

WISP: A WIRELESS INFORMATION SECURITY PORTAL

By

SOUMAILA DIT MOULE DIAKITE

A dissertation submitted in fulfillment of the
requirements for the degree of



MASTER OF SCIENCE

in

COMPUTER SCIENCE

in the

FACULTY OF SCIENCE

at the

UNIVERSITY OF JOHANNESBURG

SUPERVISOR: PROF. S.H. VON SOLMS

June 2008

Acknowledgments

I would like to thank God for helping me throughout this dissertation. I want to thank my parents (Kalilou Dit Babakaou and Rokia) for their support. I also want to express my gratitude to the University of Johannesburg for their support.

Thank you Prof. S.H Von Solms for everything.



Abstract

Wireless networking is a fairly new technology that is important in information technology (IT). Hotels, Airports, Coffee shops, and homes are all installing wireless networks at a record pace, making wireless networks the best choice for consumers. This popularity of wireless networks is because of the affordability of wireless networks devices, and the easy installation [11].

In spite of the popularity of the wireless networks, one factor that has prevented them from being even more widespread can be summed up in a single word: **security**. It comes as no surprise that these two – **wireless** and **security** – converge to create one of the most important topics in the IT industry today [11].

Wireless networks by nature bring about new challenges unique to its environment. One example of these new challenges is: "Signal overflow beyond physical walls", and with these kinds of new challenges unique to wireless networks, we have new security risks. Hence wireless networks lend themselves to a host of attack possibilities and risks. That is because wireless networks provide a convenient network access point for an attacker, potentially beyond the physical security controls of the organization [7].

Therefore it is challenging for managers to introduce wireless networks and properly manage the security of wireless networks, Security problems of wireless networks are the main reason for wireless networks not being rolled out optimally [1].

In this dissertation, we aim to present to both specialist and non-specialists in the IT industry the information needed to protect a wireless network. We will first identify and discuss the different security requirements of wireless networks. After that we shall examine the technology that helps make wireless networks secure, and describe the type of attacks against wireless networks and defense techniques to secure wireless networks.

The research will concentrate on wireless LANs (Local Area Networks), and leading wireless LAN protocols and standards. The result of the research will be used to create WISP (A Wireless Information Security Portal). WISP will be a tool to support the management of a secure wireless network, and help assure the confidentiality, integrity, and availability of the information systems in a wireless network environment.

Table of Contents

Abstract	3
Preface	11
Chapter 1 - Thesis Overview	12
1.1 Introduction	13
1.2 Problem Statement	13
1.3 Objective	13
1.4 Approach	14
1.5 Deliverables	14
1.6 Document Structure	15
Part I	17
Chapter 2 - Computers and Computer Networks Overview	18
2.1 Introduction	19
2.2 Computer Systems	19
2.2.1 Hardware Components of the Computer Systems	19
2.2.2 Software Components of the Computer Systems	19
2.3 Computer Networks	21
2.3.1 Computer Network Types	21
2.3.1.1 LANs	21
2.3.1.2 MANs	21
2.3.1.3 WANs	21
2.3.2 Computer Network Architectures	23
2.3.2.1 Client/Server Networks	23
2.3.2.2 Peer-to-Peer Networks	23
2.3.3 Computer Network Standards	23
2.3.3.1 OSI Model	24
2.3.3.2 Ethernet	25
2.3.3.3 Token Ring	25
2.3.3.4 TCP/IP	25
2.3.3.5 802.11	25
2.3.3.6 WiMAX	26
2.4 Summary	27
Chapter 3 - Wired Networks Overview	28
3.1 Introduction	29
3.2 Wired Networks Transmission Media	29
3.2.1 Copper Wires	29
3.2.2 Fiber-Optic Cable	30
3.3 Wired Networks Topologies	31
3.3.1 Bus Network	32
3.3.2 Ring Network	32
3.3.3 Star Network	32
3.4 Wired Networks Standards	33
3.4.1 Ethernet	33
3.4.2 Token Ring	33

3.5	Wired Network Devices	34
3.5.1	Modems	34
3.5.2	Network Interface Card (NIC)	34
3.5.3	Routers	34
3.6	Wired Networks Advantages and Disadvantages	35
3.6.1	Wired Network Advantages	35
3.6.2	Wired Network Disadvantages	35
3.7	Summary	36

Chapter 4 - Wireless Networks Overview 37

4.1	Introduction	38
4.2	Wireless Network Types	38
4.2.1	Wireless PAN	38
4.2.1.1	Bluetooth	38
4.2.1.2	IrDA	39
4.2.2	Wireless LANs	39
4.2.2.1	802.11	39
4.2.2.2	802.11a	39
4.2.2.3	802.11b	40
4.2.2.4	802.11g	40
4.3	Wireless Network Devices	41
4.3.1	Wireless Access Point	41
4.3.2	Wireless Modems	41
4.3.3	Wireless Client	41
4.4	Wireless Networks Advantages and Disadvantages	43
4.4.1	Advantages	43
4.4.2	Disadvantages	44
4.5	Summary	45

Chapter 5 - Information Security Overview 46

5.1	Introduction	47
5.2	What is Information Security?	47
5.3	The Information Security Pillars	49
5.3.1	Identification and Authentication	49
5.3.2	Authorization	50
5.3.3	Confidentiality	50
5.3.4	Integrity	50
5.3.5	Non-repudiation	50
5.6	Summary	51

Part II 52

Chapter 6 - Wireless LANs Security Risks 53

6.1	Introduction	54
6.2	Category 1: Inherent Security Risks of Wireless Networks	54
6.2.1	Signal Overflow	54
6.2.2	Easy Deployment	56
6.3	Category 2: Security Risks of Wireless Networks Devices	58
6.3.1	Rogue APs	58
6.3.2	Wireless Clients	61

6.4	Category 3: Security Risks of Wireless Networks Communication	62
6.4.1	Lack of encryption	62
6.4.1.1	WEP	62
6.4.2	Lack of MAC Address Filtering	63
6.5	Summary	64

Chapter 7 - Wireless LANs Type of Attacks **65**

7.1	Introduction	66
7.2	Class 1: Passive Attacks	66
7.2.1	Open System Authentication	66
7.2.2	Shared Key Authentication	67
7.3	Class 2: Active Attacks	70
7.4	Class 3: Insertion Attacks	72
7.5	Class 4: Jamming Attacks	73
7.6	Summary	74

Chapter 8 - Wireless LANs Security and Countermeasures **75**

8.1	Introduction	76
8.2	WLAN Security Countermeasures	76
8.2.1	Countermeasures to Category 1: Inherent Security Risks of WLANs	76
8.2.1.1	Risk - Signal Overflow	77
8.2.1.2	Risk - Easy Deployment	77
8.2.2	Countermeasures to Category 2: WLAN Devices Risks	78
8.2.2.1	Risk – Rogue Wireless Access Points	78
8.2.2.2	Risk – Rogue Wireless clients	78
8.2.3	Countermeasures to Category 3: WLAN Communications Risks	79
8.2.3.1	Risk – WEP	79
8.2.3.1.1	WEP2	80
8.2.3.1.2	WPA (Wi-Fi Protected Access)	80
8.2.3.1.3	RADIUS (Remote Authentication Dial In User Service)	80
8.2.3.1.4	LEAP (Lightweight Extensible Authentication Protocol)	80
8.2.3.1.5	PEAP (Protected Extensible Authentication Protocol)	81
8.2.3.1.6	VPN (Virtual Private Networks)	81
8.2.3.2	Risk - MAC Address Filtering	83
8.3	Additional Monitoring Suggestion	84
8.4	Summary	85

Part III **87**

Chapter 9 - WISP Overview **88**

9.1	WISP Introduction	89
9.2	Part I: WISP Definitions	89
9.3	Part II: WISP Assessments	91
9.4	Part III: WISP Solutions	91
9.5	System Administration	92
9.6	Developing WISP	92

Chapter 10 – WISP User Guide **93**

10.1	WISP Definitions	94
10.2	WISP Assessments	95
10.3	WISP Solutions	97

Chapter 11 - WISP Administrator Guide	99
11.1 System Requirements	100
11.2 Installation Guide	100
11.3 Administration Structure	101
 Chapter 12 - Dissertation Conclusion and Future Research	
12.1 Introduction	108
12.2 The problem Statement	108
12.3 The Objectives	109
12.4 Future Research	111
12.5 Final Word	112
 Appendix A – Detailed Description	113
A.1 Computer Systems Hardware Components	113
A.2 Definitions	114
A.3 OSI Model	118
A.4 Wardriving	121
 Appendix B – Freeware Applications	125
B.1 NetStumbler	125
B.2 Nmap "Network Mapper"	125
B.3 AirSnort	126
B.4 WEP Crack	127
 Appendix C – Sample Security Solutions	128
C.1 Security Strategy	128
C.2 Security Awareness Program	129
C.3 Sample Security Policy	130
 References	133

List of Figures

Figure 1.1: Dissertation layout.	16
Figure 2.1: Some examples of computer systems components.	20
Figure 2.2: An example of a LAN.	22
Figure 2.3: An example of a MAN.	22
Figure 2.4: An example of a WAN.	22
Figure 3.1: A twisted pair and coaxial cable.	30
Figure 3.2: Fiber-Optic Cable.	31
Figure 3.3: Network Topologies.	32
Figure 4.1: A possible wireless LAN architecture.	40
Figure 4.2: An example of an access point.	42
Figure 4.3: An example of a wireless client.	42
Figure 5.1: Incidents reported by CERT.	48
Figure 5.2: Relationships between Info. Sec., Confidentiality, Integrity, and Availability	49
Figure 6.1: Signal overflow.	55
Figure 6.2: Easy deployment.	57
Figure 6.3: Easy deployment behind firewall.	57
Figure 6.4: A rogue AP installed by an end user.	59
Figure 6.5: A rogue AP installed by a hacker.	59
Figure 7.1: Open System Authentication.	67
Figure 7.2: Shared Key Authentication.	68
Figure 7.3: An example of a passive attack.	69
Figure 7.4: An example of an active attack.	71
Figure 7.5: An example of a jamming attack.	73
Figure 9.1: WISP Navigation Links	90
Figure 9.2: WISP Main Page	92
Figure 12.1 Research objectives relative to dissertation layout	111



List of Tables

Table 2.1: The OSI Model.	24
Table 2.2: The various 802.11 standards with their data transfer rates.	26
Table 3.1: Types of cables and transfer rates.	31
Table 6.1: Default Wireless SSIDs.	60
Table 6.2: WLAN Security Risks.	64
Table 7.1: WLAN Types of Attacks.	74
Table 8.1: Data protection technologies.	82
Table 8.2: Countermeasures to WLAN Security Risks.	85



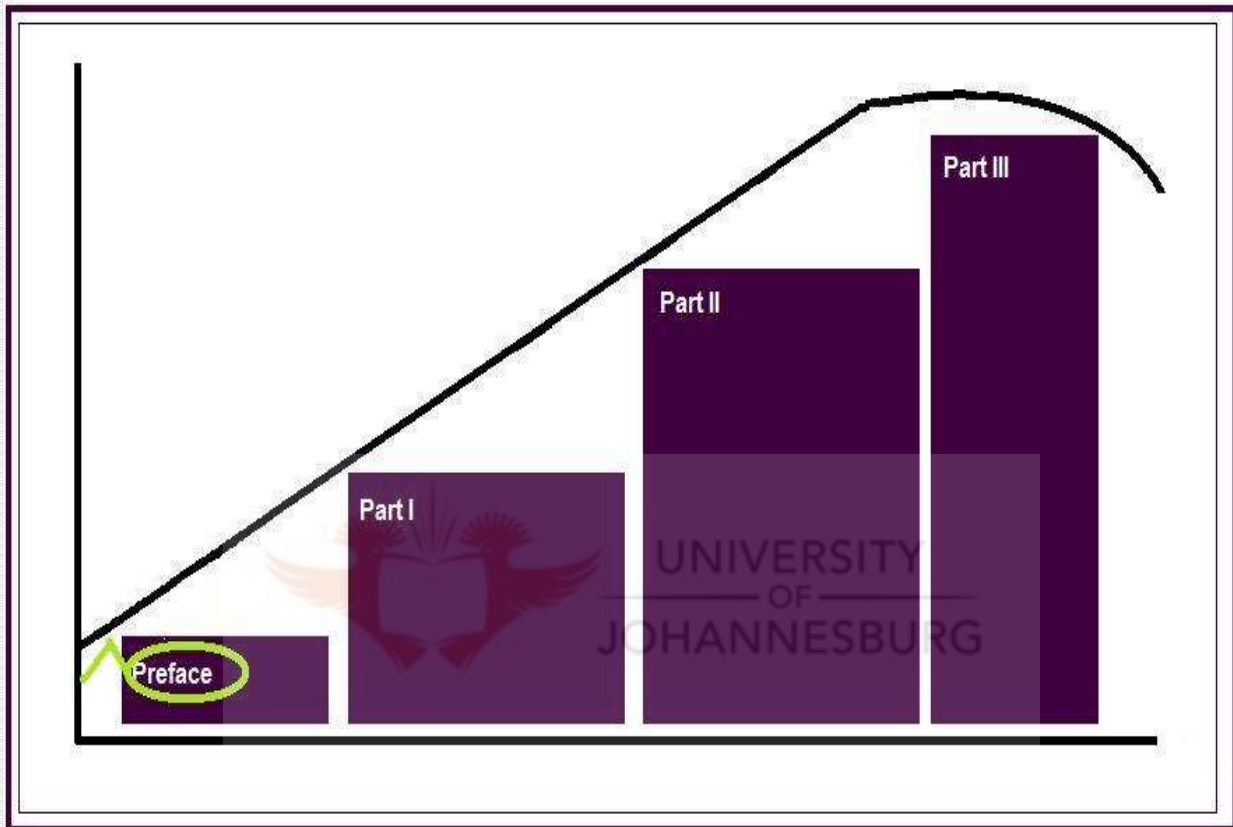


Writing Policy

Although this dissertation is an academic document, and conforms to the requirement of such a document, the dissertation is also intended to be read by a wider audience of interested parties. For that reason the writing style is a little more informal than could be expected. The term 'we' will be used throughout the document for the specific purpose to make it more readable for a wider audience.



