crucial activity because it succeeds risk analysis and aids in reducing the exposure of risk.

The objective of this chapter is the enforcement of the WLAN enterprise-wide protection strategy and implementation of the WLAN intrusion security risk mitigation plan.

7.2 STRUCTURE OF THIS CHAPTER

This chapter focuses on conducting the WLAN intrusion security risk management process whereby the organisation actually implements the results of the WLAN intrusion security risk analysis exercise. This entails carrying out the post-OCTAVE activities.

The following diagram (figure 7-1) depicts the role of this chapter within the overall context of the dissertation.

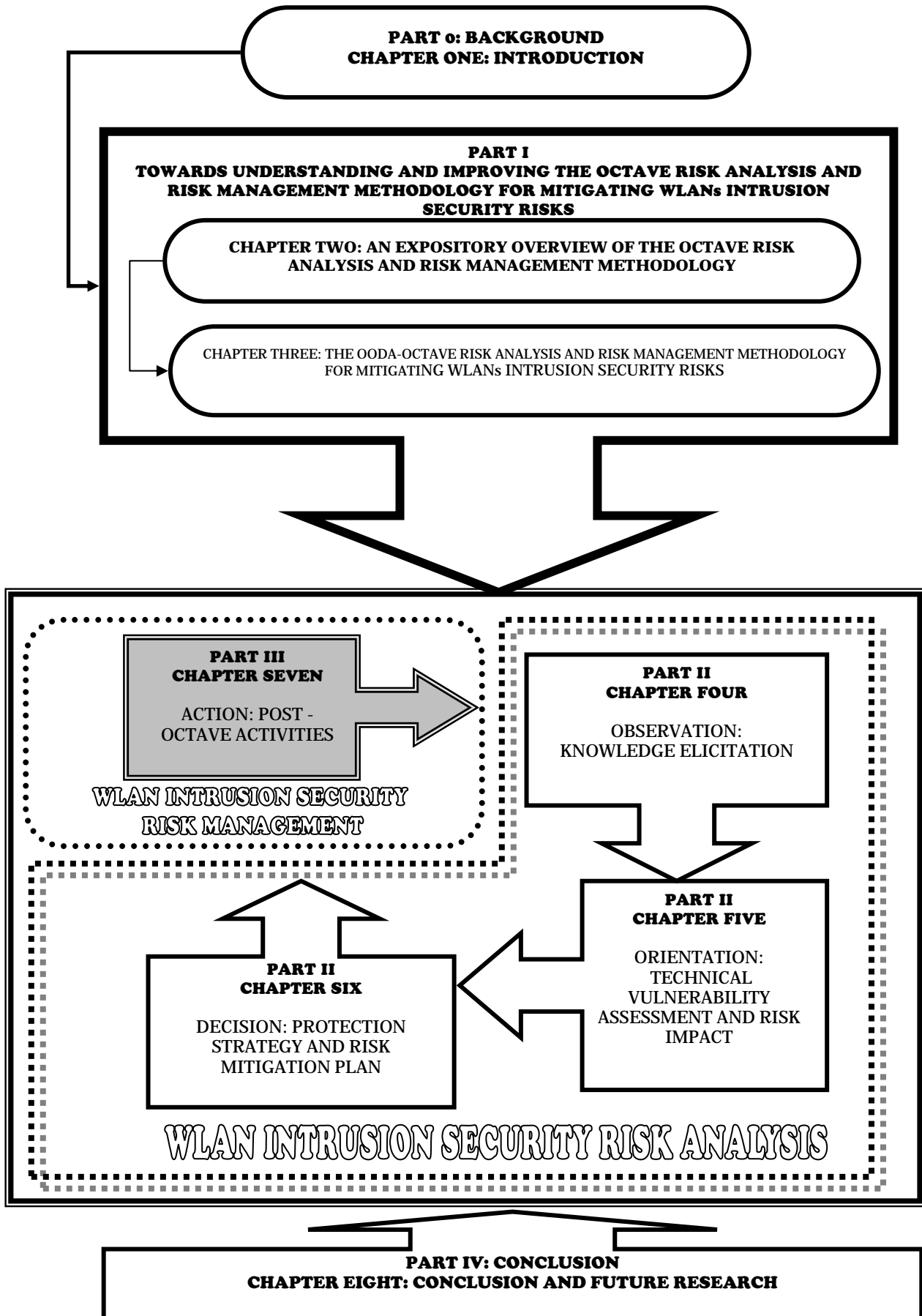


Figure 7-1: The role of chapter seven within the overall context of the dissertation

The post-OCTAVE activities include:

7.3 PLANNING HOW TO IMPLEMENT THE WLAN ENTERPRISE-WIDE PROTECTION STRATEGY AND WLAN INTRUSION SECURITY RISK MITIGATION PLAN

Implementation of a wireless IDS/IPS entails contacting the relevant vendors. Carefully designed countermeasures such as wireless IDSs/IPSs can detect and mitigate WLAN intrusion security risks but a great deal of forethought has to go into the deployment issues of such a countermeasure. In the initial stages, an organisation should develop a detailed, well-designed deployment plan.

7.4 IMPLEMENTING THE PLANS

This entails circulating the enterprise-wide protection strategy document to all personnel within the University. The corporate manual on the University intranet should contain a copy of this policy. As far as implementing the wireless IDS/IPS is concerned, the AirMagnet Surveyor should be used to determine the strategic location of APs. It will be possible to determine where to place the network-based sensors after determining where the APS should be located as the consensus is to deploy sensors (network-based sensors) wherever an AP is located. AirMagnet Surveyor permits the conduction of site surveys by providing a range of scientific tools to assist with the positioning of APs. AirMagnet Surveyor allows one to see the RF coverage, signal interference and packet statistics as well as simulate corrective action before actual implementation.

AirMagnet Survey PRO is a separate version of the Survey software released with the new version of AirMagnet Enterprise 7.0. The Survey PRO caters for ("AirMagnet Survey", 2002-2006; "AirMagnet Survey", 2006:2):

- ▣ Integration with AirMagnet spectrum analyser-using both Survey PRO and Spectrum Analyser facilitates viewing both WiFi and spectrum analysis data. This provides an overview of how the RF spectrum relates to WiFi performance.
- ▣ AirWISE for site surveys-AirWISE allows users to enter a variety of design requirements for the wireless LANs and document all areas that fail to meet their standards.
- ▣ Capacity planning-ensures that there are enough access points to meet the number of users for that particular area and satisfy their network performance needs.

- ▣ Multi-floor survey-simultaneously displays results of up to four floors of a structure allowing a user to map an AP's signal and view how it reaches and affects floors above and below the AP. This can prevent signal leakage. This can therefore mitigate the second area of concern (figure 11-3).

7.5 PROMOTING AWARENESS OF THE PLANS

User awareness is paramount for the successful implementation of the WLAN security policy. Users are sometimes oblivious to the security policies, procedures and standards of an organisation (Von Solms & Von Solms, 2004:375). At present, less than half of all organisations keep users abreast of the impact of information security issues and users receive no training on how to respond to a security breach ("Global Information", 2005:13). A survey conducted by Deloitte reveals that only 22% of the respondents have issued guidelines for safe use of WiFi and only 57% have established security policies regarding organisational wireless usage ("2005 Global", 2005:30). A study conducted by the U.S. GAO, revealed that 18 out of 24 federal agencies have not established any training programmes with regard to wireless security policies ("Federal Agencies", 2005:18).

7.6 MONITORING THE PLANS FOR EFFECTIVENESS AND PROGRESS

A dedicated network administrator should continuously monitor the wireless IDS/IPS system to see if intrusion attempts are averted and if users are complying with the wireless policy. It is necessary to take reactive measures when an intrusion is detected.

7.7 CONTROLLING BY TAKING APPROPRIATE CORRECTIVE ACTION FOR ANY VARIATIONS IN THE EXECUTION OF THE PLAN

To date, AirMagnet has been capable of detecting more than 130 threats ("Mobile Solution", 2005). However, WLAN intruders always find new and innovative ways of intruding WLANs. AirMagnet can detect these "day-zero" attacks which are vulnerabilities exploited on the very day they are discovered. Enterprise 6.0 includes day-zero alarms, which look specifically for out of the ordinary clustering or trends to identify new variations on existing attacks or novel tools that combine and repeat attacks ("AirMagnet Completes", 2005). Another form of control can be to take action against personnel contravening the WLAN policy rules.

The database contains a section (figure 7-2) for the post-OCTAVE activities, which can be used by the network administrator subject to senior management approval of the WLAN enterprise-wide protection strategy and WLAN intrusion security risk mitigation plan.

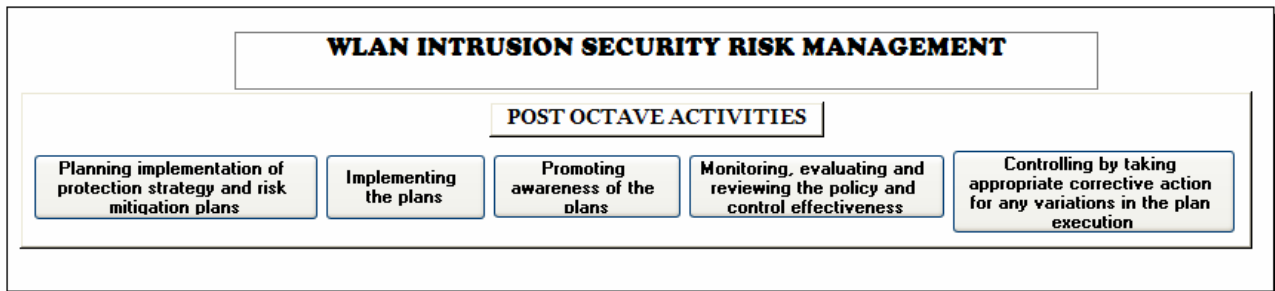


Figure 7-2: Post-OCTAVE activities

This terminates the WLAN intrusion security risk management process. It is therefore fitting to review the objective of risk management as outlined in chapter two, section 2.5.4 to ascertain whether this objective has been realised.

The objective of risk management is the implementation of appropriate risk mitigation (implementing the WLAN enterprise-wide protection strategy and WLAN intrusion security risk mitigation plan subject to senior management approval), risk transfer and risk recovery measures to reduce business exposure by balancing countermeasure investment against risk (the benefits of deploying a wireless IDS as a risk mitigation countermeasure can transcend the costs incurred of deploying this system).

7.8 CONCLUSION

This chapter terminates the OODA-OCTAVE risk analysis and risk management methodology for mitigating WLANs intrusion security risks. The next chapter concludes with final remarks about this methodology.



CONCLUSION

CHAPTER EIGHT

CONCLUSION

AND FUTURE

RESEARCH

The policy of being too cautious is the greatest risk of all.

- Jawaharlal Nehru

A square graphic with a grey background and a white border. Inside the square, the word "CHAPTER" is written in a bold, black, serif font. A large, white, stylized number "8" is superimposed over the text, with a white pen nib at the top of the upper loop.

CHAPTER

8. CONCLUSION AND FUTURE RESEARCH

8.1 INTRODUCTION

This principle aim of this research was to develop a risk analysis and risk management methodology for mitigating WLANs intrusion security risks.

In this chapter, the researcher evaluates the degree to which this aim has been accomplished. This dissertation terminates with a section reflecting possible avenues for further research.

8.2 ASSESSING THE DEGREE TO WHICH RESEARCH QUESTIONS HAVE BEEN ADDRESSED

The research questions posed in chapter one will be re-examined to determine the extent to which they have been addressed in this dissertation.

8.2.1 WHAT ARE THE POSSIBLE TYPES OF INTRUSION ATTACKS THAT CAN BE LAUNCHED ON WLANs?

This question was answered by studying the OODA cycle of WLAN intruders. This presented insight to the real and perceived security issues of WLANs. A literature study revealed DOS attacks, masquerade attacks, penetration of the security control system, leakage, eavesdropping, malicious use, replay attacks, social engineering and brute force attacks as some of the possible WLAN invasion attacks (chapter four). The default settings of WEP, SSID, MAC address filtering, AP passwords, SNMP and DHCP settings also provide opportunities for attack.

8.2.2 HOW SHOULD A WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE BE CONDUCTED?

The OCTAVE risk analysis methodology was selected for conducting the WLAN intrusion security risk analysis exercise. This methodology was put through the GAO strength test

(appendix A) and the outcome of this test revealed that the OCTAVE risk analysis methodology is a sound risk analysis methodology. However, the OCTAVE risk analysis methodology was found to be flawed in a few respects as outlined in chapter two, section 2.7.2.1. These flaws, which could have an impact on a WLAN intrusion security risk analysis exercise, include an extremely long time to conduct the process and relying on a brainstorming process for asset and threat scenario identification.

To overcome these weaknesses, it was proposed that the OCTAVE risk analysis methodology be improved by fusing it with the *observe*, *orient* and *decision* elements from the OODA cycle. The OODA cycle can overcome the weaknesses of the OCTAVE risk analysis methodology because it advocates moving rapidly through the cycle thereby arriving at a decision in a shorter time. It also entails getting into the mind of the adversary. This unravels typical threat scenarios which can not be done by a brainstorming process. Unravelling typical threat scenarios eliminates the need to go through the structured interviews (phase1, processes 1-3), which in turn facilitates shortening of the OCTAVE risk analysis process. A database was created for the storage, retrieval and printing of WLANs intrusion security risk analysis and risk management information. This database precluded the need for formal training and investment in paper and human resources, thereby shortening the OCTAVE risk analysis process.

The OODA cycle can also ensure that the OCTAVE risk management process is recognised as a vital follow-up activity of the risk analysis process. This is because the OODA cycle has a clearly delineated element, *action*, which advocates executing the decision. This element is an integral part of the cycle. Therefore, the OODA cycle was assimilated with the OCTAVE risk analysis and risk management processes. Consequently, it evolved into the OODA-OCTAVE risk analysis and risk management methodology for mitigating WLANs intrusion security risks (chapter three).

The WLAN intrusion security risk analysis exercise was conducted in a sample educational environment. By conducting a WLAN intrusion security risk analysis exercise, it was possible to determine the most important assets, the current protection practices and organisational vulnerabilities and the real and perceived threat scenarios in the WLAN operating environment (appendix C). Nine areas of concern (appendix C, figures 11-2 to 11-

10) were identified. A vulnerability scan uncovered technological vulnerabilities and the threat impact on the University's mission and objective was examined (chapter five).

The risk impact criteria connoted a high degree of impact (figure 5-21). It therefore became necessary to create a WLAN enterprise-wide protection strategy (appendix D) and to justify the deployment of a wireless IDS/IPS as one of several security countermeasures capable of mitigating WLANs intrusion security risks (chapter six).

The WLAN enterprise-wide protection strategy (appendix D) documents a host of strategic and operational practices to be adopted by the University.

To justify the deployment of a wireless IDS/IPS, the operational and deployment issues of a wireless IDS/IPS were investigated. A wireless IDS/IPS can only possess a certain degree of functionality before a new WLAN security attack emerges, in which case the impact of the threat has to be determined and the functionality of the wireless IDS/IPS has to be updated. It is because of the cyclic nature of WLAN attacks that the operational design of the wireless IDS/IPS was constructed using the OODA cycle (chapter six). Two selected wireless IDSs/IPSs, AirMagnet Enterprise 6.0 and AirDefense Enterprise 7.0 were studied.

It was illustrated that by enforcing a WLAN enterprise-wide protection strategy and deploying a wireless IDS/IPS (chapter 6), WLANs intrusion security risks can be reduced to an acceptable level either by taking action after an intrusion has taken place to prevent its reoccurrence (intrusion detection) or to prevent an intrusion from taking place altogether (intrusion prevention).

AirMagnet and AirDefense are intrusion detection systems rather than intrusion prevention systems because they are able to report that an intrusion attack has taken place and then offer advice on how to remedy the situation. The only real intrusion prevention feature of these systems is its ability to auto trace and auto block rogue APs.

As far as the deployment issues are considered, AirMagnet Surveyor was reviewed (chapter seven) as it can determine the strategic location of APs. It will be possible to determine where to place the network-based sensors after determining where the APS should be

located as the consensus is to deploy sensors (network-based sensors) wherever an AP is located.

8.2.3 WHAT STEPS MUST AN ORGANISATION TAKE TO ENFORCE THE RESULTS OF A WLAN INTRUSION SECURITY RISK ANALYSIS EXERCISE?

Post-OCTAVE activities were critically evaluated and expanded (chapter two). These activities conforming to the action phase of the OODA cycle were included as a vital component in the OODA-OCTAVE risk analysis and risk management methodology for mitigating WLANs intrusion security risks. The database also has a separate form for storing WLANs intrusion security risk management information.

The post-OCTAVE activities focused on the actual institutionalisation of the WLAN enterprise-wide protection strategy and WLAN intrusion security risk mitigation plan and the continuous monitoring thereof (chapter seven). It was deduced that promoting user awareness is an activity that requires attention.

8.3 EXTENSIBILITY OF RESEARCH

This research specifically focused on addressing the intrusion security risks of a WLAN operating environment as this technology has been statistically proved to be a promising future technology (chapter one). However, because of the relentless pace at which technology evolves, no technology can be stagnant and there will always be future developments and enhancements.

One particular technology, WiMax (world interoperability for microwave access) based on the IEEE 802.16a standard, is destined to have more than 7 million subscribers by 2009 and is expected to grow more rapidly than WiFi with Intel anticipating WiMax functionality on half of the world's notebooks by 2008 (Carter, 2005:21-22). Other projected standards include the 802.16e standard and Mobile Broadband Wireless Access (MBWA), based on the IEEE 802.20 standard (Cannon, 2006:180). Since these are also wireless networks, they also require an expeditious risk analysis methodology. The OODA-OCTAVE risk analysis and risk management methodology can in future be used to address the intrusion security risks of these wireless networking environments.

8.4 FUTURE RESEARCH

The following issues require further research:

- ▣ To study the OODA cycle of the WLAN intruder, a great deal of reference to existing literature was made. This served to expose the current vulnerabilities of these networks. A more adept approach would be to use a *honeypot*. A honeypot, or a network of honeypots, termed a *honeynet* can be used to "research hacking methods and techniques" (Carter & Shumway, 2002:73). By using such a decoy tool, it will be possible to observe the behaviour of WLAN intruders and to ascertain the different types of attacks that can occur. A honeypot will not affect the operational systems therefore posing no risk to the network (Endorf et al., 2004:358).
- ▣ The database has several limitations that require enhancement. These include enhancing the database to cater for the probability that not all of the outcomes may materialise. Furthermore, the database should be converted into an executable file that can be used on any system, precluding the need to have the Microsoft Access 2003 application installed on that particular system.
- ▣ Constructing a comprehensive WLAN policy can be an exercise in futility if no one takes heed of this policy. It is therefore necessary to create a WLAN user awareness model. In addition, it is important to enlist the participation of senior management for the enforcement of the WLAN policy and deployment of the WLAN risk mitigation plan.

8.5 CONCLUSION

In conclusion, it is befitting to include a piece of the eulogy that was published in *Inside the Pentagon* written by General Charles Krulak who was at that stage the Commandant of the U.S. Marine Corps (Hammond, 2001:3) after Colonel John Boyd's demise in 1997.

11 Mar 97

To the Editor:




"I was deeply saddened to learn of the passing of Colonel John Boyd, USAF (Ret). How does one begin to pay homage to a warrior like John Boyd? He was a towering intellect who made unsurpassed contributions to the American art of war. Indeed, he was one of the central architects in the reform of military thought which swept the services, and in particular the Marine Corps, in the 1980s. From John Boyd we learned about competitive decision making on the battlefield-






*compressing time, using time as an ally. Thousands of officers in all our services knew John Boyd by his work on what was to be known as the **Boyd Cycle or the OODA Loop**."*


Colonel Boyd's contribution to military strategy, in particular his development of the OODA cycle was acknowledged even in his eulogy. Colonel Boyd advocated that attacking the mind of the adversary prior to a battle is the quintessence of intelligent fighting. This philosophy was extended to the risk analysis process. The development of the OODA-OCTAVE risk analysis and risk management methodology can allow organisations to proactively defend their WLAN operating environments and reap the benefits of this promising technology.





9. APPENDIX A: ASSESSING THE STRENGTH OF THE OCTAVE RISK ANALYSIS METHODOLOGY

The GAO guideline is used to assess the strength of the OCTAVE risk analysis methodology. A denotes that OCTAVE has satisfied the particular criterion.

(GAO:1999)	
<i>Obtain senior management support and involvement</i>	
	OCTAVE stipulates senior management sponsorship to the point that senior managers actually have to participate in the process (phase 1, process 1). This is a crucial step in order to leverage interest and commitment from the rest of the team as information security will not be sufficiently addressed without the support and initiative of executive management (Von Solms & Von Solms, 2004:372). Furthermore, the success of any risk analysis exercise is subject to the role of top management in decision-making and selection undertaking (Broder, 1984:3; Badenhorst & Eloff, 1990:342).
<i>Designate focal points: This entails assembling a group of individuals to guide and govern the risk analysis process.</i>	
	The focal point of the OCTAVE method is the analysis team, a group of people from various hierarchical levels of the organisation who have a substantial amount of knowledge regarding the organisation, its business and technological processes to lead and manage the OCTAVE risk analysis process.
<i>Define procedures</i>	
	<p>OCTAVE uses a three-phase approach to examine the organisational and technological issues of the organisation (Whitman & Mattord, 2004: 345). Each phase consists of a number of processes.</p> <ul style="list-style-type: none"> ▣ <i>Phase 1: Build asset-based threat profiles</i> <ul style="list-style-type: none"> ▣ Identify senior management knowledge. ▣ Identify operational area management knowledge. ▣ Identify staff knowledge. ▣ Create threat profiles.

(GAO:1999)	
	<ul style="list-style-type: none"> ▣ <i>Phase 2: Identify infrastructure vulnerabilities</i> <ul style="list-style-type: none"> ▣ Identify key components. ▣ Evaluate selected components. ▣ <i>Phase 3: Develop security strategy and plans</i> <ul style="list-style-type: none"> ▣ Conduct risk analysis. ▣ Develop protection strategy.
<i>Involve business and technical experts</i>	
	This criterion is satisfied because the analysis team incorporates participants from both business units and the IT sector.
<i>Hold business units responsible</i>	
	Since the analysis team comprises people from the business sector, it is safe to assume that these people are conversant with the business processes and could therefore be held accountable for this aspect.
<i>Limit scope of individual assessments</i>	
	In phase 1, senior management pinpoints the operational areas to be included in the scale of the evaluation.
<i>Document and maintain results</i>	
	The results can be stored in a database for future reference and modification.
<i>Identify threats and the likelihood of those threats materialising</i>	
	In OCTAVE, participants examine threats to the top five assets that they have identified. OCTAVE has four predefined sources of threat (Alberts & Dorofee, 2003:94).
THREAT SOURCES	
Deliberate Actions by People	
<ul style="list-style-type: none"> ▣ People inside the organisation. ▣ People outside the organisation. 	
Accidental Actions by People	

(GAO:1999)	
<ul style="list-style-type: none"> ▣ People inside the organisation. ▣ People outside the organisation. 	
System Problems	
<ul style="list-style-type: none"> ▣ Hardware defects. ▣ Software defects. ▣ Unavailability of related systems. ▣ Viruses. ▣ Malicious code. ▣ Other. 	
Other Problems	
<ul style="list-style-type: none"> ▣ Power outages. ▣ Unavailability of water. ▣ Unavailability of telecommunications. ▣ Unavailability of ISP. ▣ Floods. ▣ Earthquakes. ▣ Other. 	
<p>The outcome of each threat materialising is also examined (Alberts & Dorofee, 2003:95).</p> <ul style="list-style-type: none"> ▣ Disclosure or viewing of sensitive information. ▣ Modification of important or sensitive information. ▣ Destruction or loss of important information, hardware or software. ▣ Interruption of access to important information. 	
<i>Identify and rank critical assets and operations</i>	
	<p>Asset identification is the very first activity of the knowledge elicitation workshop (phase 1, processes 1-3). The participants outline a general list of the assets used by the organisation. They then filter out the most important assets and provide a rationale for the selection of these particular assets.</p>

(GAO:1999)	
<i>Estimate potential damage</i>	
	It is possible to estimate the potential damage by virtue of frequency and subjective probability in phase 3, process 8 (Alberts & Dorofee, 2003:184).
<i>Identify cost-effective mitigating controls</i>	
	Based on the compilation of results from the risk impact assessment, the analysis team constructs a set of protection strategies, mitigation plans and a list of near-term item actions for the organisation under review (phase 3, process 8A).
<i>Document assessment findings</i>	
	<p>Outputs of OCTAVE include:</p> <ul style="list-style-type: none"> ▣ Asset-based threat profile. ▣ Organisation-wide protection strategy. ▣ Asset risk mitigation plan. ▣ Action list. ▣ Asset-based risk profile. ▣ Final report.
<i>Questionnaires</i>	
	In OCTAVE, there are a number of methods for eliciting the information requirements of users. Interviews are conducted with various members of the organisation from different hierarchical levels. Information is collected with the aid of <i>questionnaires</i> and surveys to be analysed by the analysis team. The following table is an example of a questionnaire to determine the assets that are most important to the OCTAVE participants (Alberts & Dorofee, 2003:365-367).
<p>Interview Questions – Asset Worksheet</p> <p>Process 1 – Identify Senior Management Knowledge</p> <p>Process 2 – Identify Operational Area Knowledge</p> <p>Process 3 – Identify General Staff Knowledge</p> <p>Process 3 – Identify IT Staff Knowledge</p>	
1. What are the important assets?	

(GAO:1999)

Consider:

- information*
- systems*
- software*
- hardware*
- people*

2. Are there any other assets that the department/service is required to protect (e.g., by law or regulation)?

3. What related assets are important to the department/service?

Consider:

- information*
- systems*
- software*
- hardware*
- people*

4. Of the assets that have been identified for the department/service, which are the most important? What is the rationale for selecting these assets as important?

Software to facilitate documentation and analysis



OCTAVE is a manual risk analysis approach and does not leverage the use of automated tools. This does not mean that a software tool cannot be created for the OCTAVE risk analysis methodology. The Advanced Technology Institute ("OCTAVE Automated", n.d) has created such a tool. (figure 9-1).

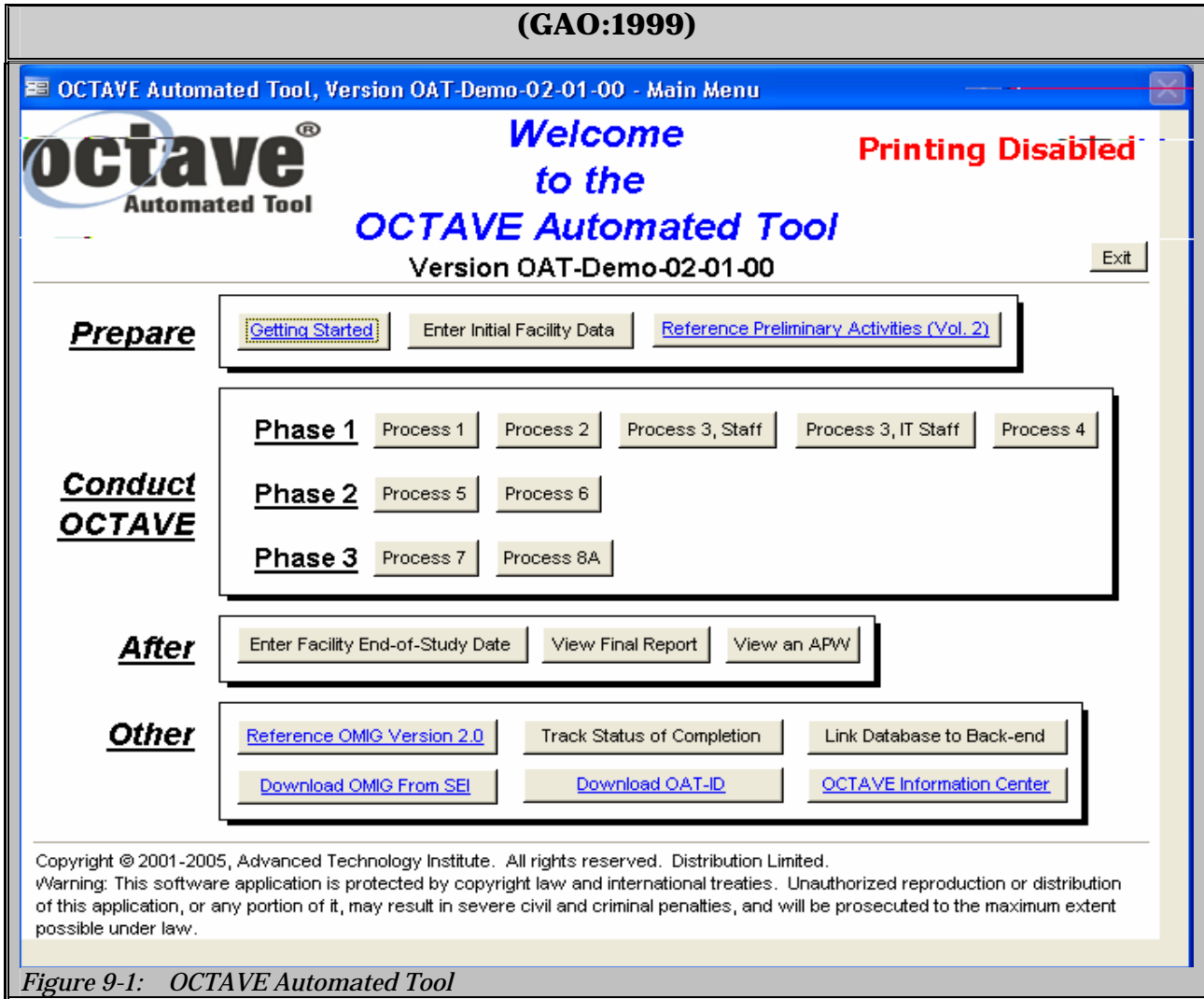


Table 9-1: Assessing the strength of the OCTAVE risk analysis methodology

10. APPENDIX B: ACTIVE AND PASSIVE WLAN DISCOVERY FOR SELECTED AREAS IN SOUTH AFRICA

10.1 ACTIVE WLAN DISCOVERY IN V & A WATERFRONT (CAPE TOWN) USING NETSTUMBLER

Active WLAN discovery is a relatively easy task accomplished by using:

- ▣ A portable computer.
- ▣ A wireless NIC.
- ▣ Software such as NetStumbler 0.4.0 ("NetStumbler", n.d.) (figure 10-1).

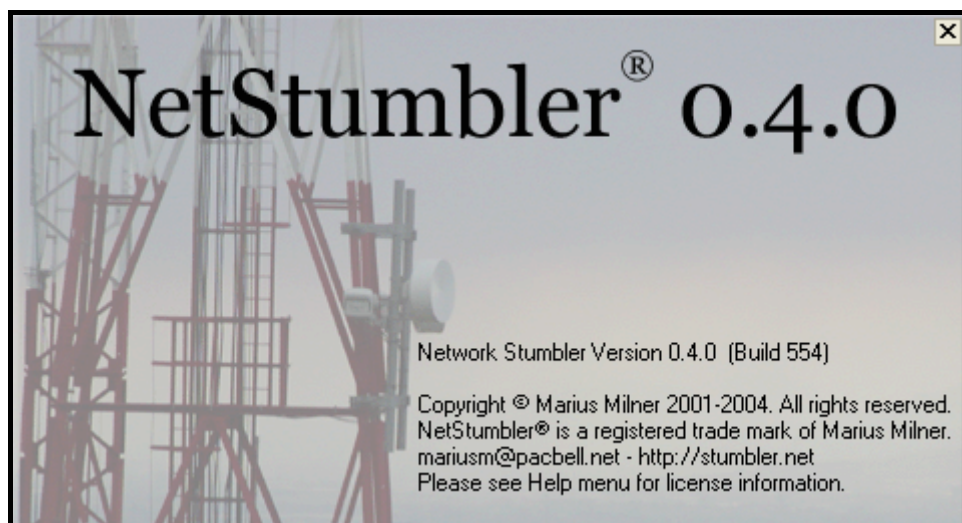


Figure 10-1: NetStumbler 0.4.0

- ▣ An optional external antenna to receive signals from greater distances and a global positioning system (GPS) to record the precise location where each AP is situated.

NetStumbler, authored by Marinus Milner, a freeware Windows utility that allows the detection of WLANs using 802.11b, 802.11a and 802.11g is probably the most extensively used wireless site survey tool (Cannon, 2006:115). NetStumbler operates by sending a probe-request signal from the wireless client to which APs within the signal range respond by broadcasting their beacon frames approximately every 10 milliseconds (Peikari & Fogie, 2003:29), provided they are configured to broadcast their SSIDs. NetStumbler works in concert with a GPS to map precise locations of identified WLANs and the resulting maps and data are posted on websites such as the Wigle website ("WiGLE-Wireless", n.d.).

The following diagram (figure 10-2) illustrates a subsection of a scan that was conducted at the V & A Waterfront area and surrounding areas, Cape Town by the researcher on 28th September 2005 at 10:30 using NetStumbler, an HP Compaq nx9010 notebook and a Cisco Aironet 350 series WNIC. NetStumbler provides detailed information about APs including the MAC address of the AP, the SSID, which is the WLAN's name, the radio channel in use, the vendor name, whether or not encryption has been enabled and the RF signal strength which is basically the signal-to-noise ratio.

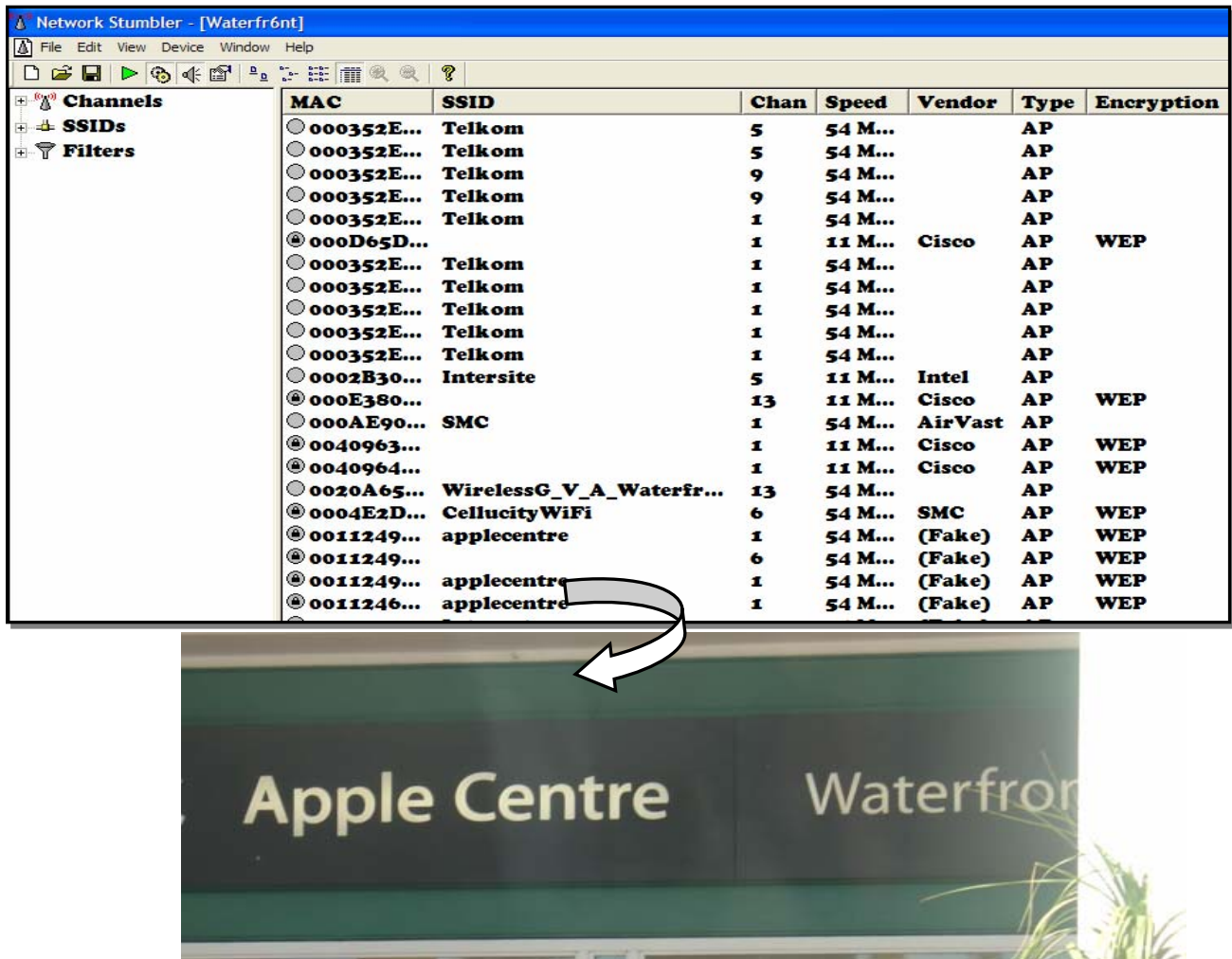


Figure 10-2: Active WLAN discovery at the V & A Waterfront, Cape Town using NetStumbler

The following diagram (figure 10-3) illustrates the signal-to-noise ratio of a particular AP depicting how strong the signal in this particular area is. WLAN intruders can use this information and look for where the signal increases and decreases to locate the base on the wireless network.