Preface



Preface

Chapter 1 – Dissertation Overview

Chapter 1

Dissertation Overview



In this chapter, we will discuss:

Problem Statement	Page 13
Objectives	Page 13
Approach	Page 14
Deliverables	Page 14
Document Structure	Page 15

1.1 Introduction

In this chapter we will give an overview of the dissertation. We will start with the **problem statement**. Thereafter, we will discuss the **objective** of the research, and the **approach** used in this dissertation. The **dissertation layout** will be described at the end of this chapter.

The research will concentrate on wireless LANs (Local Area Networks), and leading wireless LAN protocols and standards. Wireless networking is a fairly new technology that is important in information technology (IT). Wireless technologies are new scientific concepts, and scientific concepts have always faced challenges prior to maturity. The major challenge for wireless technologies is **security** [7].

1.2 Problem Statement

Wireless Local Area Networks (WLANs) use radio signals to transmit data. Contrary to the wired LAN technologies which are often protected by physical security, wireless signals are accessible to everyone within a certain range. Physical restrictions are limited, leading to an increased level of insecurity. This “Signal overflow beyond physical walls”, is one example of challenges faced by wireless LANs.

It is challenging for managers to introduce wireless networks and properly manage the security of wireless networks. Security problems of wireless networks are the main reason for wireless networks not being rolled out optimally [1]. Tools to support such management are available, but spread over many books, papers and websites. No real centralized place exists where all essential support can be found.

1.3 Objective

The research objectives are:

- Review of computers and computer networks including both wired and wireless networks.
- Introduce the concept of Information Security emphasizing Network Security.
- Understand how the wireless LANs work and investigate the security risks of wireless LANs.
- Propose a solution for securing wireless LANs.
- Demonstrate how a web portal (WISP) can be used to consolidate support tools and manage the information security requirements of a wireless LAN.

1.4 Approach

In this dissertation, we aim to present to both specialist and non-specialists in the IT industry the information needed to protect a wireless network. The research will discuss answers for the following questions:

- What is a wireless LAN?
- What are the devices used in wireless LANs?
- What are the inherent security risks of wireless networks?
- What are the new security risks unique to a WLAN?
- What kind of attacks can be launched against WLANs?
- How do we protect the wireless LAN devices?
- How do we protect the wireless LAN communication?

The approach is to investigate the information security requirements for wireless networks, and then compare that with the information security requirements for wired networks. The extra requirements needed for wireless networks security are then identified and discussed [1].

The dissertation will first discuss the introductory concepts: Computer Systems, Wired Networks, Wireless Networks, and Information Security. Secondly, the different categories of information security risks for wireless networks will be discussed.

Thirdly, the type of attacks that can be launched against wireless networks will be discussed. Fourthly, the wireless LAN security solutions will be studied. Lastly, WISP (A Wireless Information Security Portal), a dynamic portal to support the management of wireless LAN security will be introduced, and demonstrated.

1.5 Deliverables

The main deliverable of this dissertation will be a portal called Wireless Information Security Portal (WISP), which will be a functional portal to support the management of wireless networks information security. WISP will be developed using LAMP (LINUX, APACHE, MYSQL and PHP). LINUX will be used as the operating system, APACHE is the web server, MYSQL is the relationship database management system and PHP is the programming language.

1.6 Document Structure

This document consists of three parts, namely: Introductory concepts, Wireless Security, and WISP. Figure 1.1 depicts the layout of this dissertation.

Part I consist of four chapters, Chapter 2, 3, 4 and 5. Part I is the introductory concepts.

Chapter 2 defines computer systems and computer networks. Different computer networks types and standards are discussed. Wired Networks Transmission Media, Topologies, Standards, and Devices will be discussed in chapter 3. Chapter 4 discusses Wireless Networks Types, Standard, and Devices, and some advantages and disadvantages of WLANs are also listed. In chapter 5, The Confidentiality, Integrity, and Availability characteristics of Information Security are discussed, as well as the five pillars of Information Security.

Part II consists of three chapters, chapter 6, 7, and 8. Part II is all about wireless networks security.

Chapter 6 discusses the security risks for wireless networks. Information security risks unique to wireless LANs are discussed in this chapter. Chapter 7 discusses the types of attacks that can be launched against wireless LANs are. In chapter 8, countermeasures required for securing wireless LANs are named and discussed in a structured way in order to provide insight into tools available.

Part III consists of four chapters, Chapter 9, 10, 11, and 12. Part III is about WISP, a demo portal to support the management of WLAN security.

An overview of WISP is introduced in chapter 9. Chapter 10 discusses the WISP user guide. In chapter 11, the administrator guide is discussed. In Chapter 12, a conclusion to this dissertation is reached and possible future research is discussed.

The document includes three appendices namely, Appendix A, Appendix B and Appendix C. The list of references used in the document follows the appendices.

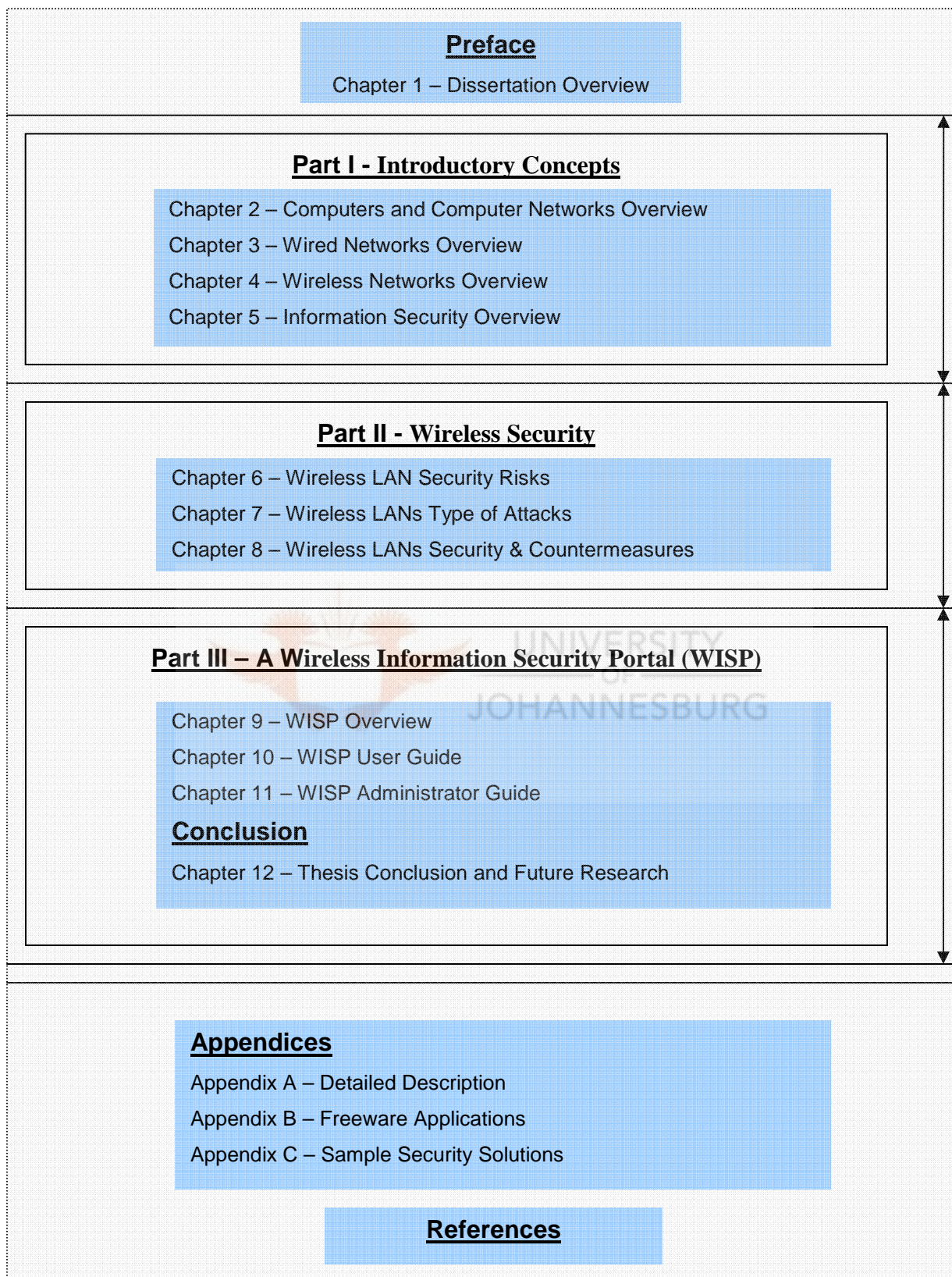
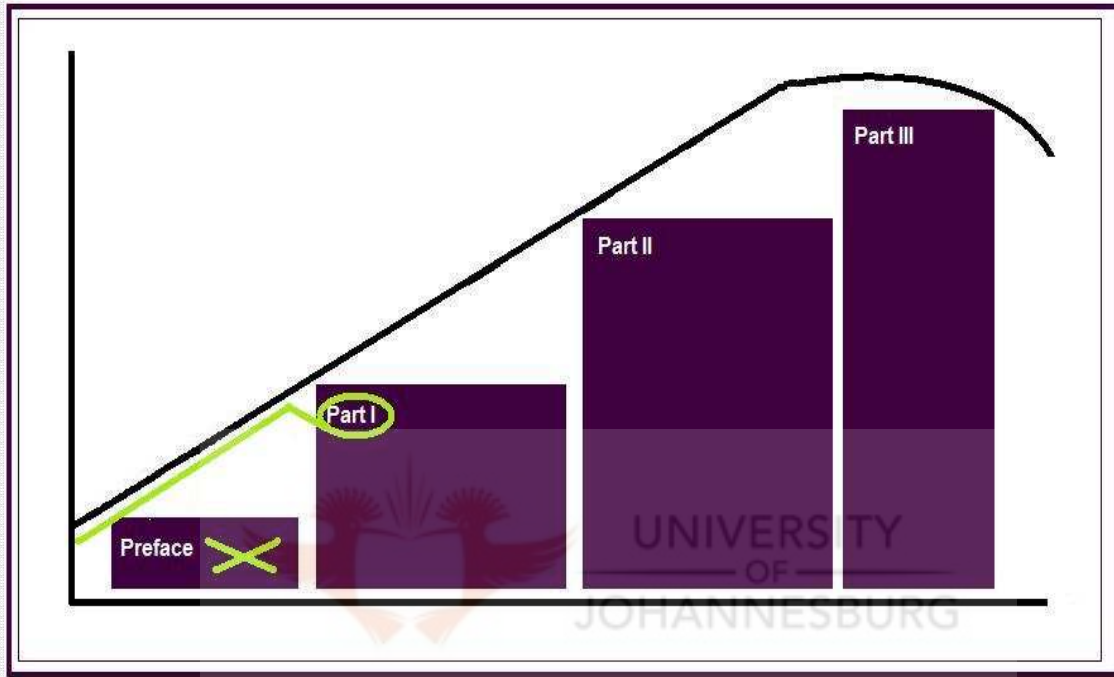


Figure 1.1: Dissertation layout.

Part I



Part I

Chapter 2 – Computers and Computer Networks Overview

Chapter 3 – Wired Networks Overview

Chapter 4 – Wireless Networks Overview

Chapter 5 – Information Security Overview

Chapter 2

Computers and Computer Networks Overview



CHAPTER OBJECTIVES

In this chapter, we will discuss:

Computer Systems	Page 19
Computer Networks	Page 21
Computer Network Types	Page 21
Computer Network Architecture	Page 23
Computer Network Standards	Page 23



2.1 Introduction

In this chapter we will give an overview of computers and computer networks. We will discuss computer networks, and some of the different types of computer networks, and then proceed to protocols and technologies used in those computer networks.

Before we can talk about computer networks, we first need to know what a computer system is, and what a computer system consist of. To understand how computer networks operate, we also need to understand the basis elements of computer networks. The next paragraph is a quick review of Computer Systems. After that we will discuss Computer Networks.

2.2 Computer Systems

The computer architecture is described by the building blocks of the computing system [13]. These building blocks can be grouped into two main categories namely, hardware and software. These hardware and software components together create the entire computing system.

2.2.1 Hardware Components of the Computer Systems

The hardware component of the computing system has five basic elements [13]:

- System Unit
- Input Devices
- Output Devices
- Storage Devices
- Communication Devices

Figure 2.1 shows some examples of computer systems components. Refer to Appendix A for more details about these elements.

2.2.2 Software Components of the Computer Systems

The software element of the computer system consists of the programs that control or operate the computer and its devices. Two types of software are operating system and application software. The operating system is the primary program that controls the operations of the computer [7]. Some widely used operating systems include Windows XP, Windows Vista, Ubuntu Linux and UNIX.

The application software consists of programs that functions together to carry out a specific task [7]. Some widely used application software includes Microsoft Office, Web browsers, and multimedia players.

We have briefly discussed the Computer Systems, and we have discussed the hardware components of the computer system and the software components as well. Our next topic is the Computer Network, where we will discuss the Computer Network Types, and Architectures.