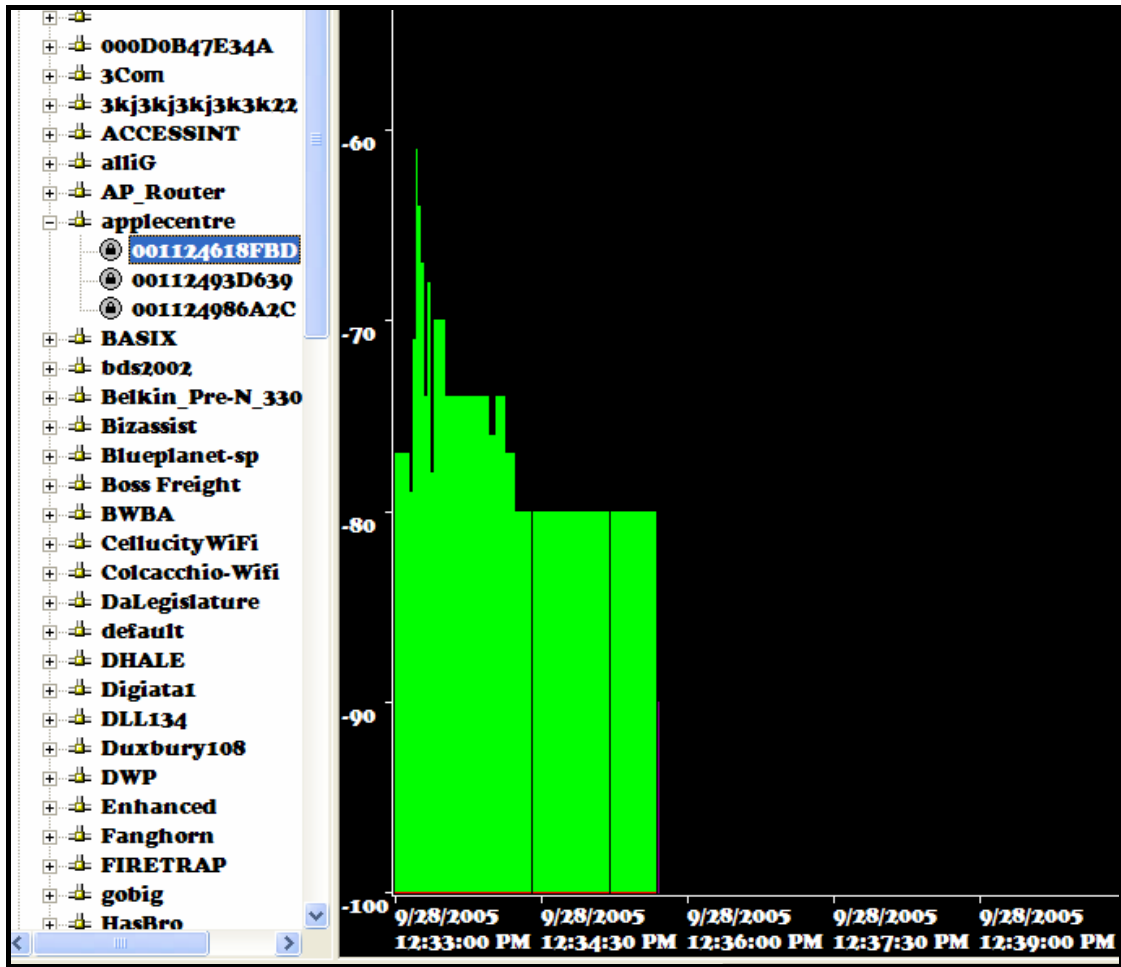


Figure 10-3: Signal-to-noise ratio

The filters facilitate distilling precise information about a particular AP. For illustrative purposes, the author has singled out all APs that do not have encryption enabled (figure 10-4).

MAC	SSID	Name	C...	Speed	Vendor	Type	Encryption
000FB599E...	NETGEAR		11	54 Mbps		AP	
001195BC8...	default		6	54 Mbps	(Fake)	AP	
000AE90A0...	Boss Freight		1	54 Mbps	AirVast	AP	
7AB0A8E1...	hpsetup		6	11 Mbps	(User-defined)	Peer	
001346606...	DHALE		6	54 Mbps	(Fake)	AP	
0050C2152...	Wireless		1	11 Mbps	IEEE Registr...	AP	
020225E36...	MNR		1	11 Mbps	(User-defined)	Peer	
7AC1387E...	SMC		1	54 Mbps	(User-defined)	Peer	
001195E4D...	default		6	54 Mbps	(Fake)	AP	
00095B4C2...	Wireless		6	11 Mbps	Netgear	AP	
020CF13D3...	SMC		1	54 Mbps	(User-defined)	Peer	
00022D4A0...			7	11 Mbps	Proxim (Age...	AP	
00904B0AF...	AP_Router		6	54 Mbps	Gemtek	AP	
0011958EF...	default		6	54 Mbps	(Fake)	AP	
5EC101A8E...	hpsetup		10	11 Mbps	(User-defined)	Peer	
000352E6E...	Telkom		11	54 Mbps		AP	
00095BA0B...	Colcacchio-Wifi		11	54 Mbps	Netgear	AP	
000352E77...	Telkom		1	54 Mbps		AP	
000352EA0...	Telkom		5	54 Mbps		AP	
000352EAE...	Telkom		5	54 Mbps		AP	
000352E9F...	Telkom		13	54 Mbps		AP	
000352ED1...	Telkom		5	54 Mbps		AP	
000352ED1...	Telkom		5	54 Mbps		AP	
000352ECA...	Telkom		9	54 Mbps		AP	
000352E9F...	Telkom		9	54 Mbps		AP	
000352EAF...	Telkom		1	54 Mbps		AP	
000352E9F...	Telkom		1	54 Mbps		AP	
000352E9F...	Telkom		1	54 Mbps		AP	
000352E9F...	Telkom		1	54 Mbps		AP	
000352EA0...	Telkom		1	54 Mbps		AP	

Figure 10-4: APs that do not have encryption enabled

Statistical Analysis: The researcher located the presence of 124 APs in a span of approximately 30 minutes. Of these 124 APs, 30 did not have WEP enabled (figure 10-5).

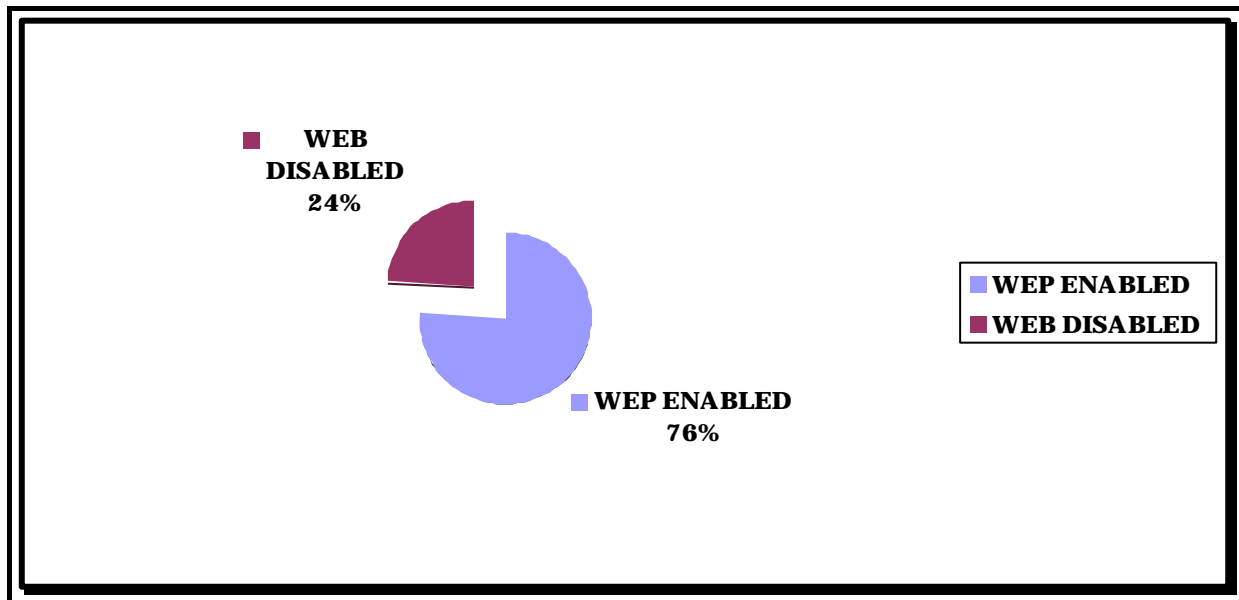
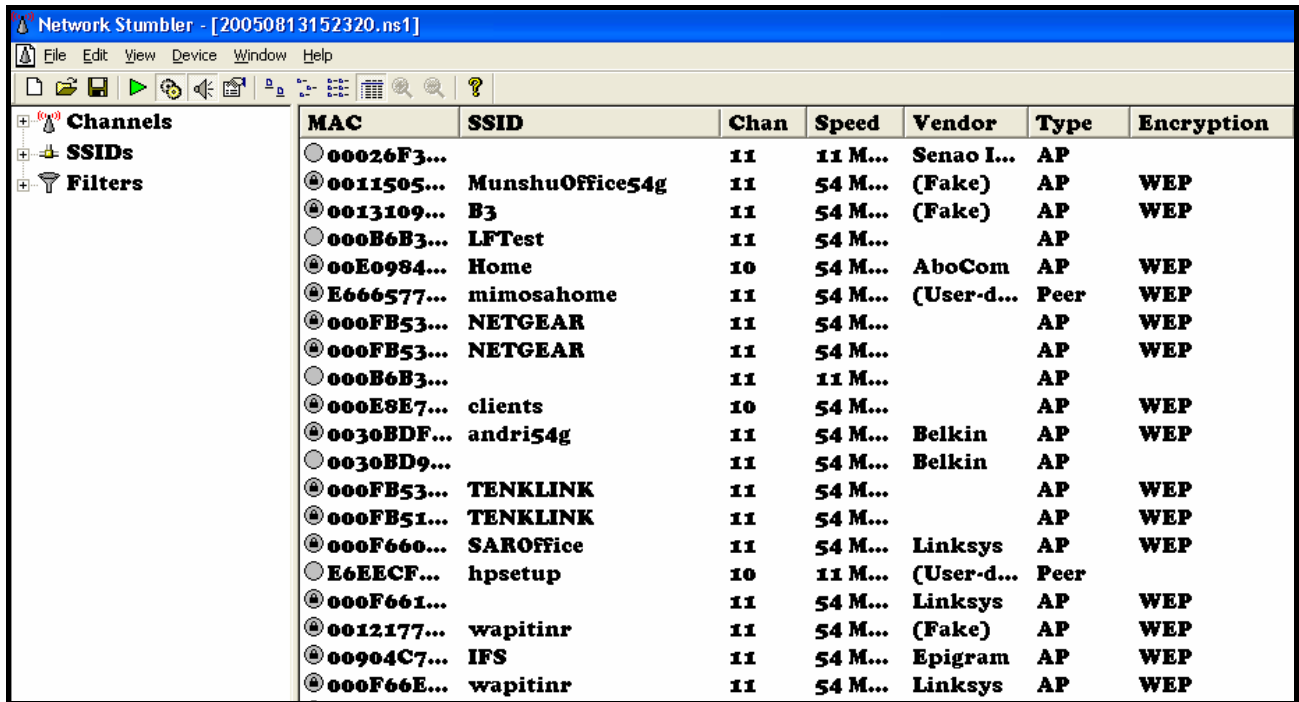


Figure 10-5: Statistical analysis of War driving at V & A Waterfront, Cape Town

Thus it can be inferred from the above statistical analysis that WLAN security is indeed a very critical problem.

10.2 ACTIVE WLAN DISCOVERY IN MIDRAND USING NETSTUMBLER

The following subsection of a NetStumbler log (figure 10-6) illustrates a typical WLAN discovery exercise conducted by Stephan Blanchard in the Midrand area, South Africa on 13th August 2005.



MAC	SSID	Chan	Speed	Vendor	Type	Encryption
00026F3...		11	11 M...	Senao I...	AP	
0011505...	MunshuOffice54g	11	54 M...	(Fake)	AP	WEP
0013109...	B3	11	54 M...	(Fake)	AP	WEP
000B6B3...	LFTest	11	54 M...		AP	
00E0984...	Home	10	54 M...	AboCom	AP	WEP
E666577...	mimosahome	11	54 M...	(User-d...	Peer	WEP
000FB53...	NETGEAR	11	54 M...		AP	WEP
000FB53...	NETGEAR	11	54 M...		AP	WEP
000B6B3...		11	11 M...		AP	
000E8E7...	clients	10	54 M...		AP	WEP
0030BDF...	andri54g	11	54 M...	Belkin	AP	WEP
0030BD9...		11	54 M...	Belkin	AP	
000FB53...	TENKLINK	11	54 M...		AP	WEP
000FB51...	TENKLINK	11	54 M...		AP	WEP
000F660...	SAROffice	11	54 M...	Linksys	AP	WEP
E6EECF...	hpsetup	10	11 M...	(User-d...	Peer	
000F661...		11	54 M...	Linksys	AP	WEP
0012177...	wapitinar	11	54 M...	(Fake)	AP	WEP
00904C7...	IFS	11	54 M...	Epigram	AP	WEP
000F66E...	wapitinar	11	54 M...	Linksys	AP	WEP

Figure 10-6: Active WLAN discovery in Midrand, South Africa using NetStumbler

The following diagram (figure 10-7) illustrates the number of APs that have retained their default SSIDs.

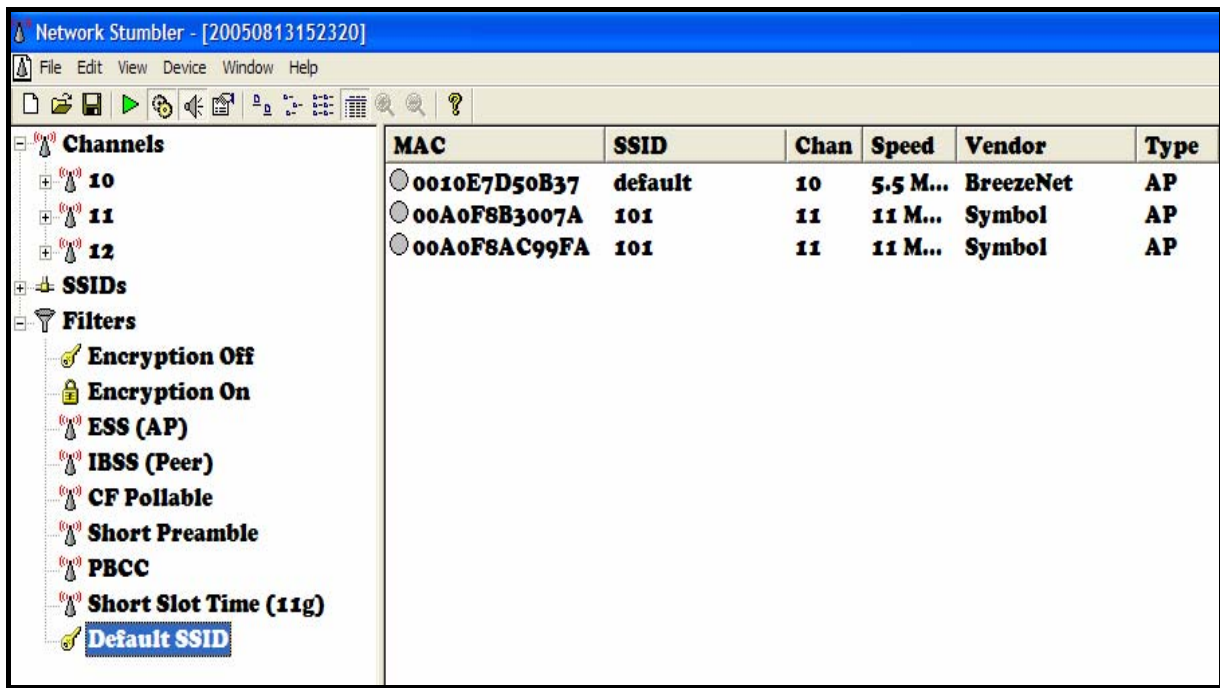


Figure 10-7: Example of APs that have retained their default SSIDs

It can again be deduced, that WLAN security is indeed cause for concern.

NetStumbler can also provide information on what type of WLAN network exists, i.e. infrastructure-based or peer-to-peer. The following diagram (figure 10-8) depicts how NetStumbler detected an ad hoc network created by the researcher.

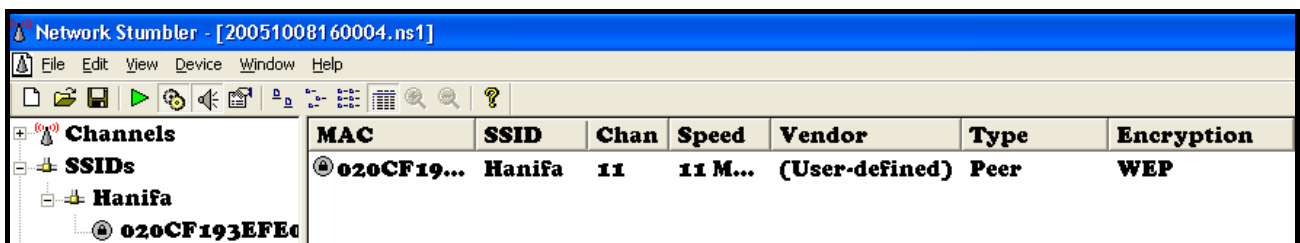


Figure 10-8: Using NetStumbler to detect the type of network

10.3 PASSIVE WLAN DISCOVERY IN EASTERN PRETORIA USING KISMET

NetStumbler is an active scanner, sending out probe requests and waiting for probe responses. This means that it will not detect networks that disable SSID broadcasting. This activity can be accomplished by using a passive scanner such as Kismet ("Kismet", n.d.), which runs on Linux or AirMagnet ("Enterprise Wireless", n.d.) which runs on Windows. Passive scanners can detect cloaked SSIDs and other devices probing APs without participating rendering it difficult to detect this type of intrusive activity (Sharma, 2004:116). It can identify clients that have associated to an AP (either by MAC addresses -

which are not encrypted, even with WEP-enabled WLANs) or IP addresses, and determine the manufacturer/model ID of the devices. The downside to passive scanners is that if an AP sends out beacon signals occasionally, the passive scanner will not pick up these APs (Howlett, 2005:328).

The following example provided by Nic Roets illustrates how APs are graphically mapped. Roets performed this WLAN scanning between 17th November 2004, scanning very small part of Eastern Pretoria. The following hardware was used:

- ▣ Notebook with 802.11b (BenQ JB 5000U).
- ▣ Entry level GPS (Garmin Etrex). The Garmin Etrex is the size of a large cellphone and is battery-powered. It locks on to the signals of the GPS satellites (about 1 minute). Thereafter it performs certain calculations and displays the location on it's black and white screen. It is accurate to about 4 metres when there are no obstructions. The GPS will then report the location to Kismet via the non-USB serial port.

The following software was used:

- ▣ The Gentoo-linux operating system.
- ▣ Kismet WLAN discovery which runs on Linux. Kismet creates a number of files, including Kismet.csv, a comma delimited file which can be exported into Excel (figure 10-9).
- ▣ Gpsbabel software to graphically map the location of APs and other wireless devices (including clients and active scanners) from Kismet to GoogleEarth (figure 10-10).

	A	B	C	D	E	F	G	H	I
174	Network	NetType	ESSID	BSSID	Info	Channel	Cloaked	WEP	Decrypt
175	21	infrastructure	Fort Knox	00:07:40:76:DA:09		3	No	Yes	No
176	9	infrastructure	G604T_WIRELESS	00:0F:3D:B9:A2:88		6	No	No	No
177	22	infrastructure	Greenfields Hatfield	00:E0:98:98:E0:66		3	No	No	No
178	19	probe	Greenfields Hatfield	00:11:0A:2B:5C:67		0	No	No	No
179	16	probe	home	00:E0:98:B5:41:6F		0	No	No	No
180	28	ad-hoc	hotel	02:02:06:08:61:50		6	No	No	No
181	8	infrastructure	IFS-Africa	00:E0:98:4F:58:5C		2	No	No	No
182	8	infrastructure	IFS-Africa	00:E0:98:4F:58:5C		2	No	No	No
183	15	infrastructure	IFS-Africa	00:E0:98:4F:58:5C		2	No	No	No
184	4	probe	ISIntCafe	00:0C:F1:35:36:1A		0	No	No	No
185	36	infrastructure	Jacques	00:90:4B:26:7D:F3		11	No	Yes	No
186	47	infrastructure	KlapWNNR	00:90:4B:63:43:45		5	No	Yes	No
187	22	infrastructure	KlapWNNR	00:90:4B:63:43:45		5	No	Yes	No
188	7	probe	Iarochelle	00:0C:F1:3D:F3:8C		0	No	No	No
189	43	infrastructure	LegalEDGE	00:0E:A6:9F:06:61		8	No	Yes	No
190	25	probe	LEGDE	00:A0:F8:6A:5B:B2		0	No	No	No
191	12	infrastructure	Leo2	00:0F:3D:DF:47:1A		6	No	No	No
192	5	infrastructure	linksys	00:0F:66:00:7D:8E		6	No	No	No
193	5	infrastructure	linksys	00:0F:66:00:7D:8E		6	No	No	No
194	10	infrastructure	linksys	00:06:25:ED:15:1F		11	No	No	No
195	14	infrastructure	linksys	00:06:25:C6:0B:94		11	No	No	No
196	1	infrastructure	Lynnwood Park	00:E0:98:4E:AD:04		1	No	No	No

Figure 10-9: Passive WLAN Discovery in Eastern Pretoria using Kismet



Figure 10-10: Graphical depiction of APs in Eastern Pretoria

10.4 ACTIVE AND PASSIVE WLAN DISCOVERY IN SUNNYSIDE, PRETORIA USING AIRMAGNET

To illustrate the differences between active and passive WLAN discovery, the researcher sampled a small area in Sunnyside, Pretoria on 10th October 2005 using a HP Compaq nx9010 notebook and a Cisco Aironet 350 series WNIC. Figure 10-11 illustrates active WLAN discovery using NetStumbler and figure 10-12 illustrates passive WLAN discovery using AirMagnet done at precisely the same time.

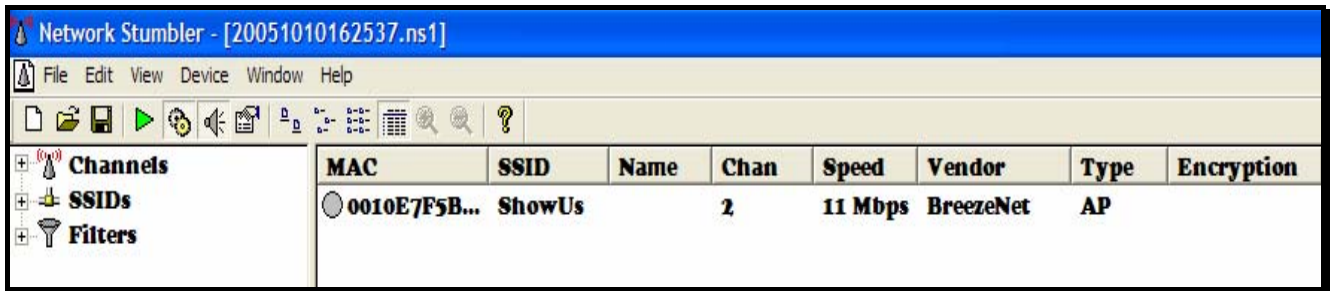


Figure 10-11: Active WLAN discovery in Sunnyside, Pretoria using NetStumbler

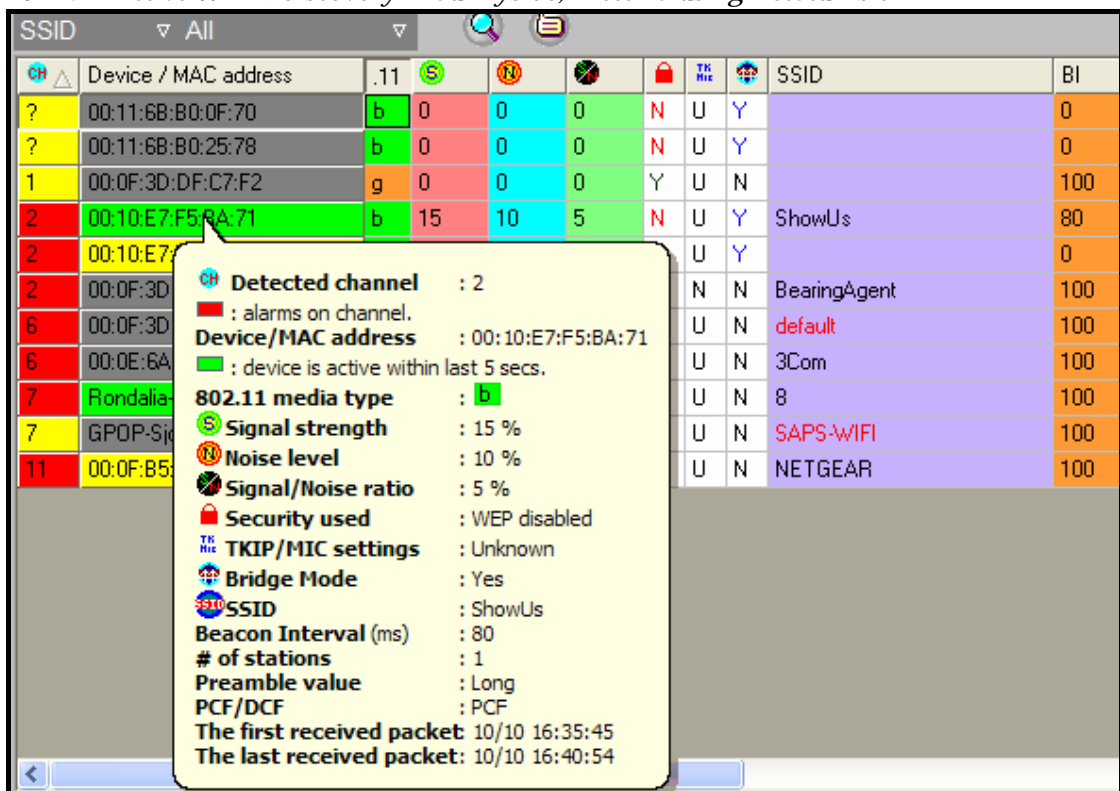


Figure 10-12: Passive WLAN discovery in Sunnyside, Pretoria using AirMagnet

Figures 10-11 and 10-12 make it unmistakably clear that passive WLAN discovery reveals much more information than active WLAN discovery and actually detects APs that have cloaked SSIDs. Both NetStumbler and AirMagnet detected the AP with SSID *ShowUs* since

this AP is configured to broadcast its SSID. AirMagnet, however detected several other APs that were not detected by NetStumbler.

11. APPENDIX C: WLAN INTRUSION SECURITY ORGANISATIONAL KNOWLEDGE

11.1 KNOWLEDGE ELICITATION

This activity requires that staff from different hierarchical levels of the organisation contributes their perspectives on what they regard as being the most important assets, what is currently being done to protect these assets and what organisational vulnerabilities exist. The information stated above is obtained via structured interviews and workshops. Since one of the premises of the OODA cycle entails moving through the OODA cycle faster than the intruder, this laborious and time-consuming can be eliminated, since all this information can be retrieved from studying the WLAN operating environment and the OODA cycle of the WLAN intruder as well as the organisations own susceptibility to WLANs intrusion security risks.

The information required for the WLAN intrusion security organisational knowledge elicitation process is stored in the database. The following activities are undertaken during this phase (Alberts & Dorofee, 2003:47):

11.1.1 IDENTIFY THE MOST IMPORTANT ASSETS

Having a basic understanding of WLANs is particularly important to an organisation since this highlights what *assets* are important and worth defending.

Assets broadly fall into the following categories (Alberts & Dorofee, 2003:88):

- Information-documented (paper or electronic) information or intellectual assets used to meet the mission of the organisation.
- Systems—information systems that process and store information. Systems are a combination of information, software, and hardware assets. Any host, client, server, or network can be considered a system.
- Software—software applications such as operating systems, database applications, networking software, office applications and custom applications.
- Hardware—information technology physical devices.
- People—the people in the organisation, including their skills, training, knowledge and experience.

By studying the WLAN operating environment the following important system asset has been identified (figure 11-1):

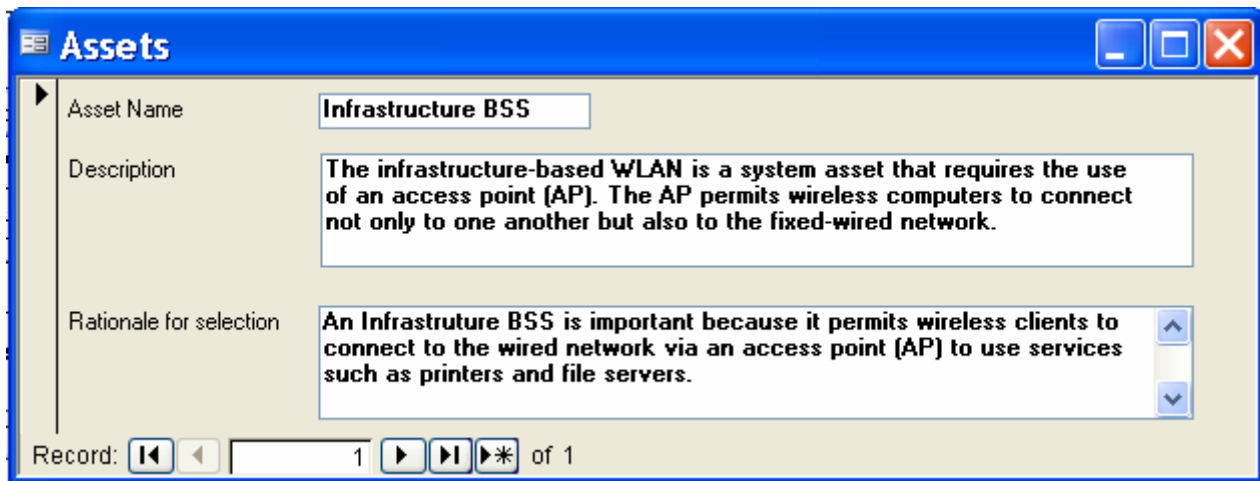


Figure 11-1: Identify the most important assets

11.1.2 IDENTIFY AREAS OF CONCERN

Scenarios that threaten the most important assets based on typical sources and outcomes of threats are constructed.

The sources include (Alberts & Dorofee, 2003:95):

- ▣ Deliberate actions by people—This group includes people inside and outside the organisation who might take deliberate action against the assets.
- ▣ Accidental actions by people—This group includes people inside and outside the organisation who inadvertently harm the assets.

The threat outcomes fall into the following categories (Alberts & Dorofee, 2003:95):

- ▣ Disclosure or viewing of sensitive information.
- ▣ Modification of important or sensitive information.
- ▣ Destruction or loss of important information, hardware or software.
- ▣ Interruption of access to important information, software, applications or services.

The following nine areas of concern have been identified (figures 11-2 to 11-10).

AreasofConcern

Assets: Infrastructure BSS

Type of threat: Human actors using wireless access

Describe area of concern: A rogue AP can cause a man-in-the middle attack, session hijacking attack and a denial-of-service (DOS) attack. All these types of attack can compromise the confidentiality and integrity of information by capturing the users credentials and hijacking the users session. The DOS attack can also lead to an interruption of service.

Outcome(s):

- Disclosure
- Modification
- Loss/Destruction
- Interruption

Record: 1 of 9

Figure 11-2: First area of concern

AreasofConcern

Assets: Infrastructure BSS

Type of threat: Human actors using wireless access

Describe area of concern: Passive and active WLAN discovery and brute force probes can violate the confidentiality of the user session because the WLAN intruder listens to the network transmission in a bid to acquire information flowing from the wireless client to the APs. Leakage can occur when an AP that emanates a strong signal that filtrates into the air space of a neighbouring WLAN can cause the wireless clients of the neighbouring WLAN to associate with it and reveal sensitive information.

Outcome(s):

- Disclosure
- Modification
- Loss/Destruction
- Interruption

Record: 2 of 9

Figure 11-3: Second area of concern

Assets Infrastructure BSS

Type of threat Human actors using wireless access

Describe area of concern
Cyclic Redundancy Checks do not provide any means of ensuring the integrity of a data stream that has been corrupted by a WLAN intruder. If a WLAN intruder has knowledge of a certain data stream, it is possible to change the contents and successfully complete the transaction with a legitimate checksum. The receiver would have no knowledae of this because the checksum would match.

Outcome(s)

Disclosure Modification

Loss/Destructi Interruption

Record: 3 of 9

Figure 11-4: Third area of concern

Assets Infrastructure BSS

Type of threat Human actors using wireless access

Describe area of concern
Luring unsuspecting WLAN users to disclose their usernames and passwords in order to gain illicit entry into the network can compromise the confidentiality and integrity of information because the user will have access to the legitimate users information and can modify this information at will.

Outcome(s)

Disclosure Modification

Loss/Destructi Interruption

Record: 4 of 9

Figure 11-5: Fourth area of concern

Assets Infrastructure BSS

Type of threat Human actors using wireless access

Describe area of concern A Denial-of service attack is specifically aimed at denying legitimate users access to system resources. This leads to an interruption of service and the loss/destruction of data.

Outcome(s)

Disclosure Modification

Loss/Destruction Interruption

Record: 5 of 9

Figure 11-6: Fifth area of concern

Assets Infrastructure BSS

Type of threat Human actors using wireless access

Describe area of concern MAC addresses are broadcast in plain text by WEP during packet transfer. A WLAN intruder can capture a valid MAC address by eavesdropping and then programing his/her card to have the identical MAC address and successfully gain free rein entry to the WLAN as a legitimate user. The WLAN intruder can view the confidential information of the legitimate user leading to information disclosure.

Outcome(s)

Disclosure Modification

Loss/Destruction Interruption

Record: 6 of 9

Figure 11-7: Sixth area of concern

The screenshot shows the 'AreasofConcern' application window. The 'Assets' dropdown is set to 'Infrastructure BSS'. The 'Type of threat' is 'Human actors using wireless access'. The 'Describe area of concern' text box contains the text: 'Stealing a WLAN card with a pre-programmed MAC address, as allowed on the AP and then using this card to obtain illicit entry into the network violates the confidentiality and integrity of information.' The 'Outcome(s)' section has four checkboxes: 'Disclosure' (checked), 'Modification' (checked), 'Loss/Destruction' (unchecked), and 'Interruption' (unchecked). The record navigation bar shows 'Record: 7 of 9'.

Figure 11-8: Seventh area of concern

The screenshot shows the 'AreasofConcern' application window. The 'Assets' dropdown is set to 'Infrastructure BSS'. The 'Type of threat' is 'Human actors using wireless access'. The 'Describe area of concern' text box contains the text: 'The IV problems of WEP make it possible to view the plaintext of a message, compromising the confidentiality of information.' The 'Outcome(s)' section has four checkboxes: 'Disclosure' (checked), 'Modification' (unchecked), 'Loss/Destruction' (unchecked), and 'Interruption' (unchecked). The record navigation bar shows 'Record: 8 of 9'.

Figure 11-9: Eight area of concern

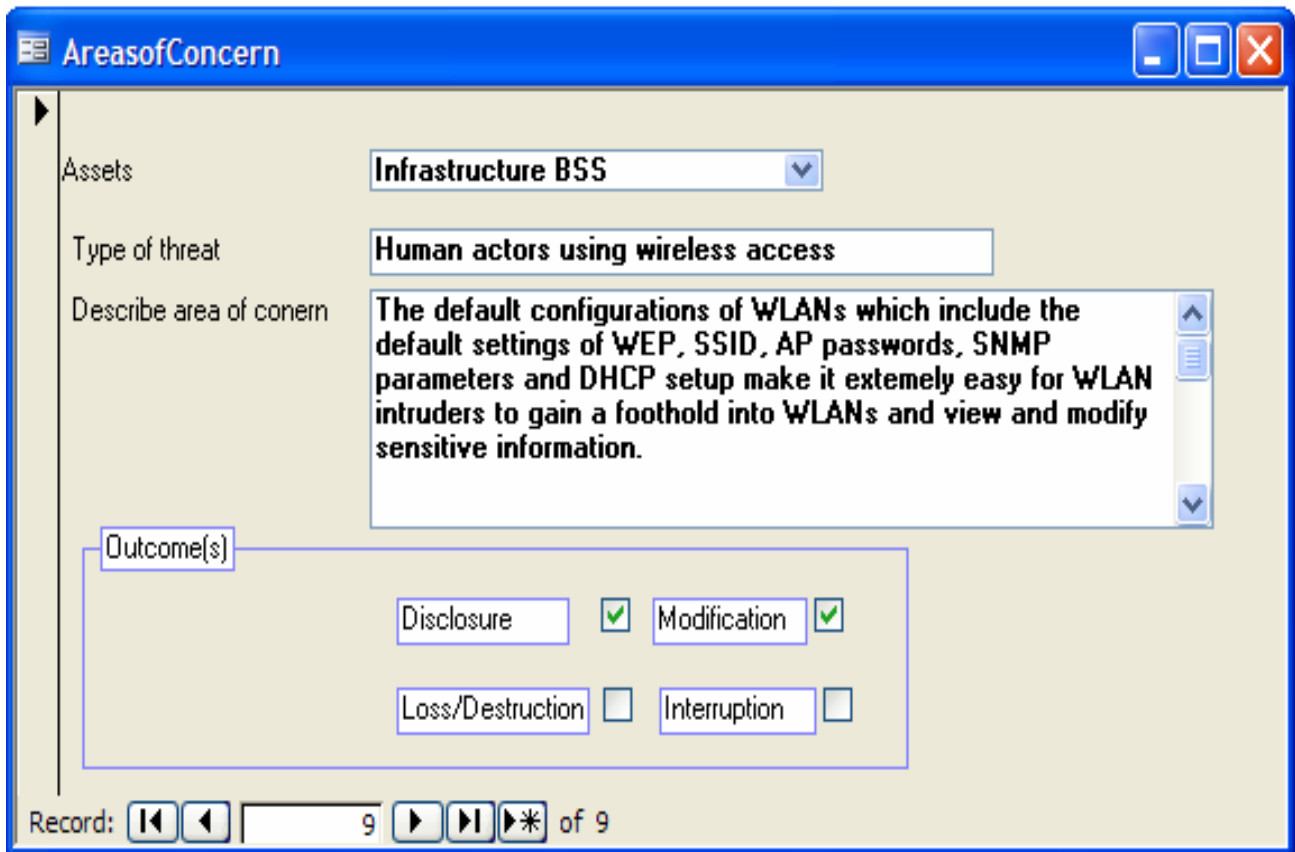


Figure 11-10: Ninth area of concern

Although 802.1x is also subject to man-in-the middle attacks and session hijacking attacks, (section 4.5.2.4), this is not a major concern for the University as the University has the EAP-FAST encryption scheme which is quite a robust encryption scheme. EAP-FAST helps prevent man-in-the-middle attacks, dictionary attacks, packet and authentication forgery attacks ("AirMagnet Enterprise", 2005, 141). A man-in-the-middle attack is therefore not a major cause for concern. TKIP is also prone to man-in-the-middle attacks (Table 4-1) but not a major cause for concern as EAP-FAST prevents this type of attack.