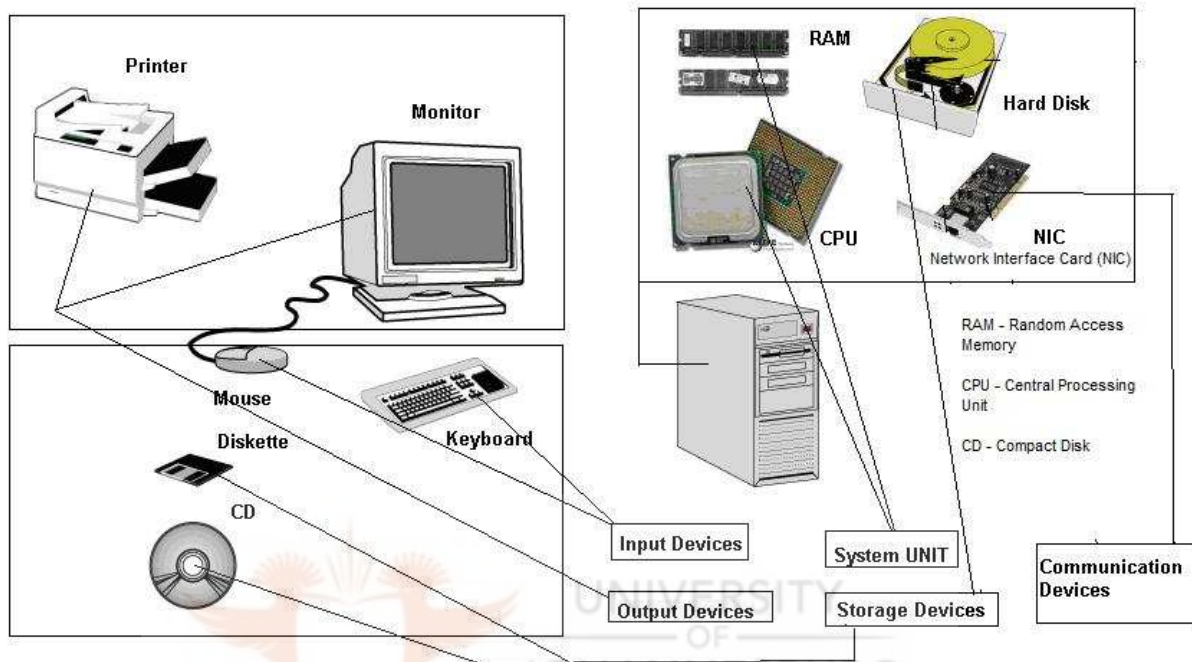


Figure 2.1: Some examples of computer systems components



2.3 Computer Networks

A computer network is composed of multiple connected computers that communicate over a wired or wireless medium to share resources. For instance, a home computer network may consist of two or more computers that share files and a printer using the network. The next section discusses the Computer Network Types.

2.3.1 Computer Network Types

Some types of computer networks are Local Area Networks (LAN), Metropolitan Area Networks (MAN) and Wide Area Networks (WAN). The main difference among these classifications is their area of coverage [40].

2.3.1.1 LANs

A local area network (LAN) is a network connecting computers in a relatively small area such as a building. Because the network is known to cover only a small area, optimizations can be made in the network signal protocols that permit data rates up to 1000Mb/s. LANs are communications network connecting computers by wire, or wireless link. LANs serve as parts of an organization located close to one another, generally in the same building. LANs allow users to share software, hardware and data [40]. Figure 2.2 shows an example of a LAN.

2.3.1.2 MANs

A Metropolitan Area Network (MAN) is a data network designed for a town or city. In terms of geographic breadth, MANs are larger than local-area networks (LANs), but smaller than wide-area networks (WANs). MANs are usually characterized by very high-speed connections using fiber optical cable or other digital media [40]. Figure 2.3 shows an example of a MAN.

2.3.1.3 WANs

A Wide Area Network (WAN) is a computer network that covers a broader area. i.e., any network whose communications links cross metropolitan, regional, or national boundaries. Or, less formally, a network that uses public communications links [53]. WAN communications links cross metropolitan, regional, or national boundaries. WANs use routers and public communications links. The largest and most well-known example of a WAN is the Internet [53]. Figure 2.4 shows an example of a WAN.

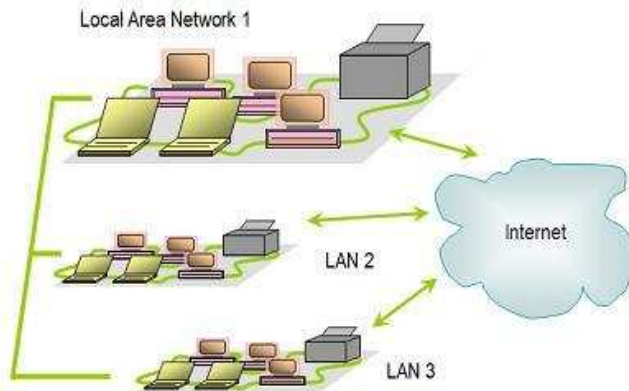


Figure 2.2: An example of a LAN.

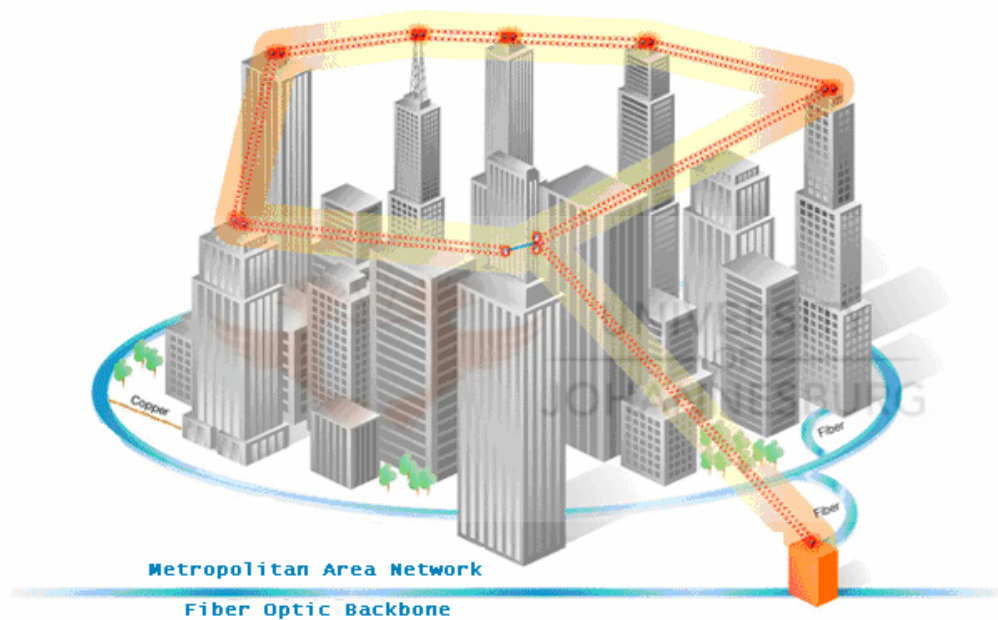


Figure 2.3: An example of a MAN.

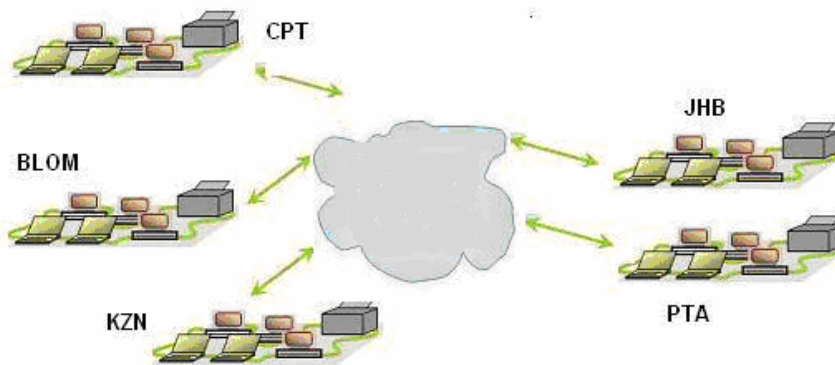


Figure 2.4: An example of a WAN.

We have discussed the Computer Network, and Computer Network Types, namely: LANs, MANs and WANs. Our next discussion is on Computer Network Architectures.

2.3.2 Computer Network Architectures

Computer network architecture specifies the design of a computer network, for example a computer network consisting of multiple connected nodes that communicates over a wired or a wireless medium. Two examples of network architectures are: client/server networks and peer-to-peer networks. The following paragraphs discuss these network architectures [40].

2.3.2.1 Client/Server Networks

Client/Server is a network architecture which separates a client (often an application that uses a graphical user interface) from a server. Each instance of the client software can send requests to a server. Specific types of servers include web servers, application servers, file servers, terminal servers, and mail servers. While their purposes vary somewhat, the basic architecture remains the same.

2.3.2.2 Peer-to-Peer Networks

A peer-to-peer (or P2P) computer network relies primarily on the computing power and bandwidth of the participants in the network rather than concentrating it in a relatively low number of servers [56]. P2P networks are typically used for connecting nodes via largely ad hoc connections. Such networks are useful for many purposes. Sharing content files (see file sharing, in Appendix A) containing audio, video, data or anything in digital format is very common [56]. The next section discusses some of the computer network standards.

2.3.3 Computer Network Standards

Computer networks connect terminals, devices, and computers from many different manufacturers across many types of networks, such as metropolitan areas, local areas, and wide areas. The connection device can be either wired or wireless. For the different devices on various types of networks to be able to communicate, the network must use similar techniques of moving data through the network from one application to another. For example, an IBM server with UNIX as operating system cannot communicate directly with a Dell PC running Windows XP. Some form of translation must occur for these two types to communicate [13].

To alleviate the problems of incompatibility and ensure that hardware and software components can be integrated into any network, organizations such as ANSI (American National Standard

Institute) [13], and IEEE – (Institute of Electrical and Electronics Engineers) [13] propose, develop, and approve network standards. A network standard defines guidelines that specify the way computers access the medium to which they are attached, the type(s) of medium used, the speed used on different types of networks, and the type of the physical cable and /or the wireless technology used [13].

A standard that outlines characteristics of how two network devices communicate is called a protocol. A protocol would define packet format, coding scheme, error handling, and sequencing techniques. Software and hardware manufacturers design their products to meet the guidelines specified in a particular standard [13]. The following sections discuss some of the more widely used network standards and protocols for both wired and wireless networks. These network standards and protocols work together to move data through a network. Thus, as data moves through the network from one application to another, it may use one or more of these standards. We will discuss six such standards.

2.3.3.1 OSI Model

We have stated that protocols allow incompatible systems to communicate. A protocol that would allow any two different types of systems to communicate regardless of their underlying architecture is called an open system. The Open Systems Interconnection Model (OSI Model) is a layered, abstract description for communications and computer network protocol design, developed by the International Organization for Standardization (ISO) as part of the Open Systems Interconnection (OSI) initiative. It is also called the OSI seven layer model [49].

The OSI model is a seven layer model (Table 2.1). Each layer performs a specific function and communicates with the layer directly above and below it. Higher layers deal more with user services, and the lower layers deal more with the actual transmission of data [9]. For more details refer to the OSI Model in Appendix A.

OSI Model			
	Data unit	Layer	Function
Host layers	Data	Application	Network process to application
		Presentation	Data representation and encryption
		Session	Inter host communication
	Segments	Transport	End-to-end connections and reliability (TCP)
Media layers	Packets	Network	Path determination and logical addressing (IP)
	Frames	Data link	Physical addressing (MAC & LLC)
	Bits	Physical	Media, signal and binary transmission

Table 2.1: The OSI Model

2.3.3.2 Ethernet

Ethernet is a local-area network (LAN) protocol developed by Xerox Corporation in cooperation with Intel in 1976 [38]. It is one of the most widely implemented LAN standards. Each node attempts to transmit data when it determines the network is available to receive communications. If two nodes on the Ethernet network attempt to send data at the same time, a collision will occur, and the nodes must attempt to send their message again [13]. Ethernet is usually based on a bus topology, which is a wired network topology [13]. We will discuss Network Topology in chapter 3.

2.3.3.3 Token Ring

The token ring standard specifies that computers and devices on the network share or pass a special signal, called a token, in a unidirectional manner and in a preset order.

A token is special series of bits that function like a ticket. The device with the token can transmit data over the network, and only one token exist per network [13].

Token ring is based on a ring topology, which is also a wired network topology. We will discuss this standard as well fully, in chapter 3.

2.3.3.4 TCP/IP

The TCP/IP is short for Transmission Control Protocol/ Internet Protocol, TCP/IP is a network standard, and a protocol, that defines how messages (data) are routed from an end point of a network to the other end, ensuring the data arrives correctly [45].

TCP/IP describes rules for dividing messages into small pieces called packets; providing addresses for each packets checking for and detecting errors; sequencing packets; and regulating the flow of messages along the network. TCP/IP has been adopted as a network standard for internet communication. Thus, all hosts on the internet follow the rules defined in this standard [46].

2.3.3.5 802.11

Developed by IEEE – (Institute of Electrical and Electronics Engineers), 802.11 is a series of network standards that specifies how two wireless devices communicate over air with each other [13]. By using the 802.11 standard, computers or devices that have built-in wireless capability or the appropriate wireless client can communicate via radio waves with other computers or devices. Table 2.2 outlines various 802.11 standards and their transfer rates. We will discuss these various 802.11 standards in detail in chapter 4.

The term Wi-Fi (Wireless Fidelity) is a consortium of wireless equipment manufacturers and software providers that was formed to promote wireless network technology [11]. One of their

goals is to test and certify that wireless products adhere to the IEEE 802.11 standards to ensure product interoperability.

Standard	Transfer Rates
802.11	Up to 2 Mbps
802.11a	Up to 54 Mbps
802.11b	Up to 11 Mbps
802.11g	Up to 54Mbps and higher

Table 2.2: The various 802.11 standards with their data transfer rates.

2.3.3.6 WiMAX

WiMAX (Worldwide Interoperability for Microwave Access), also known as 802.16, is a newer network standard developed by IEEE that specifies how wireless devices communicate over the air in a wide area [13]. By using the WiMAX standard, computers or devices with a built-in WiMAX wireless capability, or the appropriate wireless network card, can communicate via radio waves with other computers or devices via a WiMAX tower. The WiMAX tower, which can cover up to 50 KM radius, connects to the internet or to another WiMAX tower [13].

The WiMAX Forum is a wireless industry association of more than 240 suppliers and service providers dedicated to developing specifications and testing equipment. Current WiMAX standards have data transfer rates from 54Mbps to 70 Mbps. The WiMAX standard, similar to the Wi-Fi standard, connects mobile users to the internet via hotspots. The next generation of PDAs and game consoles also plans to support the WiMAX standard [13].



2.4 Summary

The computer system consists of two main categories: hardware and software. These hardware and software elements together create the entire computing system.

The five basic elements of a hardware component of the computing system are: the System Unit, the Input Devices, the Output Devices, the Storage Devices and the Communication Devices. The software element of the computer system consists of the programs that control or operate the computer and its devices.

Some types of computer networks are Local Area Networks (LAN), Metropolitan Area Networks (MAN) and Wide Area Networks (WAN). The main difference among these classifications is their area of coverage.

Incompatible systems communicate through protocols. The Open Systems Interconnection Model (OSI Model) is a layered, abstract description for communications and computer network protocol design, developed by the International Organization for Standardization (ISO) as part of Open Systems Interconnection (OSI) initiative.

The wireless 802.11 standard is developed by IEEE – (Institute of Electrical and Electronics Engineers). 802.11 is a series of network standards that specifies how two wireless devices communicate over air with each other.

WiMAX (Worldwide Interoperability for Microwave Access), also known as 802.16, is a newer network standard developed by IEEE that specifies how wireless devices communicate over the air in a wide area.

The next chapter discusses Wired Networks. We will discuss the different technologies that make up wired networks.

Chapter 3

Wired Networks Overview



CHAPTER OBJECTIVES

In this chapter, we will discuss:

Wired Networks Transmission Media	Page 29
Wired Networks Topologies	Page 31
Wired Networks Standards	Page 33
Wired Networks Devices	Page 34
Wired Networks Advantages and Disadvantages	Page 35

3.1 Introduction

Computer networks can be defined as a data communications system that interconnects computer systems at various different sites. Today's networks use two different communication channels, and sometimes a combination of the two, namely, wired and wireless networks. In chapter 2, we had an overview of computers and computer networks. In this chapter we will discuss wired networks.

This chapter will discuss wired networks transmission media, the different wired network topologies, and some of the standards of wired networks. We will highlight some of the devices used in a wired network infrastructure. We will also discuss some of the advantages and disadvantages of wired networks. The next paragraph discusses wired network transmission media.

3.2 Wired Networks Transmission Media

At the lowest level, all computer communication involves encoding data in a form of energy, and sending the energy across a transmission medium. For example, electric current can be used to transfer data across wires or radio waves can be used to carry data through the air [8].

3.2.1 Copper Wires

Copper wire is a transmission medium where signals travel in the form of electric current. Although wires can be made from various metals, many networks use copper because of its low resistance to electric current and signal can travel further [13]. The type of wiring used for computer networks is chosen to minimize interference. Interference arises because an electric signal traveling across a wire acts like a miniature radio station – the wire emits a small amount of electromagnetic energy, which can be travel through the air [8].

To minimize interference, networks use one of two basic wiring types: twisted pair or coaxial cable. Twisted pair wiring is also used by telephone systems. The simple twists change the electrical properties of the wire, and help make it suitable for use in a network [13]. The twists help limit the electromagnetic energy the wire emits, and help electric currents on the wire from radiating energy that interferes with other wires.

The second type of copper wiring used in networks is coaxial cable. This type of wiring is used for cable TV. Coaxial cable provides even more protection from interference than twisted pair.

Instead of twisting wires around one another to limit interference, a coaxial cable consists of a single wire surrounded by a heavier metal shield [13]. Figure 3.1 shows a picture of a twisted pair and coaxial cable.

3.2.2 Fiber-Optic Cable

The core of fiber-optic cable consists of dozen or hundreds of thin strands of glass or plastic that use light to transmit signals [8]. Each strand, called an optical fiber, is as thin as a human hair. Inside the fiber-optic cable, an insulating glass cladding and a protective coating surround each fiber (Figure 3.2) [13].

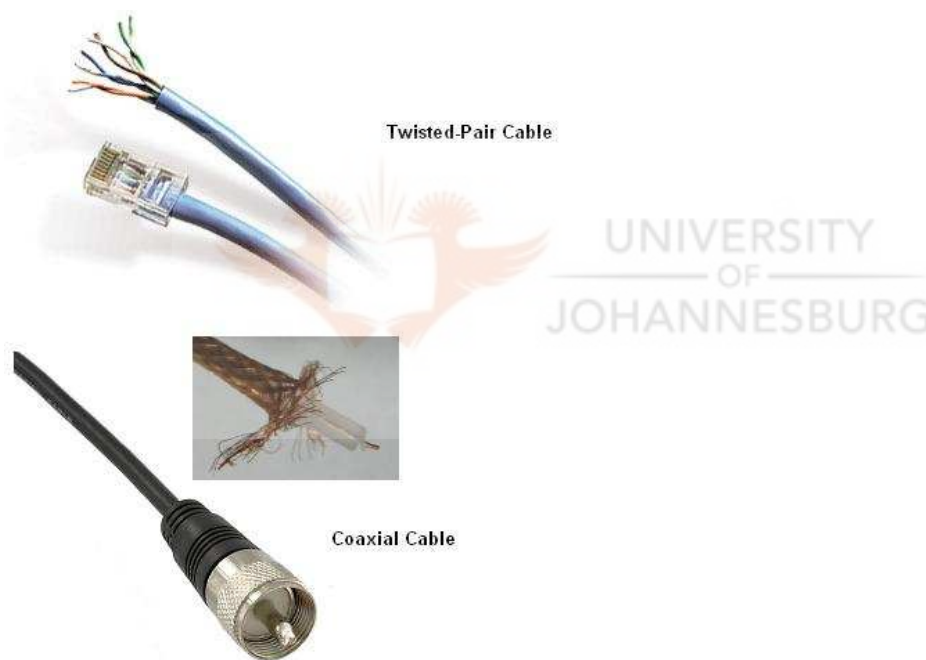


Figure 3.1: A twisted pair and coaxial cable.

Fiber-optic cables have the following advantages over cable that use wire, such as twisted-pair and coaxial cables [13]:

- Capability of carrying significantly more signals than wire cables.
- Faster data transmission
- Better security for signals during transmission because they are less susceptible to interference

Disadvantages of fiber-optic cable are that it costs more than copper wires and can be difficult to install and modify. Despite these limitations, many telephone companies are replacing existing

telephone lines with fiber-optic cables. Businesses also are using fiber-optic cables in high-traffic networks or as the backbone in a network [13].

As a summary, physical transmission media used in wired networks include twisted-pair cable, coaxial cable, and fiber-optic cable. Table 3.1 lists the transfer rates of LANs using various physical transmission media.



Figure 3.2: Fiber-Optic Cable

Types of Cables	Transfer Rates
Twisted-Pair Cable	From 4 Mbps up to 1 Gbps
Coaxial Cable	10 Mbps
Fiber Optic Cable	From 10Mbps up to 10 Gbps

Table 3.1: Types of cables and transfer rates

N.B: Note that the speed depends on the type of network. (See paragraph 2.3.1).

3.3 Wired Networks Topologies

A system connecting different devices such as PCs, printers and storage servers is a network, and each device can be refer to as a node on the network. Each node in a network serves a specific purpose for one or more individuals [8]. The connection strategy that is adopted by the network designer is the network topology. Hence, network topology can be described as the physical and logical relationship of nodes in a network.

Three commonly used topologies are bus, ring, and star. Networks usually use combinations of these topologies. The best topology depends on the type of devices and user needs. What works well for one group may perform dismally for another [13].

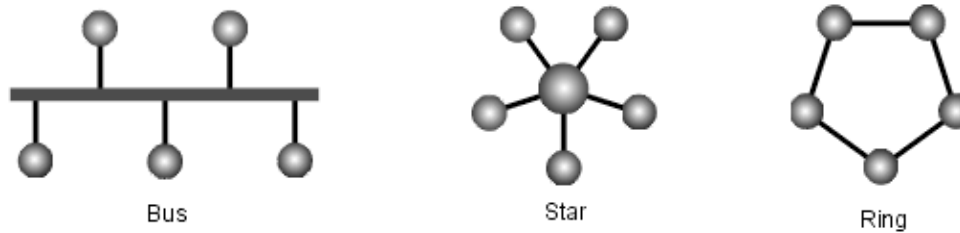


Figure 3.3: Network Topologies.

3.3.1 Bus Network

A bus topology consists of a single central cable, to which all nodes connect (Figure 3.3). The bus is the physical cable that connects the nodes [13]. The bus network transmits data, instructions, and information in both directions. One advantage of the bus network is that nodes can be attached and detached at any point on the bus without disturbing the rest of the network. Another advantage is that failure of one node usually does not affect the rest of the bus network. The major risk to a bus network is that the bus itself might become inoperable. If that happens, the network remains inoperative until the bus is back in working order [13].

3.3.2 Ring Network

On a ring network, a cable forms a closed loop (ring) with all nodes arranged along the ring (Figure 3.3). Data transmitted on a ring network travels from node to node around the entire ring, in one direction [13]. If a node on a ring network fails, all nodes before the failed node are unaffected, but those after the failed node cannot function. A ring network can span a larger distance than a bus network, but it is more difficult to install [13].

3.3.3 Star Network

On a star network, all of the nodes on the star network connect to a central node (Figure 3.3). The central node that provides a common connection point for nodes on the network, often called the hub [13]. All data transmitted passes through the hub. Star Networks are fairly easy to install and maintain. Nodes can be added to and removed from the network with no disruption to the network. If one node fails, only that node is affected, the other nodes continue to operate normally. However, if the hub fails, the entire network is inoperable until the hub is fixed or replaced [13].

3.4 Wired Networks Standards

3.4.1 Ethernet

As stated in chapter 2, Ethernet is a local-area network (LAN) protocol developed by Xerox Corporation in cooperation with Intel in 1976 [38]. It is one of the most widely implemented LAN standards. Ethernet has been standardized as IEEE 802.3. The combination of the twisted pair versions of Ethernet for connecting end systems to the network, along with the fiber optic versions for site backbones, has become the most widespread wired LAN technology. It has been in use from the 1990s to the present [38].

In its original version, an Ethernet LAN consisted of a single coaxial cable, called the ether, to which multiple computers connect [9]. Engineers use the term segment to refer to the Ethernet coaxial cable. A given Ethernet segment is limited to 500 meters in length, and the standard requires a minimum of 3 meters between each pair of connection [9]. The original Ethernet hardware operated at a bandwidth of 10 Megabits per second (Mbps), a version known as Fast Ethernet operates at 100 Mbps, and the most recent version known as Gigabit Ethernet operates at 1000 Mbps or 1 Gigabit per second (Gbps) [8].

In an Ethernet LAN, each node attempts to transmit data when it determines the network is available to receive communications. If two nodes on the Ethernet network attempt to send data at the same time, a collision will occur, and the nodes must attempt to send their message again [13].

3.4.2 Token Ring

The token ring standard specifies that computers and devices on the network share or pass a special signal, called a token, in a unidirectional manner and in a preset order. A token is special series of bits that function like a ticket [13]. The device with the token can transmit data over the network, and only one token exist per network. When a computer need to send data, the computer must wait for permission before it can access the network. Once it obtains permission, the sending computer has complete control of the ring; no other transmissions occur simultaneously [13].

Token ring is based on a ring topology, although it can use star topology. The token ring standard defines guidelines for the physical configuration of a network. Some token ring networks connect up to 72 devices; others use a special type of wiring that allows up to 260 connections. The data transfer rate on a token ring network can be 4 Mbps, 16 Mbps, or up to 100 Mbps [13].

3.5 Wired Network Devices

A network device, also referred to as a communication device, is any type of hardware capable of transmitting data, instructions, and information between a sending device and a receiving device. The sending device sends data through the transmission medium. In this section we are discussing the wired communication devices, and one example such a device is a modem [13].

3.5.1 Modems

Computers process data as digital signal. Data, instructions, and information travel along a network channel in either analog or digital form, depending on the network channel. An analog signal consists of a continuous electrical wave. A digital signal consists of individual electrical pulses that represent bits grouped together into bytes [13].

For network channels that use analog signals such as telephone lines, the modem converts the analog signals to digital signals, and vice versa [13]. Some different types of modems are: dial-up modems, ISDN modems, Cable TV modems, and DSL modem.

3.5.2 Network Interface Card (NIC)

Network Interface Card sometimes called a network card, is an adapter card, or PC Card that enable a computer to access a network [13]. Although some computers have networking capabilities integrated, most personal computers on a LAN contain a network card. The network card coordinates the data, instructions, and information to and from the computer containing the network card.

Many of the network cards available on the market, have more than one type of port, which enable different types of cables to attach to the card. A network card follows the guidelines of a particular network communication standard, such as Ethernet or Token ring. An Ethernet card is the most common type of network card.

3.5.3 Routers

A router is a communication device that connects multiple computers or other routers together, and transmits data to its correct destination on the network [13]. A router can be used on any size of network. On the largest scale, routers along the Internet backbone forward data packets to their destination using the fastest available path. For smaller business and home networks, a router allows multiple computers to share Internet connections. Routers connect from 2 to 250 computers [13].

To prevent unauthorized access, most routers have built-in firewalls. Some also have built-in antivirus protection, some support wireless communications, eliminating the need for a separate wireless access point (a wireless network device – discussed in the next chapter). However, if the network has a separate wireless access point, it connects to the router via a cable.