11.1.3 IDENTIFY SECURITY REQUIREMENTS FOR THE MOST IMPORTANT ASSETS

The security requirement for the crucially identified asset (infrastructure BSS) (figure 11-11 to 11-13) is documented. The security requirements outline the qualities of an asset that are important to safeguard. The security requirements include (Alberts & Dorofee, 203:98):

- ▣ Confidentiality—Safeguarding information from people who are not authorised to view this information.
- ▣ Integrity—Ensuring the authenticity, accuracy and completeness of an asset.
- ▣ Availability—Denoting when or how often an asset must be present or ready for use.

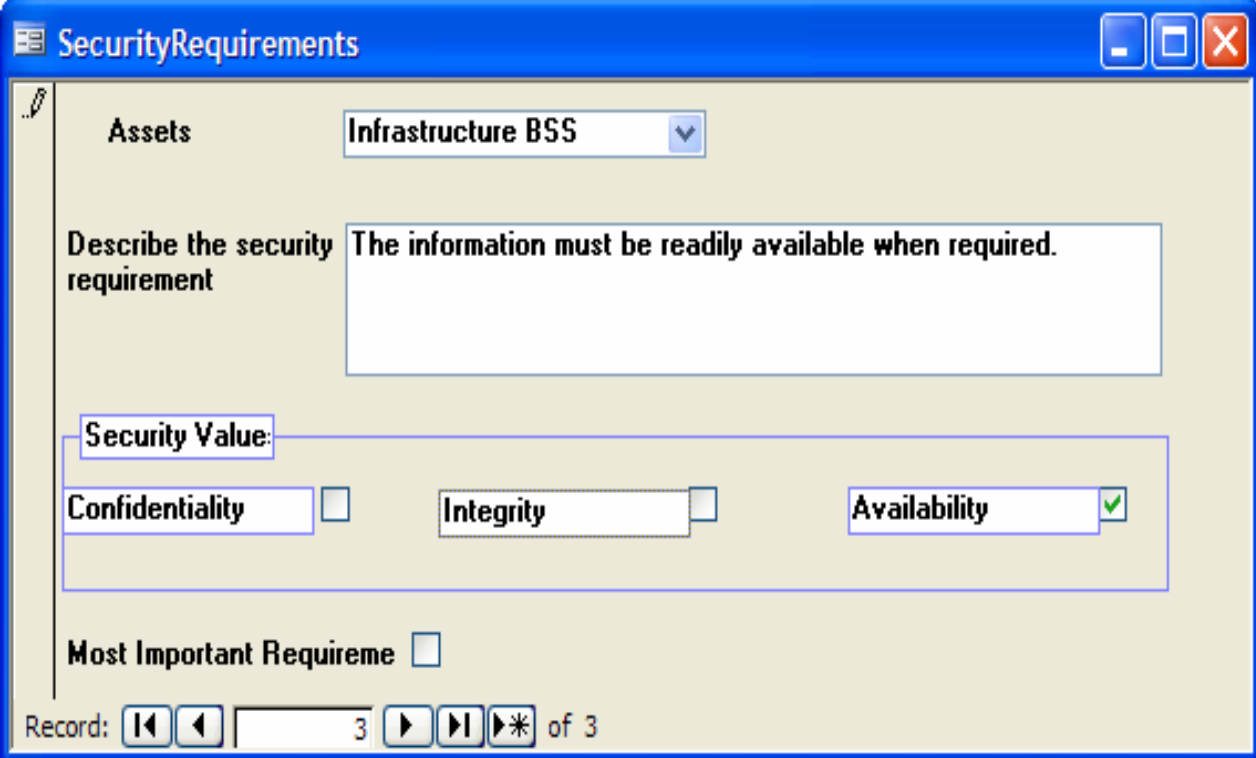
All of the security requirements are equally important. No requirement is selected as being the most important. The nine areas of concern (figures 11-2 to 11-10) have illustrated how these requirements can be compromised.

The screenshot shows a window titled "SecurityRequirements" with a blue title bar. The "Assets" dropdown menu is set to "Infrastructure BSS". The "Describe the security requirement" text box contains the text: "The information which includes the University's human resources, student academic records and financial records must be complete and accurate." Below this, the "Security Values" section has three checkboxes: "Confidentiality" (unchecked), "Integrity" (checked), and "Availability" (unchecked). The "Most Important Requirement" checkbox is also unchecked. At the bottom, the "Record:" indicator shows "1 of 3".

Figure 11-11: Security requirement in respect of integrity

The screenshot shows the same "SecurityRequirements" window. The "Assets" dropdown menu is still "Infrastructure BSS". The "Describe the security requirement" text box contains the text: "The information must be protected from disclosure and is only read by people who are authorised to read the information." In the "Security Values" section, the checkboxes are: "Confidentiality" (checked), "Integrity" (unchecked), and "Availability" (unchecked). The "Most Important Requirement" checkbox remains unchecked. The "Record:" indicator at the bottom now shows "2 of 3".

Figure 11-12: Security requirement in respect of confidentiality



The screenshot shows a window titled "SecurityRequirements" with a blue title bar. Inside the window, there is a form with the following elements:

- Assets:** A dropdown menu showing "Infrastructure BSS".
- Describe the security requirement:** A text box containing the text "The information must be readily available when required."
- Security Value:** A section containing three checkboxes: "Confidentiality" (unchecked), "Integrity" (unchecked), and "Availability" (checked with a green checkmark).
- Most Important Requireme:** A checkbox that is unchecked.
- Record:** A navigation bar at the bottom showing "Record: 3 of 3" with navigation icons for first, previous, next, last, and refresh.

Figure 11-13: Security requirement in respect of availability

11.1.4 CAPTURE KNOWLEDGE OF CURRENT SECURITY PRACTICES AND ORGANISATIONAL VULNERABILITIES

The following figure (figures 11-14 to 11-15) outlines the current security practices and organisational vulnerabilities of the University. *Organisational vulnerabilities* connote weaknesses in the organisational policy or practice that could manifest in unauthorised action (Alberts & Dorofee, 2003:105).

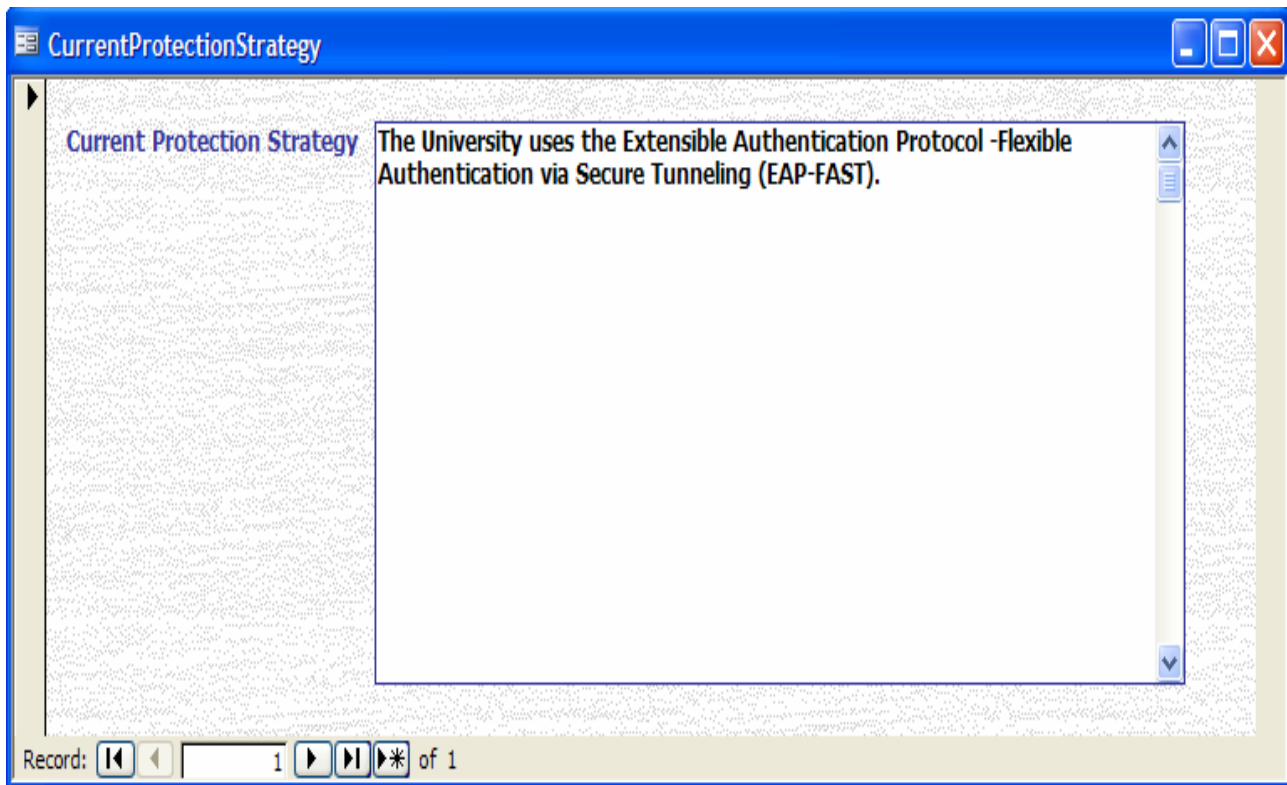


Figure 11-14: Current protection strategy

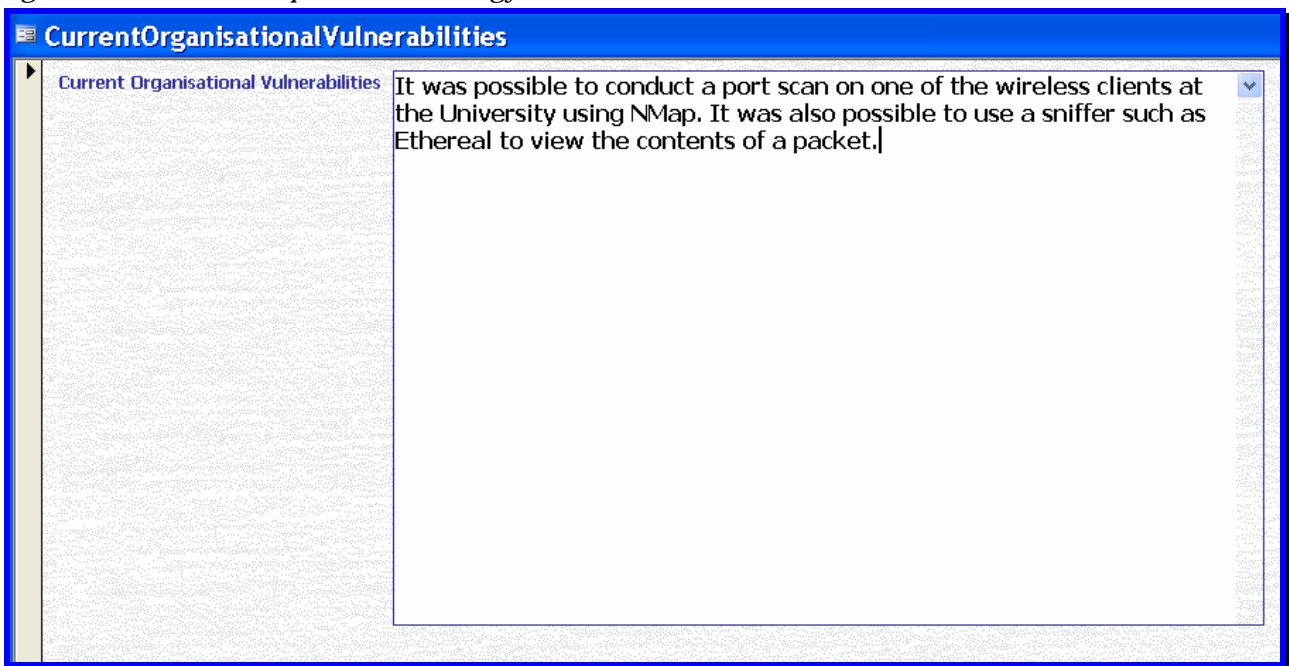


Figure 11-15: Current organisational vulnerabilities

12. APPENDIX D: WLAN ENTERPRISE-WIDE PROTECTION STRATEGY

Sections 12.1 and 12.2 cover the development of a WLAN enterprise-wide protection strategy for the University. The catalog of practices calibrated for a WLAN educational operating environment consists of two sections reflecting the strategic and operational best practices for the University. This catalog is constructed from references that were used in the original compilation of the Catalog of Practices (Alberts & Dorofee, 2003:443-445):

- ▣ British Standards (British Standards Institution, February).
- ▣ Gramm-Leach Bliley Act of 1999 ("Interagency", 2001).
- ▣ Health Insurance Portability and Accountability Act (HIPAA) of 1996 ("Security Standards", 1998).
- ▣ NIST Principles and Practices (Swanson & Guttman, 1996).
- ▣ The Cert Guide to System and Network Security Practice (Allen, 2001).

To update the catalog for a WLAN operating environment, the following references were consulted:

- ▣ Wireless Network Security: 802.11, Bluetooth and Handheld Devices. Online. NIST Special Publication 800-48. (Karygiannis & Owens, n.d:40-42).
- ▣ Wireless Policy Development (Part 1-2) (Farshchi^a, 2003; Farshchi^b, 2003).

12.1 STRATEGIC PRACTICES

WLAN SECURITY AWARENESS AND TRAINING
All WLAN users fully comprehend their respective security roles and responsibilities.
There is adequate in-house expertise for all supported services, mechanisms and technologies (e.g., logging, monitoring, or encryption) including their secure operation.
Ensure that WLAN users on the network are fully trained in computer security awareness and the risks associated with wireless technology. Periodic reminders must be provided to all WLAN users.
WLAN technology users' understanding of security information is documented and conformance is periodically verified.

Table 12-1: WLAN security awareness and training

WLAN SECURITY STRATEGY
The University's strategies routinely incorporate WLANs security considerations.
WLANs security strategies and policies take into consideration the University's mission, strategies and goals.
WLANs security strategies, goals and objectives are documented and are routinely reviewed, updated and communicated to all members of the University.

Table 12-2: WLAN security strategy

WLAN SECURITY MANAGEMENT
Management allocates sufficient funds and resources to WLANs information security activities.
Security roles and responsibilities are defined for all wireless users within the university.
Develop an agency security policy that addresses the use of wireless technology, including 802.11.
The University's hiring and termination practices for personnel take WLANs information security issues into account.
The required levels of information security regarding WLANs and how they are applied to individuals and groups are documented and enacted.
The University manages WLANs information security risks, including: <ul style="list-style-type: none"> ▣ Assessing risks to information security to comprehend the value of the assets that require protection.

WLAN SECURITY MANAGEMENT
<ul style="list-style-type: none"> ■ Taking steps to mitigate information security risks. ■ Maintaining an acceptable level of risk. ■ Using information security risk assessments to help select cost-effective security/control measures, balancing implementation costs against potential losses.
<p>Management receives and acts upon routine reports summarising the results of:</p> <ul style="list-style-type: none"> ■ Review of system logs. ■ Review of audit trails. ■ Technology vulnerability assessments. ■ Security incidents and the responses to them. ■ Risk assessments. ■ Physical security reviews. ■ Security improvement plans and recommendations.
<p>Ensure that wireless networks are not used until they comply with the agency's security policy.</p>

Table 12-3: WLAN security management

WLAN SECURITY POLICIES AND REGULATIONS
<p>The University has a comprehensive set of documented, current security policies that are periodically reviewed and updated. These policies address key security topic areas, including:</p> <ul style="list-style-type: none"> ■ WLANs security strategy and management. ■ WLANs security risk management. ■ System and network management. ■ System administration tools. ■ Monitoring and auditing. ■ Authentication and authorisation. ■ Vulnerability management. ■ Encryption. ■ Security architecture and design. ■ Incident management. ■ Staff security practices. ■ Applicable laws and regulations.

WLAN SECURITY POLICIES AND REGULATIONS
<ul style="list-style-type: none"> ■ Awareness and training. ■ Collaborative information security. ■ Contingency planning and disaster recovery.
<p>There is a documented process for management of security policies, including:</p> <ul style="list-style-type: none"> ■ Creation. ■ Administration (including periodic reviews and updates). ■ Communication.
<p>The University has a documented process for evaluating and ensuring compliance with information security policies for WLANs, applicable laws and regulations and insurance requirements.</p>
<p>The University uniformly enforces its security policies.</p>
<p>Testing and revision of security policies and procedures are restricted to authorised personnel.</p>

Table 12-4: WLAN security policies and regulations

COLLABORATIVE SECURITY MANAGEMENT
<p>The University has policies and procedures for protecting information when working with external institutions.</p>
<p>The University has verified that outsourced security services, mechanisms and technologies meet its security needs and requirements.</p>
<p>The University documents, monitors and enforces protection strategies for information belonging to external universities that is accessed from its own infrastructure components or is used by its own personnel.</p>
<p>The University provides and verifies awareness and training on applicable external universities' security policies and procedures for personnel who are involved with those external institutions.</p>
<p>There are documented procedures for external personnel whose services have been terminated specifying appropriate security measures for ending their access. These procedures are communicated and coordinated with the external university.</p>

Table 12-5: Collaborative security management

CONTINGENCY PLANNING/DISASTER RECOVERY
An analysis of operations, applications, and data criticality has been performed.
The University has documented: <ul style="list-style-type: none"> ▣ Business continuity or emergency operation plans. ▣ Disaster recovery plan(s). ▣ Contingency plan(s) for responding to emergencies.
The contingency, disaster recovery and business continuity plans consider physical and electronic access requirements and controls.
The contingency, disaster recovery and business continuity plans are periodically reviewed, tested and revised.
All personnel needed to participate are: <ul style="list-style-type: none"> ▣ Aware of the contingency, disaster recovery and business continuity plans. ▣ Understand and are able to carry out their responsibilities.

Table 12-6: Contingency planning/disaster recovery

12.2 OPERATIONAL PRACTICES

INFORMATION TECHNOLOGY SECURITY SYSTEM AND WLAN MANAGEMENT
There are documented security plans(s) for safeguarding the system and WLANs.
Security plan(s) are periodically reviewed, tested and updated.
Sensitive information is protected by secure storage such as: <ul style="list-style-type: none"> <input type="checkbox"/> Defined chains of custody. <input type="checkbox"/> Removable storage media. <input type="checkbox"/> Discard process for sensitive information or its storage media.
The integrity of installed software is regularly verified.
All systems are up to date with respect to revisions, patches and recommendations in security advisories.
There is a documented data backup plan that: <ul style="list-style-type: none"> <input type="checkbox"/> Is routinely updated. <input type="checkbox"/> Is periodically tested. <input type="checkbox"/> Calls for regularly scheduled backups of both software and data. <input type="checkbox"/> Requires periodic testing and verification of the ability to restore from backups.
All WLAN users understand and are able to carry out their responsibilities under the backup plans.
Changes to IT hardware and software are planned, controlled and documented.
IT staff members follow procedures when issuing, changing and terminating users' passwords, accounts and privileges: <ul style="list-style-type: none"> <input type="checkbox"/> Unique user identification is required for all information system users, including third-party users. <input type="checkbox"/> Default accounts and default passwords have been removed from systems.
Only necessary services are running on systems; all unnecessary services have been removed.