3.6 Wired Networks Advantages and Disadvantages

3.6.1 Wired Network Advantages

a) Fast Data Transmission Speeds

Wired connections can reach networking speeds of up to 1000 Mbps with Gigabit Ethernet networking equipment, necessary for bandwidth hungry users such as avid graphic designers or users downloading large media files [13]. However, for most users 54 or 108 Mbps networking speeds are more than sufficient for everyday networking activities such as emailing, surfing the web, downloading files, music and video, accessing corporate information.

b) Reliable Connections

Physical, fixed wired connections are not prone to interference and fluctuations in available bandwidth, which can affect some wireless networking connections [13].

3.6.2 Wired Network Disadvantages

a) High Cost

Compared with wireless network, wired network have a high cost of implementation, and maintenance. A physical wire is needed for every node on the network.

b) Difficult to Maintain

It is difficult to maintain wired networks compared with wireless networks. The larger the wired networks coverage, the more sophisticated the design of wired networks tends to be.



3.7 Summary

Computer networks consist of nodes sometimes at different sites interconnected by a data communication system. Today's computer networks use two different communication channels, and sometime a combination of the two, namely, wired and wireless networks.

Computer networks communication involves encoding data in a form of energy, and sending the energy across a transmission medium. The transmission media used in wired networks include twisted-pair cable, coaxial cable, and fiber-optic cable. The three commonly used network topologies are bus, ring, and star. Networks usually use combinations of these topologies.

Wired Networks enjoy advantages like, speed, and reliability, and drawbacks of wired networks include high cost.

The next chapter discusses Wireless Networks. We will describe types of wireless networks, and we will also discuss wireless networks devices.



Chapter 4

Wireless Networks Overview



CHAPTER OBJECTIVES

In this chapter, we will discuss:

Wireless Network Types	Page 38
Wireless Network Devices	Page 41
Wireless Networks Advantages and Disadvantages	Page 43

4.1 Introduction

While the term wireless network may technically be used to refer to any type of network that is wireless, the term is most commonly used to refer to a telecommunications network whose interconnections between nodes is implemented without the use of wires [55]. Wireless networks are generally implemented with some type of information transmission system that uses electromagnetic waves, such as radio waves, for the carrier and this implementation usually takes place at the physical level or layer of the network [55]. See Table 2.1 in chapter 2.

In this chapter we are going to discuss the different types of wireless networks, devices used to set up the wireless network, transmission media used, and conclude this chapter by discussing the advantages and disadvantages of the wireless network.

4.2 Wireless Network Types

Some types of wireless networks include Wireless PAN (Personal Area Network) and Wireless LAN (Local Area Network). Each of the categories will now be examined in detail.

4.2.1 Wireless PAN

A personal area network (PAN) is a computer network used for communication among computer devices (including telephones and personal digital assistants) close to one person [58]. The reach of a PAN is typically a few meters. PANs can be used for communication among the personal devices themselves or for connecting to a higher level network and the internet [58].

Wireless PAN can be made possible with network technologies such as Bluetooth and Infrared Data Association (IrDA).

4.2.1.1 Bluetooth

Bluetooth is a network standard, specifically a protocol, that defines how two Bluetooth devices use short range radio waves to transmit data [13]. The data transfer between devices at a rate of up to 2 Mbps. Bluetooth devices covers a range of 10 meters and can be extended to 100 meters with additional equipments [13].

Example of Bluetooth-enabled devices can include desktop computers, notebook computers, handheld computers, smart phones, headsets, microphones, digital cameras, fax machines and printers.

For computers and devices not Bluetooth-enabled, one can purchase a USB Bluetooth Adapter that will convert an existing USB port into a Bluetooth port.

4.2.1.2 IrDA

The IrDA is a standard used to transmit data wirelessly over the infrared light. Electronic equipment with IrDA can transfer data at rates from 115 Kbps to 4 Mbps between their IrDA ports [13]. Infrared requires a line-of-sight transmission; that is, the sending device and the receiving device must be in line with each other so that nothing obstructs the path of the infrared light wave.

Because Bluetooth does not require line-of-sight transmission, some experts predict that Bluetooth will replace infrared [13]. The next section discusses wireless Local Area Networks (LANs).

4.2.2 Wireless LANs

A Wireless LAN (WLAN) is a wireless local area network, which is the linking of two or more computers without using wires [22]. WLANs provide wireless network communication over short distances using radio or infrared signals instead of traditional network cabling. A WLAN typically extends an existing wired local area network. WLANs are built by attaching a device called the access point (AP) to the edge of the wired network [22]. Clients communicate with the AP using a wireless network adapter similar in function to a traditional Ethernet adapter. Figure 4.1 shows a possible Wireless LAN architecture [22].

The wireless LAN is identified by their standard, the 802.x. The next paragraph will discuss the 802.11 standards.

4.2.2.1 802.11

The 802.11 refers to a family of specifications developed by the IEEE (Institute of Electrical and Electronics Engineers) for WLAN technology [25]. The 802.11 specifies an over-the-air interface between a wireless client and a base station or between two wireless clients. 802.11 per se provide 1 or 2 Mbps transmission in the 2.4 GHz ISM band (ISM—Industrial Scientific Medical) [25].

4.2.2.2 802.11a

802.11a describes the wireless networking standard for a WLAN that operates in the 5 GHz radio band. 802.11a-based WLANs can achieve a maximum speed of 54 Mbps, providing nearly five-times faster networking data rate than 802.11b, and can handle more traffic than 802.11b-based networks [56].

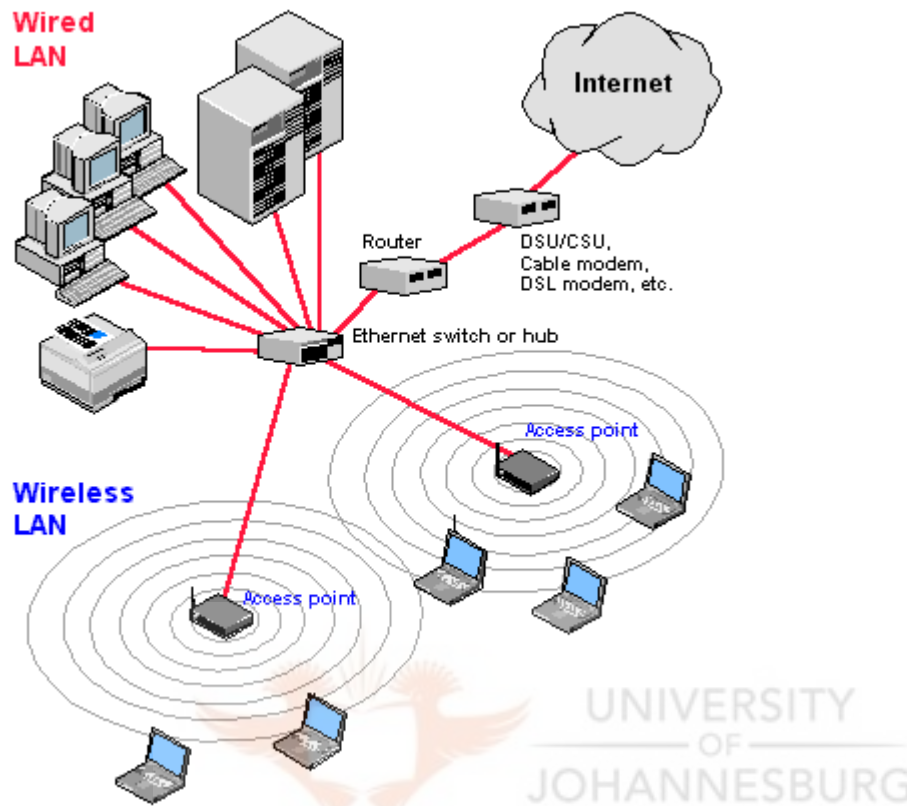


Figure 4.1: A possible wireless LAN architecture.

4.2.2.3 802.11b

The 802.11b allow network devices to communicate with each other using a 2.4-gigahertz radio frequency [56]. The data transfer rate of the 802.11b can reach up to 11 megabits per second.

The latest 802.11b standard is based on a technology called Direct Sequence Spread Spectrum (DSSS). DSSS spreads the networked data between several channels in the radio frequency band. This method reduces interference and quickens the speed [24].

4.2.2.4 802.11g

802.11g is a proposed standard, describing a wireless networking method for a WLAN that operates in the 2.4 GHz radio band (ISM—Industrial Scientific Medical frequency band). 802.11g-based WLANs will be able to achieve a maximum speed of 54 Mbps. 802.11g is backward compatible with the 802.11b standard [24]. The next section discusses wireless network devices.



4.3 Wireless Network Devices

In general, Wireless network devices include, among other things, the following:

- Wireless Access Point
- Wireless Modems
- Wireless Client

4.3.1 Wireless Access Point

A wireless access point (WAP or Wireless AP) is a device that "connects" wireless communication devices together to create a wireless network [13]. The WAP is usually connected to a wired network, and can relay data between devices on each side. Many WAPs can be connected together to create a larger network that allows "roaming". In contrast, a network where the client devices manage themselves is called an ad-hoc network [13]. Figure 4.2 displays an example of an access point.

4.3.2 Wireless Modems

A wireless modem uses radio transmission technology to transmit data between remote locations. Wireless modems are often used by mobile clients in locations where access to a landline connection is not feasible [13]. Wireless broadband Internet uses many frequency bands. Wireless broadband modems offer similar performance to cable modems [13]. A broadband wireless system can deliver up to 30 Mbps data capacity in a 6 MHz channel.

4.3.3 Wireless Client

A wireless client or wireless network interface card (WNIC) is a computer circuit board or card that is installed in a computer so that it can be connected to a wireless network [13]. Personal computers and workstations on a local area network (LAN) typically contain a network interface card specifically designed for the LAN transmission technology, such as Ethernet [13]. Network interface cards provide a dedicated, full-time connection to a network. Figure 4.3 displays an example of a wireless client.



Figure 4.2: An example of an access point.



Figure 4.3: An example of a wireless client.

We have introduced wireless devices in this section. Now we are going to discuss some advantages, and disadvantages of wireless network.

4.4 Wireless Networks Advantages and Disadvantages

The popularity of wireless technology is a testament primarily to their convenience, cost efficiency, and ease of integration with other networks and network components. The majority of computers sold to consumers today come pre-equipped with all necessary wireless technology.

4.4.1 Advantages

a) Convenience

The wireless nature of such networks allows users to access network resources from nearly any convenient location within their primary networking environment (home or office) [13]. With the increasing saturation of laptop-style computers, this is particularly relevant.

b) Mobility

With the emergence of public wireless networks, users can access the internet even outside their normal work environment [13]. Most chain coffee shops, for example, offer their customers a wireless connection to the internet at little or no cost.

c) Productivity

Users connected to a wireless network can maintain a nearly constant affiliation with their desired network as they move from place to place [13]. For a business, this implies that an employee can potentially be more productive as his or her work can be accomplished from any convenient location.

d) Deployment

Initial setup of an infrastructure-based wireless network requires little more than a single access point [13]. Wired networks, on the other hand, have the additional cost and complexity of actual physical cables being run to numerous locations (which can even be impossible for hard-to-reach locations within a building).

e) Cost

Wireless networking hardware is at worst a modest increase from wired counterparts. This potentially increased cost is almost always more than outweighed by the savings in cost and labor associated to running physical cables [13].

4.4.2 Disadvantages

Security is the greatest disadvantage to wireless networks. Many organization have resisted implementation wireless on a broad scale because of the lack of security for wireless communications [16]. A survey by Network Computing in 2005 indicated that just fewer than 50 percent of business respondents said that lack of adequate security technology was a barrier to wireless network adoption in their organization [16]. A number of different attacks on wireless networks, such as denial of service attacks, stealing passwords, altering messages, and other attacks make many organizations reluctant to use wireless technology [16].



4.5 Summary

The popularity of wireless technology is a testament primarily to their convenience, cost efficiency, and ease of integration with other networks and network components. Wireless networks are implemented with some type of information transmission system that uses electromagnetic waves, such as radio waves. Some types of wireless networks include Wireless PAN (Personal Area Networks) and Wireless LAN (Local Area Networks).

The wireless LANs are identified by their standard, the 802.x, and some example of 802.x are: 802.11, 802.11a, 802.11b and 802.11g. Wireless network devices include wireless access points, wireless modems, and wireless clients. The advantages of using wireless networks include: mobility, and convenience. Security is the greatest disadvantage to wireless networks.

In the next Chapter we will investigate what Information Security consists of, and we will have a look at the three goals of Information Security (CIA): **Confidentiality**, **Integrity**, and **Availability**. We will also discuss the five pillars of Information Security.



Chapter 5

Information Security Overview



In this chapter, we will discuss:
What is Information Security?
Information Security Pillars

Page 47
Page 49

5.1 Introduction

Knowing how to defend computer networks against attacks begins with an understanding of what Information Security is. In the previous chapter we discussed wireless LANs, and presented an overview of wireless types, and devices. In this section we will be discussing Information Security, and Information Security Pillars. Each of these topics will now be discussed in detail. We will start with Information Security.

5.2 What is Information Security?

Information Security is the process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption [41]. Information Security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms.

The security of information technology used in organizations is of utmost importance. Confidential information and private customer and employee information must be safeguarded, and systems must be protected against malicious acts intended to steal data or otherwise cause disruption.

Unfortunately, there is no doubt that the number of IT-related security incidents is increasing [17]. The Computer Emergency Response Team Coordination Center (CERT/CC) is a US federally funded research and development center at Mellon University in Pittsburgh, Pennsylvania [17]. It is charged with coordinating communication among experts during computer security emergencies and helping to prevent future incidents. The number of security problems reported to CERT increased between 1993 and 2003, (as shown in Figure 5.1).

Some of the reason for this growth can be related to [17]:

- The expanding and changing technology systems
- Increasing technology complexity
- Increasing reliance on commercial software with known vulnerabilities
- Higher computer user expectations

Incidents reported	
Year	Incidents
1993	1,334
1994	2,340
1995	2,412
1996	2,573
1997	2,134
1998	3,734
1999	9,859
2000	21,756
2001	52,658
2002	82,094
2003	137,529

Total incidents reported (1993-1999) is 24,386 and total incidents reported (2000-2003) is 294,037. As this figure indicates, the total incidents reported from 2000-2003 is 12 times the total incidents reported from 1993-1999.

Figure 5.1: Incidents reported by CERT.

The goal of Information Security is to properly address the following three important aspects of a computer related system: confidentiality, integrity, and availability.

- Confidentiality ensures that information assets are accessed only by authorized parties.
- Integrity means that assets can be modified only by authorized parties or only in authorized ways.
- Availability means that assets are accessible to authorized parties at appropriate times.

Figure 5.2 illustrates the relationship between Information Security, confidentiality, integrity, and availability.

The terms Information Security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information. However, there are some subtle differences between them. These differences lie primarily in the approach to the subject, the methodologies used, and the areas of concentration.

One approach to Information Security is the five pillars of Information Security described by SH Von Solms and Jan HP Eloff [2]. The five pillars of Information Security distinguish five different services, namely Identification and Authentication, Authorization, Confidentiality, Integrity and Non-repudiation [2].

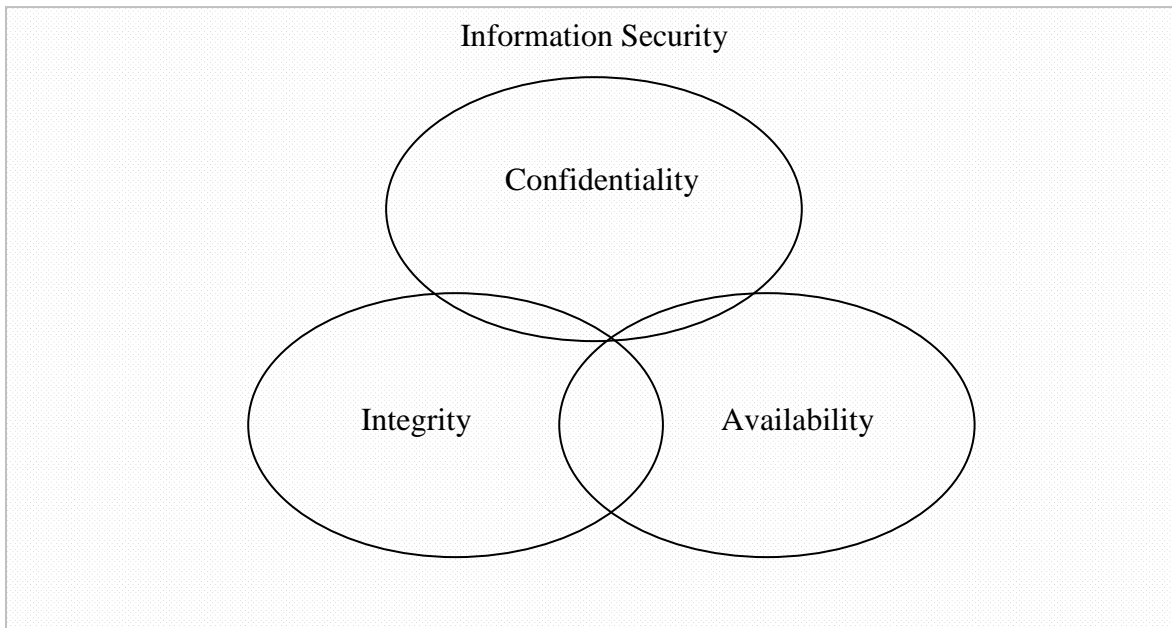


Figure 5.2: Relationships between Information Security, Confidentiality, Integrity, and Availability

The next discussion is the five pillars of Information Security.

5.3 The Information Security Pillars

As stated above the five pillars of Information Security consists of five services. If these five services are properly implemented in an environment, then it can be accepted that the environment is properly secured. Information Security according to this architecture is now to ensure that these five services are properly implemented and controlled on a continuous basis [2].

The five pillars are: Identification and authentication, authorization, confidentiality, integrity and non-repudiation.

5.3.1 Identification and Authentication

Identification is the process of matching a set of qualities or characteristics that uniquely identifies a person or an object. It is a technique used by one party to ensure a second party is very likely the party claiming the identity [2]. Assurance of identification can be increased by a number of practices appropriate to the need. These practices range from passwords to tokens, biometrics, smart cards, and public keys with Certificates [2].

Authentication is the process of attempting to verify the digital identity of the sender of a communication such as a request to log in. The sender being authenticated may be a person using a computer, a computer itself or a computer program.

5.3.2 Authorization

Authorization is a part of the service that protects computer resources, by only allowing those resources to be used by resource consumers that have been granted authority to use them.

Resources include individual files or items data, computer programs, computer devices and functionality provided by computer applications. Examples of consumers are computer users, computer programs and other devices on the computer.

5.3.3 Confidentiality

Confidentiality has been defined by the ISO (International Standards Organization) as "ensuring that information is accessible only to those authorized to have access", protecting the confidentiality of data software means the assurance that only authorized people may view the contents of data or software [2].

5.3.4 Integrity

Integrity refers to protecting the information from unauthorized access or revision, to ensure that the information is not compromised through corruption or falsification [2].

5.3.5 Non-repudiation

Non-repudiation is a method by which the sender of data is provided with proof of delivery and the recipient is assured of the sender's identity, so that neither can later deny having processed the data [2].

We learned about Information Security, Information Security goals, namely Confidentiality, Integrity, and Availability.

5.6 Summary

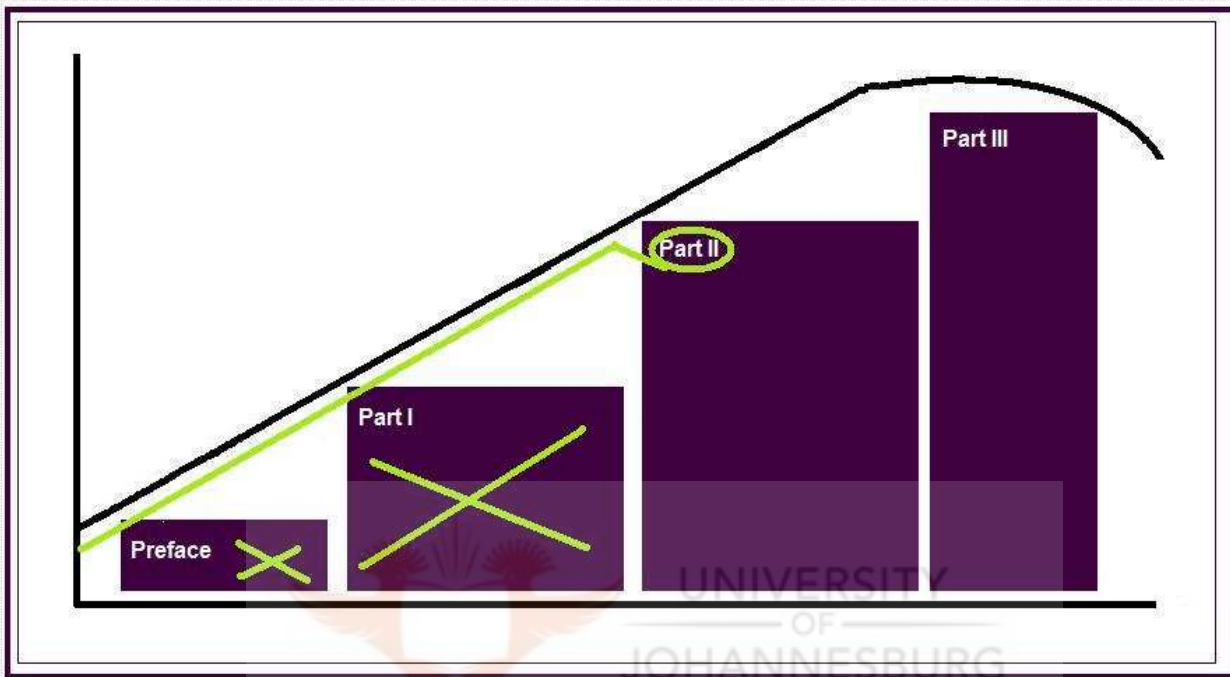
Information Security is the process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption. One approach is the five pillars of Information Security described by SH Von Solms and Jan HP Eloff. If we can enforce the five pillars of Information Security, we have gone a long way in ensuring that the information resources of the company are secure.

The goal of Information Security is to properly address the three aspects of a computer related system: confidentiality, integrity, and availability.

In the next Chapter, we will investigate the major wireless networks security risks. We will also discuss the easy access to a WLAN due to signal overflow, and issues related to access points.



Part II



Part II

Chapter 6 – Wireless LANs Security Risks

Chapter 7 – Wireless LANs Type of Attacks

Chapter 8 – Wireless LANs Security and Countermeasures

Chapter 6

Wireless LANs Security Risks



CHAPTER OBJECTIVES

In this chapter, we will discuss:

Inherent Security Risks of Wireless Networks	Page 54
Security Risks of Wireless Networks Devices	Page 58
Security Risks of Wireless Networks Communication	Page 62

6.1 Introduction

In the previous chapters we have discussed wireless networks, and we have also briefly discussed information security. In this section we will discuss the major security risks of wireless networks. The term wireless networks and wireless LAN are used interchangeably.

We will concentrate on wireless networks. We divide these security risks into three categories:

Category 1: Inherent Security Risks of Wireless Networks.

Category 2: Security Risks of Wireless Networks Devices.

Category 3: Security Risks of Wireless Networks Communication.

We will begin with the inherent security risks, which are the signal overflow and easy deployment of wireless networks. We will then discuss the security risks related to wireless networks devices, and wireless networks communications.

The next section discusses the inherent security risks of wireless networks.

6.2 Category 1: Inherent Security Risks of Wireless Networks

This section discusses signal overflow and easy deployment of wireless networks.

6.2.1 Signal Overflow

Wireless networks are easy to find. All wireless networks need to announce their existence so potential clients can link up and use the services provided by the network. WLAN requires that networks periodically announce their existence to the world with special frames called beacon frames [63].

Beacon frames are frames that have control information and are transmitted over wireless channels and help a wireless Access Point to identify nearby wireless clients. The beacon frame sent by the AP contains control information and can be used by wireless clients to locate an AP.

One aspect of a secure wired network is to know precisely where all the access points to the network are and then secure those access points through proper controls [1]. However, the

perimeters of wireless networks are difficult to determine and control. Furthermore, wireless networks waves are not restricted to wires. Figure 6.1 illustrates a possible scenario.

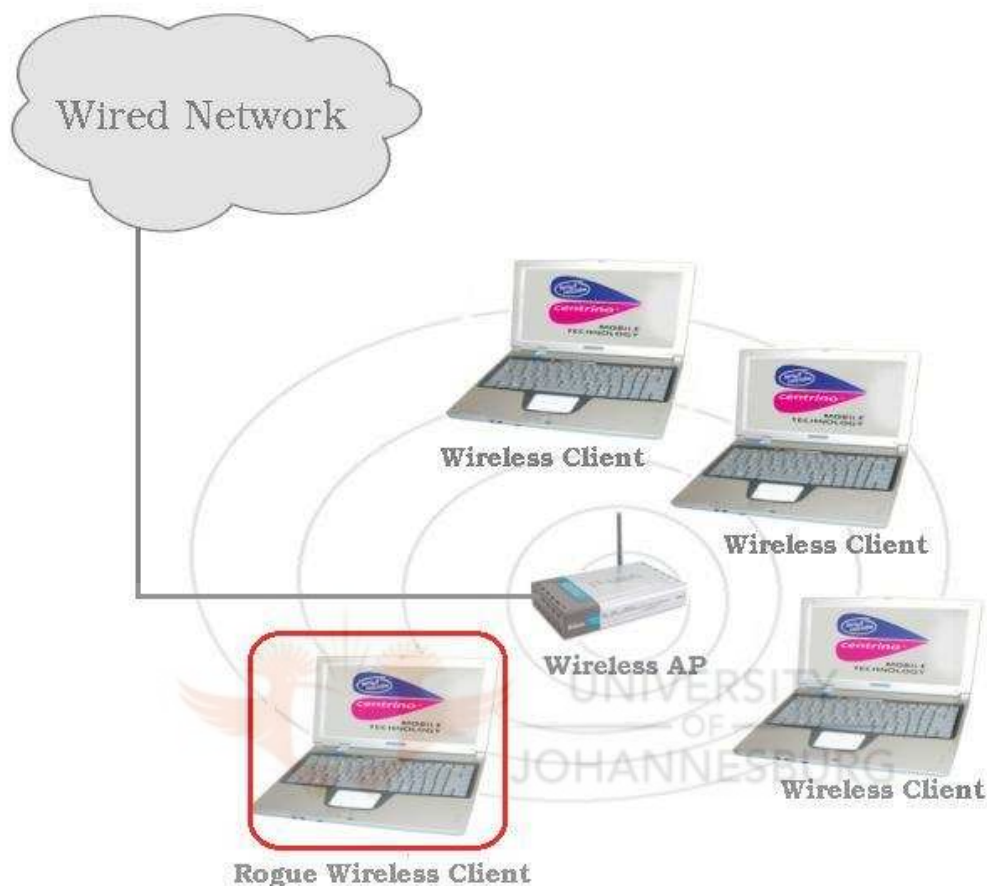


Figure 6.1: Signal overflow.

Wireless LAN boundaries, compared to the wired environment where one can literally follow the path from one component to the next, are amorphous and constantly changing [62]. They expand and contract for all sorts of reasons. Some of these reasons are [62]:

- Barriers (e.g., walls, people, and weather) can reduce the distance that an Access Point and client can be from each other.
- Antennas can increase the distance.
- Interference from other wireless devices or radio signals can reduce the distance.
- Antenna adjustments (e.g., turning it around or making it horizontal instead of vertical) and alternative antenna types (directional vs. omni-directional) can change the shape and size of the coverage area.