Table 12-7: Information technology security system and WLAN management

WLAN SECURITY SYSTEM ADMINISTRATION AND TOOLS

New security tools, procedures and mechanisms regarding WLANs are routinely reviewed for applicability in meeting the University's security strategies.

Tools and mechanisms for secure system and WLAN administration are used, routinely reviewed and updated or replaced. Examples include:

- Data integrity checkers.
- Cryptographic tools.
- Vulnerability scanners.
- Password quality-checking tools.
- Virus scanners.
- Process management tools.
- Intrusion detection systems.
- Secure remote administrations.
- Network service tools.
- Traffic analysers.
- Incident response tools.
- Forensic tools for data analysis.

Table 12-8: WLAN security system administration and tools

WLAN SECURITY MONITORING AND AUDITING

System and network monitoring and auditing tools are routinely used by the University.

- Activity is monitored by the IT staff.
- System and network activity is logged/recorded.
- Logs are reviewed on a regular basis.
- Unusual activity is dealt with according to the appropriate policy or procedure.
- Tools are periodically reviewed and updated.

Firewall and other security components are periodically audited for compliance with policy.

Table 12-9: WLAN security monitoring and auditing

WLAN AUTHENTICATION AND AUTHORISATION
Appropriate access controls and user authentication (e.g., file permissions, network configuration) consistent with policy are used to restrict user access to:
<ul style="list-style-type: none"> ■ Information. ■ Systems utilities. ■ Program source code. ■ Sensitive systems. ■ Specific applications and services. ■ WLAN connections within the University. ■ WLAN connections from outside the University.
Access control methods/mechanisms restrict access to resources according to the access rights determined by policies and procedures.
Access control methods/mechanisms are periodically reviewed and verified.
Methods or mechanisms are provided to ensure that sensitive information has not been accessed, altered or destroyed in an unauthorised manner.
Authentication mechanisms are used to protect the availability, integrity and confidentiality of sensitive information.
User authentication such as biometrics, smart cards, two-factor authentication and Public Key Infrastructure (PKI) is deployed. Biometrics can prove a user's identity before the user connects to the WLAN. PKI can ensure the integrity of the wireless transmission and ascertain who sent the message.
User authentication mechanisms for the management interfaces of the AP is enabled.
Auditing technology to analyse the records produced by RADIUS for suspicious activity is deployed.
Other forms of authentication for the wireless network such as 802.1x for port-based authentication and key distribution via an external authentication server such as RADIUS and Kerberos are considered. Kerberos is used to identify the identity of network users.
Enable utilisation of key-mapping keys (802.1x) rather than default keys so that sessions use distinct WEP keys.

Table 12-10: WLAN authentication and authorisation

WLAN SECURITY: ENCRYPTION
Appropriate security controls are used to protect sensitive information while in storage and during transmission, including:
<ul style="list-style-type: none"> ■ Data encryption during transmission. ■ Data encryption when writing to disk. ■ Use of public key infrastructure. ■ Virtual private network technology. ■ Encryption for all Internet-based transmission.
Encrypted protocols are used when remotely managing systems, routers and firewalls.
Encryption controls and protocols are routinely reviewed, verified and revised.
All security features of the WLAN product, including the cryptographic authentication and WEP privacy features are enabled. Use WEP for minimal protection when using legacy devices.
Ensure that the encryption key sizes are at least 128-bits or as large as possible.
Ensure that the encryption being used is sufficient given the sensitivity of the data on the network and the processor speeds of the computers.
AP management traffic security is enhanced by using SNMPv3 or equivalent cryptographically protected protocol.
An 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorisation features is deployed.
Use TKIP to prevent key-scheduling attacks.
Use WPA with TKIP as a secure means for encrypting the WLAN. TKIP can provide message integrity verification.
Use 802.11i with AES for the most robust form of protection if it is available on the AP.

Table 12-11: WLAN security: Encryption

WLAN SECURITY ARCHITECTURE AND DESIGN
System architecture and design for new and revised systems include consideration of:
<ul style="list-style-type: none"> ■ Security strategies, policies and procedures. ■ History of security compromises. ■ Results of security risk assessments.
The University has up-to-date diagrams that show the WLAN architecture and network topology.

Table 12-12: WLAN security architecture and design

WLAN SECURITY INCIDENT MANAGEMENT
Documented procedures exist for identifying, reporting and responding to suspected security incidents and violations, including: <ul style="list-style-type: none"> ▣ WLANs-based incidents. ▣ Social engineering incidents.
Incident management procedures are periodically tested, verified and updated.
There are documented policies and procedures for working with law-enforcement agencies.

Table 12-13: WLAN security: Incident management

STAFF SECURITY GENERAL STAFF PRACTICES
All WLAN users follow good security practice, such as: <ul style="list-style-type: none"> ▣ Securing information for which they are responsible. ▣ Not divulging sensitive information to others (resistance to social engineering). ▣ Having adequate ability to use information technology hardware and software. ▣ Using good password practices. ▣ Understanding and following security policies and regulations. ▣ Recognising and reporting incidents.
All staff at all levels of responsibility implement their assigned roles and responsibility for information security.
There are documented procedures for authorising and overseeing all personnel (including individuals from third-party universities) who work with sensitive information or who work in locations where the information resides. This includes: <ul style="list-style-type: none"> ▣ Employees ▣ Contractors, partners, collaborators and personnel from third-party universities. ▣ Systems maintenance personnel. ▣ Facilities maintenance personnel.

Table 12-14: General staff practices

TECHNICAL AND OPERATIONAL RECOMMENDATIONS
Empirically test AP range boundaries to determine the precise extent of the wireless coverage.
Make sure that APs are turned off when they are not used (e.g. after hours and on weekends).
Make sure that the reset function on APs is used only when needed and is only invoked by an authorised group of people.
Restore the APs to the latest security settings when the reset functions are used.
Place APs in secured areas to prevent unauthorised physical access and user manipulation. Mount APs out of reach and out of plain view. Bolt them down securely in locked steel enclosures.
Ensure that AP channels are at least five channels removed from any other nearby wireless networks to prevent interference.
When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.
Disable all insecure and nonessential management protocols on the APs.
Change the default SSID in the APs.
Disable the broadcast SSID feature, so that the client SSID must match that of the AP.
Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products.
Ensure that all APs have strong administrative passwords and that the passwords are changed regularly.
If the access point supports logging, turn it on and review the logs on a regular basis. This can be used to determine tracking of user activities and misuse detection.
Take a complete inventory of all APs and 802.11 wireless devices.
Locate APs on the interior of buildings instead of near exterior walls and windows as appropriate.
Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they become available (prior to purchase).
Configure SNMP settings on APs for least privilege (i.e., read only). Disable SNMP if it is not used. SNMPv1 and SNMPv2 are not recommended.
Use a local serial port interface for AP configuration to minimise the exposure of

TECHNICAL AND OPERATIONAL RECOMMENDATIONS
sensitive management information.
Understand and make sure that all default parameters are changed.
Make sure that default shared keys are periodically replaced by more secure unique keys.
Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).
Install antivirus software for all wireless clients. Ensure that the antivirus software is regularly updated with new virus definitions.
Install personal firewall software for all wireless clients.
Disable file sharing for wireless clients (especially in suspect environments).
Deploy MAC access control lists.
Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.
Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.
Fully test and deploy software patches and upgrades regularly.
Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.
Ensure that the “ad hoc mode” for 802.11 has been disabled.
Use static IP addressing on the network.
Disable DHCP.
Ensure that management traffic destined for APs is on a dedicated wired subnet.
Use SNMPv3 and/or SSL/TLS for Web-based management of APs.
Ensure that the client NIC and AP support firmware upgrade so that security patches may be deployed as they become available (prior to purchase).
Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.
Deploy intrusion detection agents on the wireless part of the network to detect suspicious behaviour or unauthorised access and activity.
Fully comprehend the magnitude of deploying any security feature or product prior to deployment.
Designate an individual to track the progress of 802.11 security products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology.

TECHNICAL AND OPERATIONAL RECOMMENDATIONS
--

Wait until future releases of 802.11 WLAN technologies incorporate fixes to the security features or provide enhanced security features.
--

Table 12-15: Technical and operational recommendations

13. APPENDIX E: DEVELOPMENT OF THE OODA-OCTAVE RISK ANALYSIS AND RISK MANAGEMENT DATABASE

The aim of this appendix is to illustrate the logical development of the OODA-OCTAVE risk analysis and risk management database. The database was developed in Microsoft Access 2003 as shown in figure 13.1.

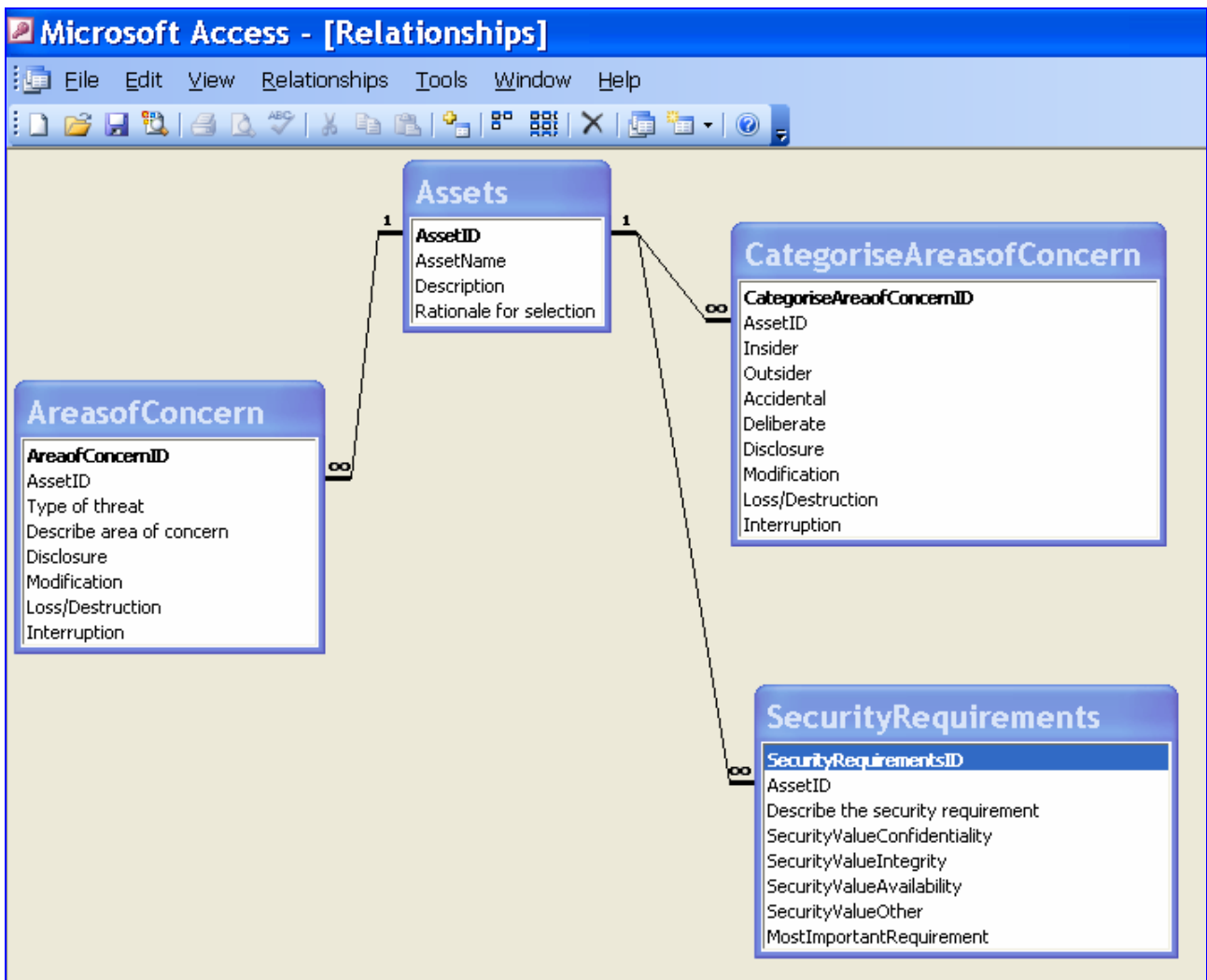


Figure 13-1: The Entity-Relationship diagram as shown in Microsoft Access 2003

The accompanying CD contains the OODA-OCTAVE database. The interested reader can view the contents of this CD for the design of the tables, queries, forms and reports.

14. REFERENCES

1. *2005 Global Security Survey*. 2005. Retrieved January 15, 2006 from http://www.deloitte.com/dtt/cda/doc/content/dtt_financialservices_2005GlobalSecuritySurvey_2005-07-21.pdf.
2. *2600 The Hacker Quarterly*. 1995. Retrieved October 14, 2005 from <http://www.2600.com>.
3. Adelstein, F., Alla, P., Joyce, R. & Richard III, G.G. 2004. Physically locating wireless intruders. *Proceedings. ITCC 2004. International Conference on Information Technology: Coding and Computing*, 1: 482-489.
4. *AirDefense Enterprise 7.0: What is New: Powerpoint Presentation*. 2005, December 12.
5. *AirMagnet Completes Cisco Integration, Defends Against Critical New Wireless Attacks; AirMagnet Enterprise 6.0 Allows Cisco APs*. 2005. Retrieved February 11, 2006 from <http://www.tmcnet.com/submit/2005/jul/1162458.htm>.
6. *AirMagnet Enterprise 6.0 User Guide*. 2005.
7. *AirMagnet Enterprise 6.0 WLAN Policy Reference Guide*. 2005.
8. *AirMagnet Handheld Tour*. n.d. Retrieved February 11, 2006 from <http://www.airmagnet.com>.
9. *AirMagnet SmartEdge Sensor AM-5010-11AG and AM-5012-11AG Security Policy*. 2005, August 26. Retrieved September 11, 2005 from <http://www.airmagnet.com>.
10. *AirMagnet Spectrum Analyser*. 2006. Retrieved February 11, 2006 from <http://www.airmagnet.com>.
11. *AirMagnet Survey 3.0*. 2006. Retrieved February 11, 2006 from <http://www.airmagnet.com>.
12. *AirMagnet Survey*. 2002-2006. Retrieved February 11, 2006 from <http://www.airmagnet.com>.
13. *AirSnort Homepage*. n.d. Retrieved July 12, 2004 from <http://airsnort.shmoo.com>.
14. *AirTight Networks, Inc. - Home Page*. 2005. Retrieved October 14, 2005 from <http://www.airtightnetworks.net/main/index.html>.
15. Alberts, C. & Dorofee, A. 2003. *Managing Information Security Risks: The OCTAVE Approach*. Boston, MA: Addison-Wesley.

-
16. Alberts, C. & Dorofee, A. 2004, June. Security incident response: rethinking risk management. *International Congress Series*, 1268: 141-146.
 17. Alberts, C., Dorofee, A., Stevens, J. & Woody, C. 2003. *Introduction to the OCTAVE® Approach*. Retrieved February 04, 2004 from http://www.cert.org/octave/approach_intro.pdf.
 18. Allen, J.H. 2001. *The CERT Guide to System and Network Security Practice*. New York: Addison Wesley.
 19. Anderson, J.P. 1980. Computer Security Threat Monitoring and Surveillance, Technical Report, Fort Washington, PA. Retrieved May 5, 2005 from <http://seclab.cs.ucdavis.edu/projects/history/paper/ande80.pdf>.
 20. Arbaugh, W. & Mishra, A. 2002, February 06. *An Initial Security Analysis of the IEEE 802.1x standard*. Retrieved May 16, 2005 from <http://www.cs.umd.edu/~waa/1x.pdf>.
 21. Arbaugh, W.A., Shankar, N. & Wan, J. 2001. Your 802.11 network has no clothes. *In Proceedings of the First IEEE International Conference on Wireless LANs and Home Networks*: 131-144.
 22. Arora, R. 2003, January 30. *State of Affairs of Wireless Networks*. Retrieved September 14, 2004 from <http://www.sans.org/rr/whitepapers/wireless/944.php>.
 23. Babiak, J., Butters, J. & Doll, M.W. 2005. *Defending the digital frontier: Practical security for management* (2nd ed.). Hoboken, New Jersey: John Wiley and Sons.
 24. Baccam, T. 2004, February 23. *Security Assessments: Reducing the Security Risk to Your Enterprise*. Retrieved April 12, 2005 from http://http://www.vigilar.com/img/whitepapers/20020210-Assessment_Whitepaper.pdf.
 25. Bace, R. 2000. *Intrusion Detection*. Macmillan Technical Publishing.
 26. Bace^a, R. 2002, June 3. *An Introduction to Intrusion Detection and Assessment*. Retrieved January 02, 2004 from <http://downloads.securityfocus.com/library/intrusion.pdf>.
 27. Bace^b, R.G. 2002. Vulnerability Assessment and Intrusion Detection Systems. In Seymour Bosworth & M.E.Kabay (Eds.), *Computer Security Handbook*: 37-1-37-16. Canada: John Wiley & Sons.
 28. Badenhorst, K.P. & Eloff, J.H.P. 1990, June. Computer Security Methodology: Risk Analysis and Project Definition. *Computers & Security*, 9(4): 339-346.
-

-
29. Barnes, C., Bautts, T., Lloyd, D., Ouellet, E., Posluns, J. & Zendzian, D.M. 2002. *Hack Proofing Your Wireless Network*. Syngress Publishing.
 30. Berghel, H. & Uecker, J. 2004, December. Wireless Infidelity II: Airjacking. *Communications of the ACM*, 47(12): 15-20.
 31. *Best Practices for Rogue Wireless LAN Detection*. 2003. Retrieved July 7, 2004 from <http://www.airdefense.net>.
 32. *Best Practices for Wireless Network Security and Sarbanes-Oxley compliance*. 2004. Retrieved December 2004 from <http://www.airdefense.net>.
 33. Bhagyavati, Summers, W.C. & DeJoie, A. 2004, September 17-18. Wireless Security Techniques: An overview. *InfoSecCD Conference '04*: 82-87.
 34. Birch, D.G.W. & McEvoy, N.A. 1992, March. Risk analysis for Information Systems. *Journal of Information Technology*, 7(1): 44-53.
 35. Bladon, P., Hall, R.J. & Andy Wright, W. 2002. Situation Assessment using Graphical Models. *In: Proceedings of the Fifth International Conference on Information Fusion. FUSION 2002*, 2: 886-893.
 36. Blakley, B., McDermott, E. & Geer, D. 2001, September. Information Security is Information risk Management. *Proceedings of the 2001 workshop on New Security paradigms*: 97-104.
 37. Blodgett, D.E., Gendreau, M., Guertin, F., Potvin, J. & Seguin, R. 2003, March. A Tabu Search Heuristic for Resource Management in Naval Warfare. *Journal of Heuristics*, 9(2): 145-169.
 38. Borisov, N., Goldberg, I. & Wagner, D. 2001, July. Intercepting mobile communications: The insecurity of 802.11. *In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking*: 180-188.
 39. Boyd, J.R. 1995, June 28. *The Essence of Winning and Losing*. Retrieved July 14, 2005 from [http://www.belisarius.com/modern_business_strategy/boyd/essence/eowl_frame set.htm](http://www.belisarius.com/modern_business_strategy/boyd/essence/eowl_frame_set.htm).
 40. British Standards Institution. February, 1995. *Information Security Management, Part 1: Code of Practice for Information Security Management of Systems (BS7799: Part 1:1995)*.
 41. Broder, J.F. 1984. *Risk analysis and the Security Survey*. Butterworth Publishers.
 42. Broderick, J.S. 2001. Information Security Risk Management: When Should It be Managed. *Information Security Technical Report*, 6(3): 12-18.
-