These and other factors can make it very difficult to answer the simple question, "What are the boundaries of our wireless network?" One of the most important issues in deploying a secure wireless environment is ensuring that the coverage area of the Access Point is appropriate [62].

Because of signal overflow in wireless networks, it is possible for attackers who are within range to hijack or intercept an unprotected connection. A practice known as wardriving (see appendix A for more details about wardriving) involves individuals equipped with a computer, a wireless card, and a GPS device driving through areas in search of wireless networks and identifying the specific coordinates of a network location. This information is then usually posted online. Some individuals who participate in or take advantage of wardriving have malicious intent and could use this information to hijack the wireless network or intercept the connection between the computer and a particular wireless network [95].

6.2.2 Easy Deployment

WLANs are affordable and easy to deploy. In contrast with installing a wired network, which needs significant knowledge hardware, money, and time, a wireless network Access Point is cheap, and can be installed very easily without much technical knowledge. The Access Point is just plugged into the wired network [1]. Figure 6.2 illustrates a possible scenario.

This means that a rogue Access Point (See 6.3.1) can be installed very easily, without proper authorization and configuration, and in that way become a potential unauthorized point of entry into the wired network [1]. Access Points are easy to install. This easy deployment can cause headaches for network administrators. Any user can run to a nearby computer store, purchase an Access Point, and connect it to the corporate network without authorization. Other departments may also be able to roll out their own wireless networks without authorization from Network Administrators [63].

Furthermore, very often the wireless Access Point is connected to the wired network behind the company security controls like the firewall, which increase the risks significantly [1]. Figure 6.3 illustrates a possible scenario.

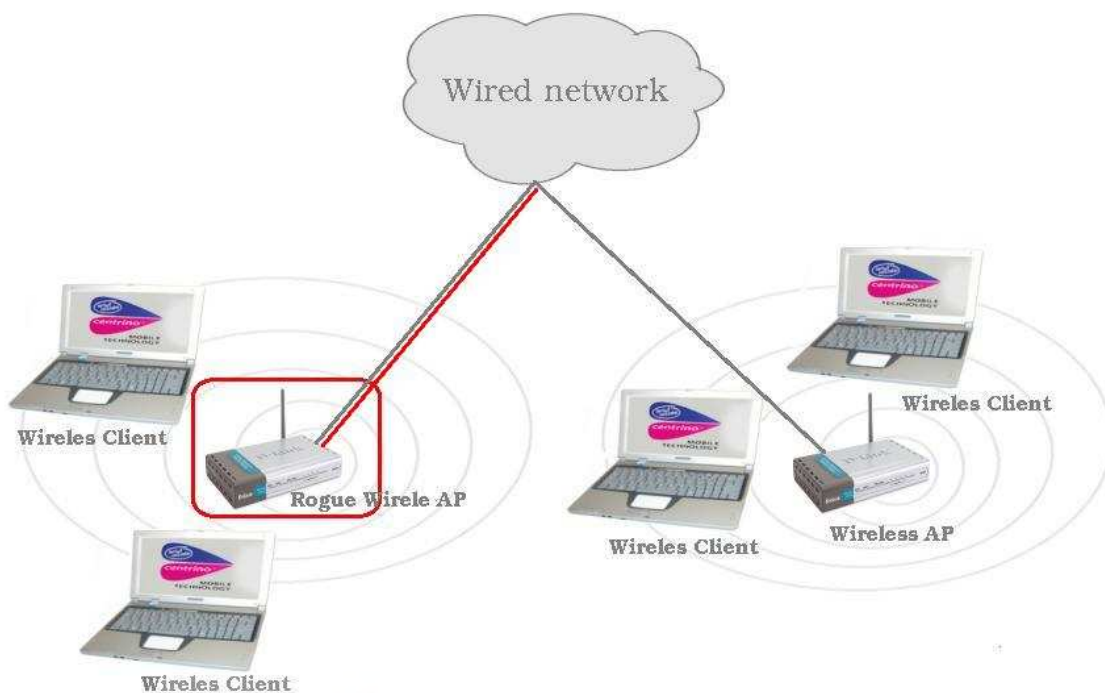


Figure 6.2: Easy deployment.

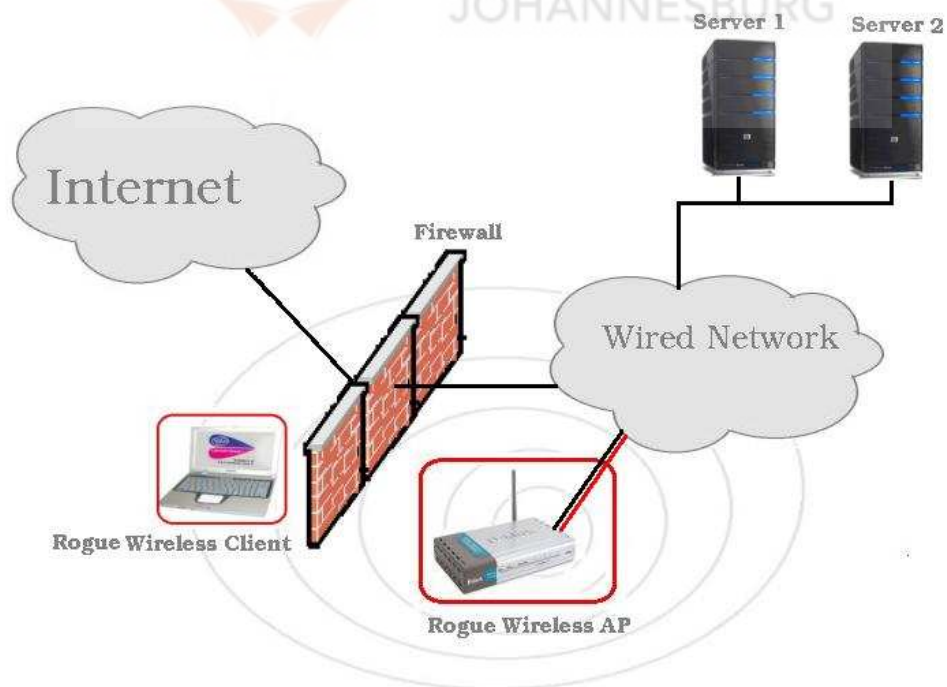


Figure 6.3: Easy deployment behind firewall.

Wireless networks are prone to attacks because of their open transport medium (airwaves) and easy availability of attack tools on the internet like NetStumbler, AirSnort and Nmap (see Appendix B).

Signal overflow coupled with easy deployment of wireless networks can cause security risks, and they must be taken into consideration when securing a wireless network. The countermeasure section (Paragraph 8.2.1) discusses some possible ways to deal with signal overflow and easy deployment. The next section discusses security risks associated with wireless networks devices.

6.3 Category 2:

Security Risks of Wireless Networks Devices

Wireless networks rely on radio waves rather than wires to connect computers to the internet. A transmitter, known as a wireless Access Point (AP), is wired into an internet connection. This provides a "hotspot" that transmits the connectivity over radio waves. Wireless networks can extend an existing wired network, and end users with a wireless client can connect wirelessly to the network as discussed in chapter 4. In this section we will discuss the security risks associated with APs, and wireless clients, the major wireless network devices.

6.3.1 Rogue APs

An unauthorized AP is referred to as a Rogue AP. Rogue Access Points deployed by end users create great security risks. Two examples of rogue APs are: rogue APs installed by end users and rogue APs installed by hackers (See Figure 6.4 and 6.5). Rogue APs installed by end users are attached to the wired network by end users, and because end users are not security experts, they may not be aware of the risks created [63]. Attackers can also deceive users with their rogue APs. Upon a successful deception, attackers can gain information needed to join the wireless network.

The difference between a rogue AP by end users and a rogue AP by attackers is that an end user rogue AP is physically attached to the wired network, and most of the time behind the firewalls, whereas the rogue AP by attackers is not attached to the wired network, but used to deceive end users.

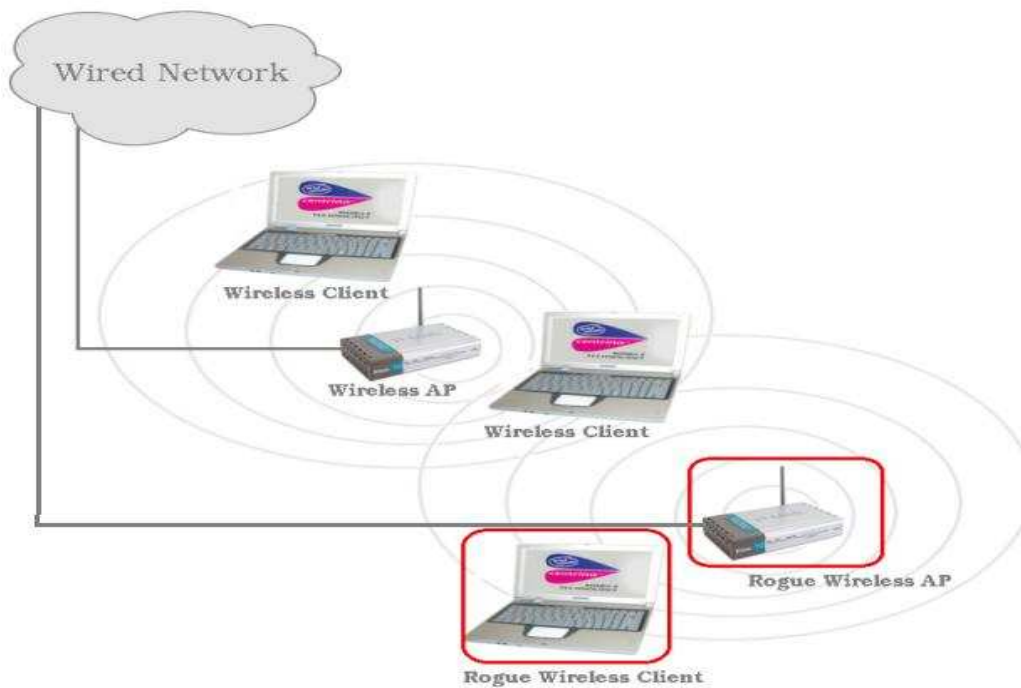


Figure 6.4: A rogue AP installed by an end user.

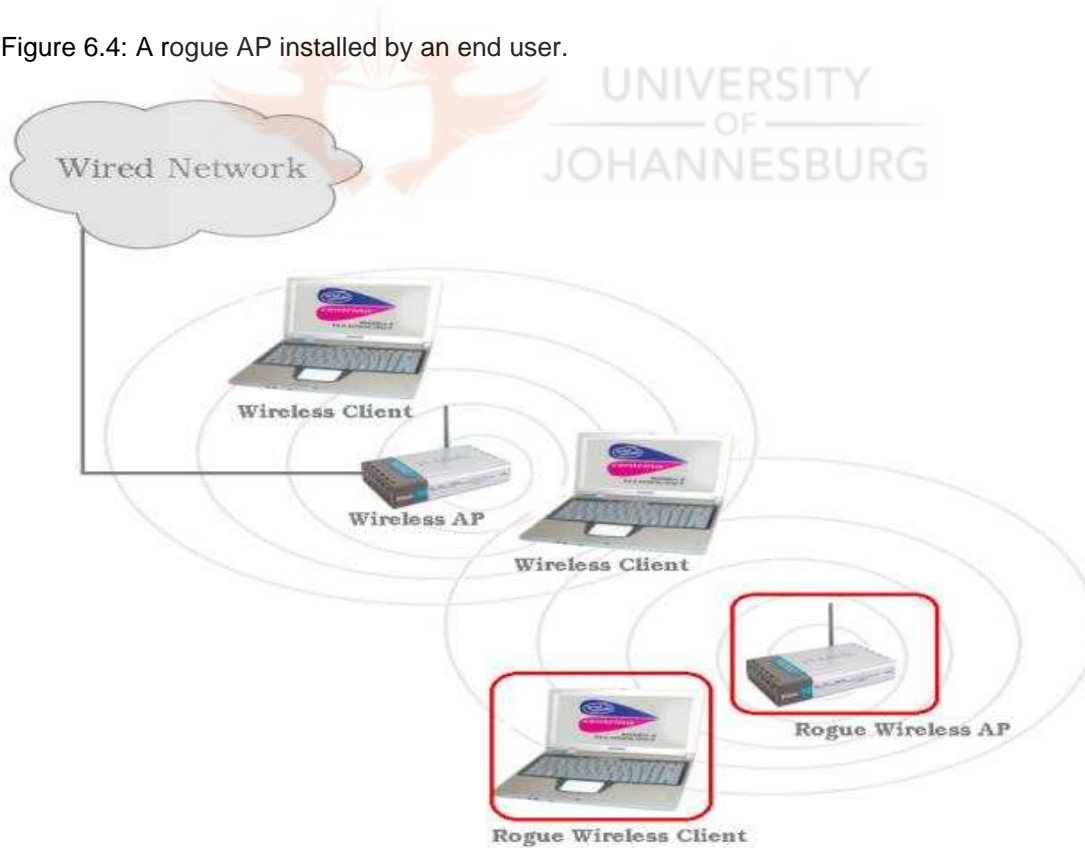


Figure 6.5: A rogue AP installed by a hacker.



There are tools freely available on the internet like NetStumbler, AirSnort and Nmap, which allows anybody to wander around buildings looking for Access Points (for more details about these tools see Appendix B). Most existing small deployments mapped by wardrivers show that, the security features are not enabled on Access Points, and many Access Points have had only minimal changes made to the default settings [63].

These default settings include among other things the following:

6.3.1.1. The administrative password, which controls the wireless network.

Just like any other password, it should not be a word that one can find in the dictionary, and it should be a combination of letters, numbers, and symbols [96].

6.3.1.2. Wireless encryption (WEP) or Wi-Fi Protected Access (WPA), which helps protect the wireless network communication [96]. For most routers, this functionality is not enabled by default.