-
43. Broodryk, B. 2005, December 15. *Enterprise risk assessment-a new approach for a tough environment*. Retrieved January 11, 2006 from <http://www.ictworks.co.za/EditorialEdit.asp?EditorialID=25209&Archive=1>.
 44. Brookhiser, R. 1986, February 14. Rescuing the military. *National Review*: 36-43.
 45. Bulk, F. 2005, June 23. *Distributed Wireless Security Monitors: Time to Tighten the Wireless Net*. Retrieved October 11, 2005 from <http://www.networkcomputing.com/showitem.jhtml?docid=1612f2>.
 46. Buzzard, K. 1999. Computer security — What should you spend your money on? *Computers & Security*, 18(4): 322-334.
 47. Caelli, W., Longley, D. & Shain, M. 1989. *Information Security for Managers*. United States and Canada: Macmillan Publishers.
 48. *Cambridge Dictionaries Online - Cambridge University Press*. n.d. Retrieved August 31, 2005 from <http://dictionary.cambridge.org>.
 49. Campbell, P., Calvert, B. & Boswell, S. 2003. *Security+ Guide to Network Security Fundamentals*. Course Technology.
 50. Cam-Winget, N., Housley, R., Wagner, D. & Walker, J. 2003, May. Security flaws in 802.11 Data Link Protocols. *Communications of the ACM*, 46(5): 35-39.
 51. Cannon, K. 2006. *Lab Manual for CWNA Guide to Wireless LANs* (2nd ed.). Course Technology.
 52. Caralli, R.A. & Wilson, W.R. 2004, August 02. *The Challenges of Security Management*. Retrieved March 26, 2005 from <http://www.cert.org/archive/pdf/ESMchallenges.pdf>.
 53. Carr, M.J. 1997, May/June. Counterpoint: Risk Management May Not Be for Everyone. *IEEE Software*, 14(3): 21-24.
 54. Carroll, J.M. 1996. *Computer Security* (3rd ed.). Butterworth-Heinemann.
 55. Carter, B. & Shumway, R. 2002. *Wireless Security End to End*. Indianapolis, Indiana: Wiley Publishing.
 56. Carter, T.W. 2005. *Wireless All-In-One Reference for Dummies*. Wiley Publishing.
 57. Chartoff, M. & Boyland, B. 2004, December 1. *Face-off: Can rogue wireless LANs be eliminated?* Retrieved February 12, 2005 from <http://www.nwfusion.com>.
 58. Chester, R.W. 1996. Agile manufacturing: Beyond lean. *Production and Inventory Management Journal*, 32(2): 60-61.
 59. Ciampa, M. 2001. *Guide to Designing and Implementing Wireless LANs*. Course Technology.
-

-
60. Ciampa, M. 2006. *CWNA Guide to Wireless LANs* (2nd ed.). Course Technology.
 61. Ciechanowicz, Z. 1997. Risk analysis: requirements, conflicts and problems. *Computers & Security*, 16(3): 223-232.
 62. *COBRA - Security Risk Assessment, Security Risk Analysis and ISO 17799 - BS7799*. n.d.. Retrieved July 13, 2005 from <http://www.riskworld.net>.
 63. Coles, R.S. & Moulton, R. 2003. Operationalising IT risk management. *Computers & Security*, 22(6): 487-493.
 64. Coopers, Theron & Du Toit, 1988. *Marion - Information System Security Assessment Reference Manual*.
 65. Coram, R. 2002. *Boyd: The fighter pilot who changed the art of war* (1st ed.). Little Brown and Company.
 66. *CORAS: A Platform for Risk Analysis of Security Critical Systems*. n.d. Retrieved July 18, 2005 from <http://www2.nr.no/coras>.
 67. *Corporate Use of Wireless Data Services Continues to Grow*. 2002, March 2. Retrieved February 24, 2005 from <http://www.instat.com/newmk.asp?ID=106>.
 68. *CRAMM Expert Walkthrough and Overview*. 2003. Insight Consulting.
 69. Cruz, G. & Klein, J. 2004, June 9. *Patient Safety Drives Healthcare Provider WLAN Investments*. Retrieved March 15, 2005 from <http://www.gartner.com>.
 70. Dean, T. 2003. *Guide to Telecommunications Technology*. Course Technology.
 71. Dean, T. 2006. *Network+ Guide to Networks* (4th ed.). Thomson Course Technology.
 72. *Default Wireless Configurations*. n.d. Retrieved May 30, 2005 from <http://www.cirt.net/cgi-bin/ssids.pl>.
 73. *Define firmware - a Whatis.com definition*. 2000-2006. Retrieved July 12, 2005 from http://whatis.techtarget.com/definition/0,,sid9_gci212127,00.html.
 74. Deloitte & Touche. 2003, August 21. *The Status of Risk Management in South Africa: Report on the Deloitte & Touche Risk Management Summit, Sandton*. Retrieved July 13, 2004 from <http://www.deloitte.com/dtt/cda/doc/content/The%20Status%20of%20Risk%20Management%20in%20SA%283%29.pdf>.
 75. Denning, D. 1986, April. An Intrusion-Detection Model. *IEEE Symposium on Security and Privacy*: 118-131.
 76. *Department of Homeland Security's Website*. n.d. Retrieved March 04, 2005 from <http://www.fedcirc.gov/library/legislation/FISMA.html>.
-

-
77. Edney, J. & Arbaugh, W.A. 2004. *Real 802.11 Security: Wi-Fi Protected Access and 802.11i*. Canada: Addison-Wesley.
 78. Eloff, J.H.P., Labuschagne, L. & Badenhorst, K.P. 1993, October. A comparative framework for risk analysis methods. *Computers & Security*, 12(6): 597-603.
 79. Endorf, C., Schultz, E. & Mellander, J. 2004. *Intrusion Detection and Prevention*. McGraw-Hill/Osborne.
 80. *Enterprise Approaches to Detecting Rogue Wireless LANs*. 2003. Retrieved July 7, 2004 from <http://www.airdefense.net>.
 81. *Enterprise Class Wireless Intrusion Prevention Systems: Requirements and Figure of Merit*. 2002-2005. Retrieved January 15, 2006 from <http://www.airdefense.net>.
 82. *Enterprise Quick Reference Guide*. 2005.
 83. *Enterprise Wireless Intrusion Detection and Prevention Solution*. n.d. Retrieved July 17, 2005 from <http://www.airmagnet.com>.
 84. *Enterprise Wireless Intrusion Prevention Rogue AP Termination, Intrusion Detection, and Wireless Security*. 2001-2005. Retrieved July 12, 2004 from <http://www.airdefense.net>.
 85. *Enterprise-hardened Wireless Intrusion Prevention*. 2005, August 1. Retrieved September 12, 2005 from http://www.airmagnet.com/products/assets/Enterprise6_DataSheet.pdf.
 86. *Expression des Besoins et Identification des Objectifs de Securite (EBIOS), Direrction Centrale de la Securite des Systemes d'Information (France)*. 2004, February. Retrieved March 15, 2005 from <http://www.ssi.gouv.fr>.
 87. Fadok, D.S. 1995. John Boyd and John Warden Air Power's Quest for Strategic Paralysis. [Abstract]. *Dissertation Abstracts International*, 1-61. Retrieved November 12, 2004 from www.maxwell.af.mil/au/aul/aupress/SAAS_Theses/Fadok/fadok.pdf.
 88. Farshchi^a. 2003, October 18. *Wireless Policy Development (Part One)*. Retrieved July 12, 2005 from <http://www.securityfocus.com/infocus/1732>.
 89. Farshchi^b, J. 2003, October 10. *Wireless Policy Development (Part Two)*. Retrieved July 12, 2005 from <http://www.securityfocus.com/infocus/1735>.
 90. *Federal Agencies Need to Improve Controls over Wireless Networks*. 2005, May. Retrieved September 12, 2005 from <http://www.gao.gov/new.items/d05383.pdf>.
-

-
91. Federal Trade Commission; 16 CFR Part 314; Standards for Safeguarding Customer Information; Final Rule. 2002, May 23. *Federal Register*, 67(100), 36484-36494. Retrieved May 30, 2005 from <http://www.ftc.gov/os/2002/05/67fr36585.pdf>.
 92. Fitzgerald, K.J. 1995. Information security baselines. *Information Management & Computer Security*, 3(2): 8-13.
 93. Flickenger, R. 2003. *Wireless hacks* (1st ed.). Sebastopol, CA: O'Reilly.
 94. Fluhrer, S., Mantin, I. & Shamir, A. 2001. Weaknesses in the key schedule algorithm of RC4. *Proceedings of the 4th Annual Workshop on Selected Areas of Cryptography*.
 95. Forcht, K.A. 1994. *Computer Security Management*. International Thomson Publishing.
 96. Forouzan, B.A. 2003. *Local Area Networks* (International ed.). Mc-Graw Hill.
 97. Foust, R. August, 2002. Identifying and Tracking Unauthorised 802.11 Cards and Access Points, A Practical Approach. 27(4): 32-43.
 98. Fung, K.T. 2005. *Network Security Technologies* (2nd ed.). Boca Raton, FL: Auerbach Publications.
 99. Gallo, M.A. & Hancock, W.M. 2002. *Computer Communications and Networking Technologies*. Brooks/Cole.
 100. GAO, *Information Security Risk Assessment - Practices of Leading Organisations, Exposure Draft, U.S. General Accounting Office*. 1999, August. Retrieved January 12, 2005 from <http://www.gao.gov/special.pubs/ai99139.pdf>.
 101. Geffert, B.T. 2004, November/December. Incorporating HIPAA Security Requirements into an Enterprise Security Program. *Information Systems Security*, 13(5): 21-28.
 102. Gilliam, D.P. 2004. Managing Information Technology Risk. *Springer-Verlag*: 296-317.
 103. *Give your network users freedom and mobile security without giving up network security*. 1995-2005. Retrieved October 17, 2005 from <http://www.cisco.com/en/US/netsol/ns340/ns394/ns348/ns337/netbr09186a00801f7d0b.html>.
 104. Glazier, D. 2006, March 8. *Mitnick warns of "holes in human firewall"*. Retrieved March 2006 24, from <http://www.itweb.co.za/sections/quickprint/print.asp?StoryID=160287>.
-

-
105. *Global Information Security Survey 2005*. 2005. Retrieved January 3, 2006 from [http://www.ey.com/global/download.nsf/International/Global_Information_Security_Survey_2005/\\$file/EY_Global_Information_Security_survey_2005.pdf](http://www.ey.com/global/download.nsf/International/Global_Information_Security_Survey_2005/$file/EY_Global_Information_Security_survey_2005.pdf).
 106. Goan, T. 1999, July. A Cop on the Beat: Collecting and Appraising Intrusion Evidence. *Communications of the ACM*, 42(7): 46-52.
 107. Godber, A. & Dasgupta, P. 2003. Countering Rogues in Wireless Networks. *2003 International Conference on Parallel Processing Workshops (ICPPW'03)*: 425-431.
 108. Good, K.J. 2005, March 3. *Got a Second? A Journey into the OODA Cycle*. Retrieved October 15, 2005 from http://www.belisarius.com/modern_business_strategy/hord/ken_good_OODA.pdf.
 109. Green, C. 2006, March 23. *Man fined \$250 in first area case of Internet piracy*. Retrieved April 11, 2006 from <http://rrstar.com/apps/pbcs.dll/article?AID=/20060323/NEWS0107/103230036/1011>.
 110. Hallberg, B.A. 2003. *Networking: A Beginner's Guide* (3rd ed.). Mc-Graw-Hill/Osborne.
 111. Hammond, G.T. 2001. *The Mind of War: John Boyd and American Society*. Smithsonian Institution.
 112. Hammonds, K.H. 2002, June. The Strategy of the Fighter Pilot. *Fast Company*
 113. Held, G. 2001, November/December. The ABCs of IEEE 802.11. *IEEE IT Pro*: 49-52.
 114. Held, G. 2003. *Securing Wireless LANs*. John Wiley & Sons.
 115. Henning, R. 2003. Vulnerability Assessment in Wireless Networks. *Symposium on Applications and the Internet Workshops*: 358-362.
 116. *Highwall Technologies - The Smart Solution for Securing the Air*. 2005. Retrieved October 14, 2005 from <http://www.highwalltech.com>.
 117. Housley, R. & Arbaugh, W. 2003, May. Security problems in 802.11-based networks. *Communications of the ACM*, 46(5): 31-34.
 118. Howlett, T. 2005. *Open Source Security Tools*. Prentice Hall.
 119. Hunter, R. & Aron, D. 2005, February. *Executive Summary: IT Risk Management: A Little Bit More Is a Whole Lot Better*. Retrieved July 7, 2005 from <http://www.gartner.com>.
-

-
120. *IEEE OUI and Company_id Assignments*. n.d. Retrieved February 02, 2005 from <http://standards.ieee.org/regauth/oui/index.shtml>.
 121. Iheagwara, C. 2003, September 24. The effects of intrusion detection management methods on the return on investment. *Computers & Security*, 23: 213-228.
 122. Ilett, D. 2005, July 22. *Wireless network hijacker found guilty*. Retrieved February 04, 2006 from <http://www.silicon.com>.
 123. In, P.H., Kim, Y., Lee, T., Moon, C., Jung, Y. & Kim, I. 2005. A Security Risk Analysis Model for Information Systems. In Doo-Kwon Baik (Ed.), *Systems Modeling and Simulation: Theory and Applications: Third Asian Simulation Conference, AsianSim 2004, Jeju Island, Korea:505-513*. Springer-Verlag GmbH.
 124. Information Security-The Great Balancing Act. 2002, February 1. *Computer Fraud & Security*, 2002(2): 12-14.
 125. Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness; Final Rule. 2001, February. *Federal Register*, 66(22): 8616-8641.
 126. Jacobson, R.V. 2002. *Using CORA to Implement the NIST Risk Management Guide*. Retrieved May 12, 2005 from <http://www.ist-usa.com/aboutcora.htm>
 127. Jenkins, B.D. 1998. *Security risk analysis and management White Paper, Countermeasures Inc.* Retrieved April 15, 2005 from http://www.cs.kau.se/~albin/Documents/RA_by%20Jenkins.pdf.
 128. Johnson, L.M. & Schulte, J.D. 2004, October. job security:7 steps for HIPAA compliance. *Healthcare Financial Management*, 58(10): 46-49.
 129. Josang, A., Bradley, D. & Knapskog, S.J. 2004. Belief-based risk analysis. *Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence and Software Internationalisation*, 32: 63-68.
 130. Kachirski, O. & Guha, R. 2002. Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks. *Proceedings of the IEEE Workshop on Knowledge Media Networking (KMN'02)*: 153-158.
 131. Kailay, M.P. & Jarratt, P. 1995. RaMex: a prototype expert system for computer security risk analysis and management. *Computers and Security*, 14(5): 449-463.
 132. Kapp, S. 2002, January-February. 802.11: Leaving the Wire Behind. *IEEE Internet Computing*, 6(1): 82-85.
 133. Karabacak, B. & Sogukpinar, I. 2005, March. ISRAM: information security risk analysis method. *Computers & Security*, 24(2): 147-159.
-

-
134. Karygiannis, T. & Owens, L. 2002. *Wireless Network Security: 802.11, Bluetooth and Handheld Devices*. Online. NIST Special Publication 80048. Computer Security Division. Information Technology Laboratory, National Institute of Standards and Technology. Gaithersburg, MD. Retrieved July 7, 2004 from http://csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.PDF.
 135. Khan, J. & Khwaja, A. 2003. *Building Secure Wireless Networks with 802.11*. Canada: Wiley Publishing, Indianapolis, Indiana.
 136. *Kismet*. n.d. Retrieved March 15, 2005 from <http://www.kismetwireless.net>.
 137. Kittelberger, K.L. 1983. Scope of Computer Security Problems. In Marvin M. Wofsey (Ed.), *Advances in Computer Security Management*: 1-37. John Wiley & Sons.
 138. Koziol, J. 2003. *Intrusion Detection with Snort*. Sams Publishing.
 139. Lackey, J., Roths, A. & Goddard, J. 2003, April. *Wireless Intrusion Detection*. Retrieved May 12, 2005 from http://www-1.ibm.com/services/us/bcrs/pdf/wp_wireless-intrusion-detection.pdf.
 140. Lanz, J. 2002, December. Prioritising Aspects of Technology Risk Assessment and Mitigation. *Bank Accounting & Finance*, 16(1): 19-26.
 141. Lewis, B.D. & Davis, P.T. 2004. *Wireless Networks for Dummies*. Indianapolis, Indiana: Wiley Publishing.
 142. Lichtenstein, S. 1996. Factors in the selection of a risk assessment method. *Information Management & Computer Security*, 4(4): 20-26.
 143. Lim, Y. & Schmoyer, T. 2003. Wireless Intrusion Detection and Response. *Proceedings of the 2003 IEEE Workshop on Information Assurance*: 68-75.
 144. Lind, W.S. 1985. *Manuver Warfare Handbook*. United States of America: Westview Press.
 145. Lindstrom, P. 2003. *Selecting a WLAN Monitoring Solution*. Retrieved August 18, 2004 from <http://www.spiresecurity.com>.
 146. Lockhart, A. 2003-2005. *Snort-wireless*. Retrieved May 15, 2005 from <http://www.snort-wireless.org>.
 147. *Loud-Fat-Blokes-World-Of-Weird*. n.d. Retrieved October 14, 2005 from <http://www.loud-fat-bloke.co.uk/w80211.html>.
 148. Maiwald, E. 2003. *Network Security: A Beginner's guide*. McGraw-Hill/Osborne.
 149. Martinez, J. 2001. Integrated Risk Management - A Concept for Risk Containment. In *Information Security Risk Analysis*: 257-271. CRC Press LLC.
-

-
150. Mash, S. 2002, December. Risk Assessment for Dummies. *Computer Fraud and Security*, 2002(12): 11-13.
 151. Maxim, M. & Pollino, D. 2002. *Wireless Security*. McGraw-Hill/Osborne.
 152. May, C. 2002, March 1. Risk Management—Practising What We Preach. *Computer Fraud & Security*, 2002(8): 10-13.
 153. May, C. 2003. Dynamic Corporate Culture Lies at the Heart of Effective Security Strategy. *Computer Fraud & Security*, 2003(5):10-13.
 154. McCauley-Bell, P. & Freeman, R. 1996. Quantification of Belief and Knowledge Systems in Information Warfare. In: *Proceedings of the Fifth IEEE International Conference on Fuzzy Systems. FUZZ-IEEE '96*, 3:1579-1585.
 155. McCullough, J. 2004. *Wireless Networking*. Indianapolis, Indiana: Wiley Publishing.
 156. McHugh, J., Christie, A. & Allen, J. 2000, September/October. Defending Yourself: The Role of Intrusion Detection Systems. *IEEE Software*: 42-51.
 157. McKeen, J.D. & Smith, H.A. 2003. *Making IT Happen: Critical Issues in IT Management*. John Wiley & Sons.
 158. McMahan, R.A. 2003. *Introduction to Networking*. Mc-Graw-Hill/Osborne.
 159. *Merriam-Webster online*. n.d. Retrieved October 07, 2005 from <http://www.m-w.com>.
 160. *Méthode Harmonisée de l'Analyse de Risques (MEHARI), CLUSIF, Version 3*. 2004, October. Retrieved February 20, 2005 from <http://clusif.asso.fr>.
 161. Microsoft Operations Framework: Risk Management Discipline for Operations. 2004, February 19: 1-64. Retrieved February 15, 2005 from <http://www.microsoft.com/technet/itsolutions/cits/mo/mof/mofrisk.mspx>.
 162. Miller, S.S. 2003. *WiFi Security*. McGraw-Hill Companies.
 163. *Mobile Solution Suite*. 2005, October 1. Retrieved September 15, 2005 from <http://www.airmagnet.com/products/assets/Mobile12-04.pdf>.
 164. Moeller, R.R. 2004. *Sarbanes-Oxley and the New Internal Auditing Rules*. Hoboken, New Jersey: John Wiley & Sons.
 165. Moses, R.H. 1992. Risk Analysis and Management. In *Computer Security Reference Book*: 227-263. Butterworth-Heinemann.
 166. Neoh, D. 2003, December 12. *Corporate Wireless LAN: Know the Risks and Best Practices to Mitigate Them*. Retrieved June 12, 2005 from <http://www.sans.org/rr/whitepapers/wireless/1350.php>.
-

-
167. *NetStumbler*. n.d. Retrieved June 11, 2004 from <http://www.netstumbler.com>.
 168. *Network Chemistry-The Wireless Security Experts*. 2005. Retrieved October 14, 2005 from <http://www.networkchemistry.com/index.php>.
 169. *Network Security and Risk Management*. 2005, October 31. Retrieved September 21, 2005 from <http://www.cs.uow.edu.au/people/bomba/iact301wk4.html>.
 170. Nixon, A. 2005, January. Analysis: Corporate governance - Internal audit: the new rock and roll. *Accountancy*, 135(1337): 48.
 171. Nosworthy, J.D. 2000. A Practical Risk Analysis approach: Managing BCM risk. *Computers & Security*, 19(7): 596-614.
 172. *OCTAVE Automated Tool from the Advanced Technology Institute*. n.d. Retrieved July 12, 2004 from http://oattool.atcorp.org/Tool_Info.html.
 173. *Overview of the New Basel Capital Accord. Technical report, Bank for International Settlements*. 2003, April. Retrieved January 05, 2005 from <http://www.bis.org/bcbs/bcbsp.htm>.
 174. Owen, J., Burstein, F. & Mitchell, S. 2004. Knowledge Reuse and Transfer in a Project Management Environment. *Journal of Information Technology Cases and Applications*, 6(4): 21-35.
 175. Ozier, W. 1995. Risk Assessment and Management. In *Information Security Risk Analysis*: 221-243. CRC Press LLC.
 176. Palmer, M. & Sinclair, R.B. 2003. *Guide to Designing and Implementing Local and Wide Area Networks* (2nd ed.). Course Technology.
 177. Palmer, M. 2004. *Guide to Operating Systems Security*. Course Technology.
 178. Pandya, P. & Frazin, R. n.d. *Information Security Management: A Research Project*. Retrieved July 12, 2005 from <http://proceedings.informingscience.org/InSITE2004/006pandy.pdf>.
 179. Panko, R.R. 2005. *Business Data Networks and Telecommunications* (5th ed.). Upper Saddle River, N.J: Prentice Hall.
 180. Park, J.S. & Dicoi, D. 2003. WLAN Security: Current and Future. *IEEE Internet Computing*, 7(5): 60-65.
 181. Park, S.H., Ganz, A. & Ganz, Z. 1998. Security protocol for IEEE 802.11 wireless local area network. *Mobile Networks and Applications*, 3: 237-246.
 182. Parker, X.L. 2001, February. Understanding risk. *The Internal Auditor*, 58(1): 61-65.
-

-
183. Passori, A. 2004, July. *Selecting the risk assessment method of choice*. Retrieved July 13, 2005 from http://searchcio.techtarget.com/originalContent/0,289142,sid19_gci994851,00.html.
 184. Paul, B. 2000, October 30. Risk-assessment strategies. *Network Computing*, 11(21): 121-125.
 185. Pech, R.J. & Durden, G. 2003. Manoeuvre warfare: A new military paradigm for business decision making. *Management Decision*, 41(1): 168-179.
 186. Peikari, C. & Fogie, S. 2003. *Maximum Wireless Security*. Sams Publishing.
 187. Peltier, T. 2001. *Information Security Risk Analysis*. Boca Raton, FL: Auerbach Publications.
 188. Peltier, T. 2005. *Information Security Risk Analysis* (2nd ed.). Boca Raton, FL: Auerbach Publications.
 189. Peltier, T.R. 2004, Sept/Oct. Risk Analysis and Risk Management. *Information Systems Security*, 13(4): 44-56.
 190. Pfleeger, C.P. & Pfleeger, S.L. 2003. *Security in Computing* (3rd ed.). Pearson Education.
 191. Poblete, O. 2005, January 24. *An Overview of Wireless intrusion Detection systems*. Retrieved August 15, 2005 from <http://www.sans.org/rr/whitepapers/wireless/1599.php>.
 192. Polk, R.B. 2000, December. A Critique of the Boyd Theory - Is it Relevant to the Army? *Defense Analysis*, 16(3): 257-277.
 193. Potter, B. 2004, April. Wireless intrusion detection. *Network Security*, 2004(4): 4-5.
 194. *Projects - FakeAP*. 2001-2002. Retrieved April 08, 2005 from <http://www.blackalchemy.to/project/fakeap>.
 195. *Public Wireless LAN Access: US Market Forecasts*. 2002, February. Retrieved February 24, 2005 from http://www.gii.co.jp/english/an9799_public_wireless_lan_toc.html.
 196. Quinion, M. 2002, October 27. Turns of Phrase Warchalking. Retrieved October 14, 2005 from <http://www.worldwidewords.org/turnsofphrase/tp-war1.htm>.
 197. Raval, V. 2004, January. *Guidelines for compliance with Sarbanes-Oxley*. *EDPACS*, 31(7): 14-20.
 198. *Red-M-Home*. 2005. Retrieved October 14, 2005 from <http://www.red-m.com>.
-

-
199. Regan, K. 2003, January. Wireless LAN Security: Things You Should Know about WLAN Security. *Network Security*, 2003(1): 7-9.
 200. Saltmarsh, T.J. & Browne, P.S. 1983. Data Processing-Risk Assessment. In Marvin M. Wofsey (Ed.), *Advances in Computer Security Management Volume 2*: 93-116. John Wiley.
 201. *SC Magazine Awards Winners*. 2006. Retrieved February 16, 2006 from <http://www.scawards.com/innners/2006.asp>.
 202. *Scanning and Hacking*. 2004, January 30. Retrieved October 12, 2005 from http://www.ingleby.com/computer-wlan_hacking.htm.
 203. Schechtman, G.M. 1996. Manipulating the Loop: The overlooked role of Information Resource Management in Information Warfare. [Abstract]. *Dissertation Abstracts International*: 1-108. Retrieved December 12, 2004 from http://www.au.af.mil/au/awc/awcgate/afit/schec_gm.pdf.
 204. *Security Risk Management Guide*. 2005, October 15. Retrieved August 31, 2005 from <http://www.microsoft.com/technet/security/topics/policiesandprocedures/secrisk//srsgc>.
 205. Security Standards and Electronic Signature Standards; Proposed Rule. 1998, August. *Federal Register*, 63(155): 43242-43280.
 206. Shaffer, S.L. & Simon, A.R. 1994. *Network Security*. Academic Press.
 207. Sharma, V. 2004. Intrusion Detection in Infrastructure Wireless LANs. *Bell Labs Technical Journal*, 8(4): 115-119.
 208. Shaw, G. & Daniels, S. 2002. Managing system risk. *Management Services*, 46(9): 14-16.
 209. Shay, W.A. 2004. *Understanding Data Communications and Networks* (3rd ed.). Brooks/Cole.
 210. *SMAC Official Website*. n.d. Retrieved October 06, 2005 from <http://www.klccconsulting.net/smac>.
 211. Smith, S.T. 1987. LAVA for Computer Security: An Application of the Los Alamos Vulnerability Assessment Methodology. *Release Version 1.01, Los Alamos National Laboratory, New Mexico*.
 212. Spitaletta, J. 2003, January. The transformation battlefield. *Industrial Engineer*, 35(1): 38-43.
-

-
213. Spitzner, L. 2003, March. The HoneyNet Project: Trapping the Hackers. *IEEE Security and Privacy*: 15-23.
 214. Stair, R. & Reynolds, G. 2006. *Principles of Information Systems* (7th ed.). Thomson Course Technology.
 215. Stallings, W. 2001. IEEE 802.11: Moving Closer to Practical Wireless LANs. *IT Pro*: 17-23.
 216. Stallings, W. 2004, September/October. IEEE802.11: Wireless LANs from a to n. *IT Pro*:32-37.
 217. *Standards Australia and Standards New Zealand AS/NZS 4360:2004, Risk Management*. 2004. Sydney, NSW.
 218. *Standards, methodologies, recommendations and legislation*. 1998-2006. Retrieved November 14, 2005 from <http://www.methodware.com/services/standards.shtml>.
 219. Stanley, R.A. 2002. Wireless LAN Risks and Vulnerabilities. *Information Systems Control Journal*, 2: 57-61.
 220. Stephenson, P. 2004, November. Risk and incident management - getting started. *Computer Fraud and Security*, 2004(11): 17-19.
 221. Stewart, A. 2004, May. On risk: perception and direction. *Computers & Security*, 23(5): 362-370.
 222. Stoneburner, G., Goguen, A. & Feringa, A. 2001, October. *Risk Management Guide for Information Technology Systems. Technical report, National Institute of Standards and Technology*. Retrieved April 30, 2004 from <http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf>.
 223. Stubblefield, A., Ioannidis, J. & Rubin, A. 2002. Using the Fluhrer, Mantin, and Shamir attack to break WEP. *In Proceedings of the 2002 Network and Distributed Systems Security Symposium*: 17-22.
 224. Suh, B. & Han, I. 2003. The IS risk analysis based on a business model. *Information & Management*, 41(2003): 149-158.
 225. Sundaram, A. 1996, April. An Introduction to Intrusion Detection. *The ACM Student Magazine*, 2(4): 3-7.
 226. Sutton, M. 2002, July 10. *Hacking the Invisible Network*. Retrieved April 12, 2005 from <http://madchat.org/reseau/wireless/wireless.pdf>.
-

-
227. Swanson, M. & Guttman, B. 1996, September. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. Retrieved July 15, 2004 from <http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf>.
228. Tanzella, F. 2003. *Wireless LAN Intrusion Detection & Protection*. Retrieved September 7, 2004 from <http://www.airdefense.net>.
229. *Tenth Annual Computer Crime and Security Survey*. 2005. Retrieved January 15, 2006 from http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2005.pdf.
230. The HoneyNet Project. 2002. *Know your Enemy: Revealing the security tools, tactics and motives of the blackhat community*. Addison-Wesley.
231. *The MARION and MELISA Methods*. 1990. Paris: XP Conceil.
232. Thomas, T. 2004. *Network security: first-step*. Indianapolis, IN: Cisco Press.
233. Timothy. 2005, February 21. Managing Information Security Risks. [Msg. 2129224]. Message posted to <http://books slashdot.org/article.pl?sid=05/02/21/2129224>.
234. Tomsho, G., Tittel, E. & Johnson, D. 2004. *Guide to Networking Essentials* (4th ed.). Thomson Course Technology.
235. *ToorCon 7*. n.d. Retrieved July 10, 2005 from <http://www.toorcon.org>.
236. Turvey, S. 2005, October 17. *Wireless crackdown*. Retrieved October 25, 2005 from http://zdnet.com.au/reviews/colgear/wireless/soa/Wireless_crackdown/0.39023505.39216347.00.htm.
237. *Tutorial Notes: The Australian and New Zealand Standard on Risk Management, AS/NZS 4360:2004*. 2004. Retrieved February 05, 2006 from http://www.broadleaf.com.au/tutorials/Tut_Standard.pdf.
238. Tzu, Sun. 1988. *The Art of War*. (Ralph D.Sawyer, Trans.). Oxford: Westview Press. (Original Work Published).
239. Varshney, U. 2003, June. The Status and Future of 802.11-Based WLANs: 102-105.
240. Veijeren, J.M. n.d. *The KING II Report On Corporate Governance*. Retrieved February 12, 2005 from <http://www.i-value.co.za/king.html>.
241. Vennaro, N. 2005, March. *Enterprise Risk Assessment Overview*. Retrieved April 14, 2005 from <http://www.AegisSecurityWorks.com>.
242. Von Solms, B. & Marais, E. 2004, December. From secure wired networks to secure wireless networks – what are the extra risks? *Computers & Security*, 23(8): 633-637.
-

-
243. Von Solms, B. & Von Solms, R. 2004, July. The 10 deadly sins of information security management. *Computers & Security*, 23(5): 371-376.
 244. Wagner, D. & Soto, P. 2000, November. Mimicry attacks on Host-Based Intrusion Detection Systems. *Communications of the ACM*: 255-264.
 245. Walker, J.R. 2000, October 27. Unsafe at Any Key Size. *An Analysis of the WEP Encapsulation. IEEE 802.11 doc 00-362*.
 246. Wei, H., Frinke, D., Carter, O. & Ritter, C. 2001. Cost-Benefit Analysis for Network Intrusion Detection Systems. *CSI 28th Annual Computer Security Conference*: 1-14.
 247. Welcome to DEF CON, the Largest Underground Hacking Convention in the World. 1992. Retrieved October 14, 2005 from <http://www.defcon.org>.
 248. Wells, S. 2002, December. 802.11 WLAN Security - Choose Wisely. *Bechtel Telecommunications Technical Journal*, 1(1): 71-75.
 249. *WEPCrack - An 802.11 key breaker*. n.d. Retrieved July 12, 2004 from <http://wepcrack.sourceforge.net>.
 250. *What is Killing the Intelligence Dinosaurs?* 2004, March. Retrieved June 1, 2005 from <http://www.mitosystems.com/pdf/Mitopia-.pdf>.
 251. White, C.M. 2004. *Data Communications and Computer Networks*. Course Technology.
 252. Whitman, M.E. & Mattord, H.J. 2004. *Management of Information Security*. Course Technology.
 253. *WiGLE-Wireless Geographic Logging Engine - Plotting WiFi on Maps*. n.d. Retrieved March 15, 2005 from <http://www.wigle.net>.
 254. Williams, A. 2004. *WLAN Best Security Practices*. Retrieved July 15, 2005 from <http://www.airmagnet.com>.
 255. Williams, J. 2002, November/December. Providing for Wireless LAN Security, Part 2. *IT Pro*: 44-48.
 256. Williamson, W. 2004. *Best Practice For Securing Your Enterprise WLAN*. Retrieved July 12, 2005 from <http://www.airmagnet.com>.
 257. Wilson, M. 2001, April. *Toward an ontology of integrated intelligence and conflict*. Retrieved November 01, 2004 from <http://www.metatempo.com/DSSIOntology.PDF>.
 258. *Wireless LAN Policies for Security & Management*. 2003. Retrieved July 7, 2004 from <http://www.airdefense.net>.
-

-
259. *Wireless LAN Security - What Hackers Know That You Don't*. 2003. Retrieved July 7, 2004 from <http://www.airdefense.net>.
 260. *Wireless LAN Security - Why Your Firewall, VPN and IEEE 802.11i Aren't Enough to protect your network*. 2005, February. Retrieved March 17, 2005 from <http://www.airtightnetworks.net>.
 261. *Wireless LANs: Defending the Enterprise Airwaves*. 2004, June. Retrieved April 14, 2005 from <http://www.networkchemistry.com>.
 262. *Wireless LANs: Is My Enterprise At Risk? 2002-2005*. Retrieved September 12, 2005 from <http://www.airdefense.net>.
 263. *WIRELESS LANs: Risks and Defenses*. 2003. Retrieved July 7, 2004 from <http://www.airdefense.net>.
 264. *Wireless Protection for the Mobile Workforce. 2002-2005*. Retrieved February 14, 2005 from <http://www.airdefense.net>.
 265. *Wireless Vulnerabilities and Exploits*. n.d. Retrieved February 12, 2006 from <http://www.wirelessve.org/info>.
 266. Wong, S. 2003, May 20. *The evolution of wireless security in 802.11 networks: WEP, WPA and 802.11 standards*. Retrieved January 12, 2005 from <http://www.sans.org/rr/whitepapers/wireless/1109.php>.
 267. Wright, J. 2002, November. *Layer 2 Analysis of WLAN Discovery Applications for Intrusion Detection*. Retrieved July 12, 2004 from <http://home.jwu.edu/wright/papers/12-wlan-ids.pdf>.
 268. Wright, J. 2003. *Detecting Wireless LAN MAC Address Spoofing*. Retrieved March 15, 2005 from <http://802.11ninja.net/papers/wlan-mac-spoof.pdf>.
 269. Wright, J. 2005, May 5. *Weaknesses in Wireless LAN Session Containment*. Retrieved August 15, 2005 from http://i.cmpnet.com/nc/1612/graphics/SessionContainment_file.pdf.
 270. Yang^a, H., Xie, L. & Sun, J. 2004. *Intrusion detection solution to WLAN. Proceedings of the IEEE 6th Circuits and Systems Symposium on Emerging Technologies: Frontiers of Mobile and Wireless Communication (IEEE Cat. No.04EX710)*, 2:553-556.
 271. Yang^b, D., Hu, C. & Chen, Y. 2004. *A framework of cooperating Intrusion Detection based on Clustering analysis and expert system. Communications of the ACM: 150-154*.
-

272. Yang^c, H., Xie, L. & Sun, J. 2004, May. Intrusion detection for wireless local area network. *Canadian Conference on Electrical and Computer Engineering (IEEE Cat. No.04CH37513)*, 4: 1949-1952.
273. Zhang, Y., Lee, W. & Huang, Y. 2003, September. Intrusion Detection Techniques for Mobile Wireless Networks. *Wireless Networks*, 9(5): 545-556.