6.3.1.3. The wireless network name, known as the SSID (Service Set Identifier).

This name identifies the wireless network. One should choose something unique that none of the neighbors will be using [96]. By default, the Access Point broadcasts the SSID every few seconds in beacon frames. Although, this makes it easy for authorized users to find the correct network, it also makes it easy for unauthorized users to find the network name [98]. If the SSID is configured to be any of the defaults cited in Table 8-1, then the SSID should be changed immediately.

Manufacturer	Default SSID
3Com	101, comcomcom
Cisco	Tsunami, WaveLAN Network
Compaq	Compaq
Dlink	WLAN
Intel	101, 195, xlan, intel
Linksys	Linksys, wireless
Lucent/Cabletron	RoamAbout
NetGear	Wireless
SMC	WLAN
Symbol	101
Teletronics	Any

Table 6.1 Default Wireless SSIDs

A complete listing of manufacturers' SSIDs and even other networking equipment default passwords can be found at <http://www.cirt.net/passwords>. As one can see, the SSIDs are readily available on the Internet, so it is a good idea to turn off SSID broadcasting as the first step [98]. This measure, coupled with keeping the Access Point from broadcasting the SSID, will stop a large proportion of attacks before they start. This easy step will make it harder to find the network, avoiding many attacks from intruders who simply search for easily detectable and vulnerable networks [102].

6.3.2 Wireless Clients

As discussed in chapter 4, a wireless client is a computer circuit board or card that is installed in a computer so that it can be connected to a wireless network. Let us take a look at what may be the most common wireless situation: public environments. More people are going to be exposed to a wireless environment out in the "public" than they are in their work environment. For example, at an airport, in a cafe, on some campus, in a networked neighborhood, in a hotel, at a conference, or some other public location [62].

The problem is the lack of understanding the subtle exposures that may result from using public networks, and the lack of appreciating how truly open the wireless environment really is [62]. For organizations that create public wireless networks, their main objective is to provide a convenient, hassle-free connection point to the Internet. The more standard, open, and generic the setup is, the easier it will be for consumers to use it [62]. It is not an accident that these types of environments are potentially risky.

In addition, there is no way to tell if someone else is sniffing the data. So, while most people intuitively understand that a public wireless network is not a secure environment, they do not understand how easy it is to accidentally or unknowingly expose private information to others within this environment [62]. So far we have discussed security risks associated with APs and wireless clients. The next section discusses the security risks of wireless networks communication. This will be our final section on WLAN security risks.

6.4 Category 3:

Security Risks of Wireless Networks Communication

In this section we will be discussing the security risks of wireless networks communications. Recall in chapter 5, information security's goal is to enforce the CIA namely, Confidentiality, Integrity and Availability. Encryption is utilized in communication to enforce the confidentiality and integrity of the communication.

6.4.1 Lack of encryption

Lesson that can be learned from a secure wired network, as far as the communication is concerned, is to use some sort of encryption to secure connection. There is a great security risk if wireless network is deployed without using encryption. We shall discuss the available encryption technologies available for wireless networks in Chapter 9. The next paragraph gives a brief overview of one such scheme.

6.4.1.1 WEP

Wired Equivalent Privacy (WEP) is a scheme to secure IEEE 802.11 wireless networks. WEP is an encryption algorithm that can be invoked to encrypt the transmissions between the wireless user and his Wireless Access Point [98]. Wireless networks broadcast messages using radio signals, so they are more susceptible to eavesdropping than wired networks. WEP was intended to provide confidentiality comparable to that of a traditional wired network. Several serious weaknesses were identified by cryptanalysts. A WEP connection can be cracked with readily available freeware tools within minutes, WEPCrack is one of such a freeware tool (see Appendix B). WEP was superseded by Wi-Fi Protected Access (WPA) in 2003, followed by the full IEEE 802.11i standard (also known as WPA2) in 2004. Despite its weaknesses, WEP provides a level of security that may deter casual snooping [80].

6.4.2 Lack of MAC Address Filtering

Media Access Control address (MAC address) is a quasi-unique identifier attached to most network adapters (NIC) (See Paragraph 3.5.2) [87]. The MAC address is a number that acts like a name for a particular network adapter, so, for example, the network cards in two different computers will have different names, or MAC addresses [87]. MAC address filtering is a feature normally turned off by the manufacturer. MAC address filtering is turned off, because it requires a bit of effort to set up properly. This is discussed in more detail in section 8.2.3.2.





6.5 Summary

WLAN signal are easily accessible and the boundary of the signal can go beyond walls, hence the boundaries are amorphous and constantly changing, the coverage area of your Access Point must be appropriate.

An unauthorized Access Point (AP) is referred to as rogue AP. Rogue Access Points deployed by end users create great security risks for organizations. One of the encryption schemes for wireless LANs is WEP, there are several serious weaknesses in WEP, and a WEP connection can be cracked with readily available software within minutes.

More people are going to be exposed to a wireless environment out in the “public” than they are in their work environment, and most people understand that a public wireless network is not a secure environment. It is easy to accidentally or unknowingly expose private information to others within this environment. Table 6.2 provides a consolidation of the discussion in this chapter.

Category 1: <i>Inherent Security Risks of Wireless Networks</i>	<ul style="list-style-type: none">• Signal Overflow• Easy Deployment
Category 2: <i>Security Risks of Wireless Network devices</i>	<ul style="list-style-type: none">• Rogue AP• Wireless Clients
Category 3: <i>Security Risks of Wireless Networks Communication</i>	<ul style="list-style-type: none">• Lack of Encryption• Lack of MAC Address Filtering

Table 6.2: WLAN Security Risks

The next chapter discusses the type of attacks that can be launched against wireless networks.

Chapter 7

Wireless LANs Type of Attacks



In this chapter, we will discuss:

Passive attacks

Page 66

Active Attacks

Page 70

Insertion Attacks

Page 72

Jamming attacks

Page 73

7.1 Introduction

In this chapter we will discuss the different types of attacks against WLANs. In general, attacks on wireless networks fall into four basic classes:

- Class 1: Passive attacks.
- Class 2: Active attacks.
- Class 3: Insertion attacks.
- Class 4: Jamming attacks.

We will now discuss each class in more detail.

7.2 Class 1: Passive Attacks

The scanning of the radio frequency airwaves for a signal can identify and map the location of a wireless network. At regular intervals (normally every 100 ms) the wireless Access Point sends a beacon frame to announce its presence and to provide the necessary information for devices that want to join the network. This process, known as beaconing, is an orderly means for wireless devices to establish and maintain communications. Each wireless device looks for those beacon frames (known as scanning). Once a wireless device receives a beacon frame it can attempt to join the network.

However, the information needed to join a network is also the information needed to launch an attack on a network. This information includes, among other things, the wireless network SSID (See paragraph 6.3.1.3), and the type of authentication (or association) scheme adopted. We can distinguish two types of associations, namely: Open System Authentication and Shared Key Authentication [79].

7.2.1 Open System Authentication

In Open System Authentication, the WLAN client need not provide its credentials to the AP during authentication. Thus, any client can authenticate itself with the Access Point and then attempt to connect to the wireless network [79]. In effect, no authentication (in the true sense of the term) occurs. At this stage WEP (See paragraph 6.4.2) is not used in the authentication but after the authentication and connection to the network, WEP can be used for encrypting the data frames.

The client needs to have the right keys. This authentication mode is the most used by Access Points, which allows any client to connect with it [62]. Figure 7.1 shows an open system authentication.

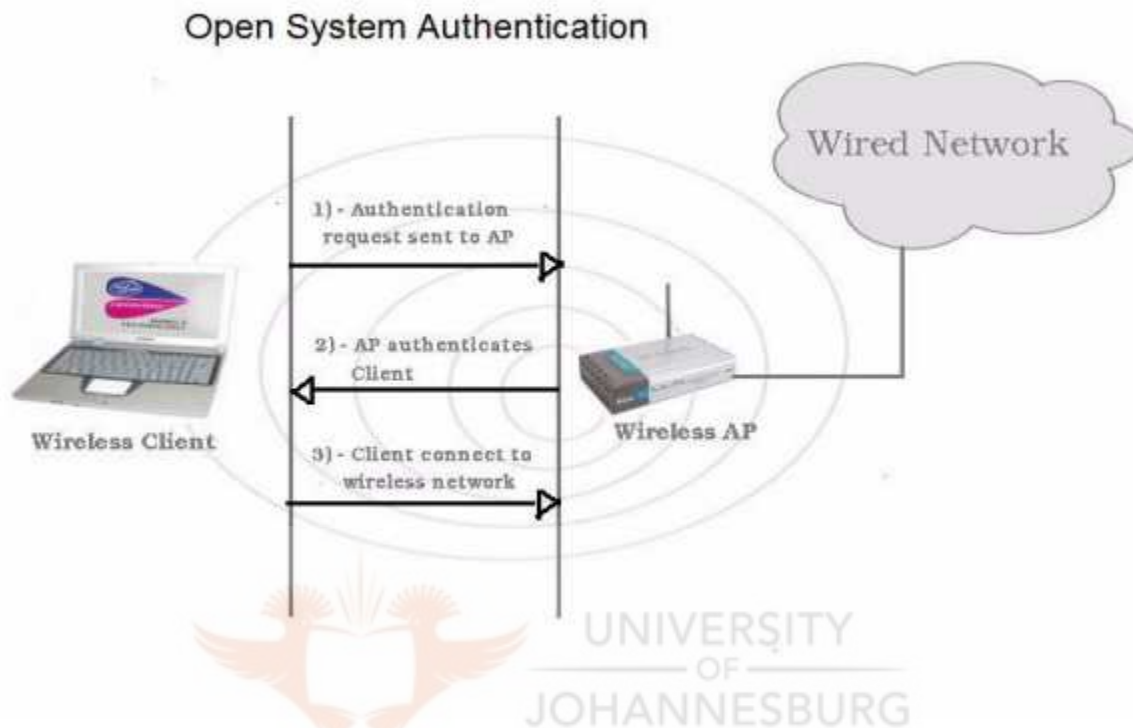


Figure 7.1: Open System Authentication.

7.2.2 Shared Key Authentication

In Shared Key authentication, WEP is used for authentication. A four-way challenge-response handshake is used [79]:

- I) The client station sends an authentication request to the Access Point.
- II) The Access Point sends back a clear-text challenge.
- III) The client has to encrypt the challenge text using the configured WEP key, and send it back in another authentication request.
- IV) The Access Point decrypts the material, and compares it with the clear-text it had sent.

Depending on the success of this comparison, the Access Point sends back a positive or negative response [79]. Figure 7.2 illustrates shared key authentication.

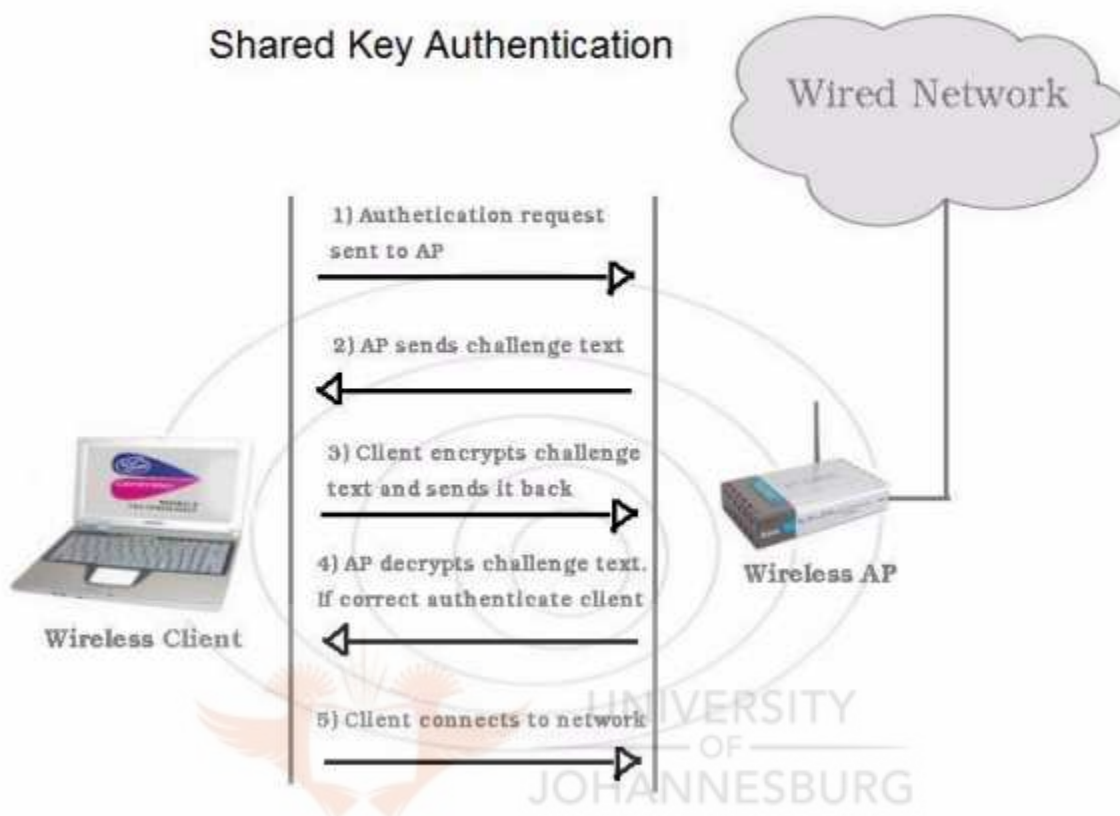


Figure 7.2: Shared Key Authentication.

A possible way to collect network information is passive attacks. A passive attack is an attack where an unauthorized attacker collects network parameters by scanning the wireless signal. A passive attacker might also monitor or listen in on the communication between two parties. Passive attacks are by their very nature difficult to detect. If an administrator is using DHCP (see Appendix A) on the wireless network, he or she might notice the presence of an unauthorized MAC address, that has acquired an IP address in the DHCP server logs [66]. Figure 7.3 shows an example of passive attack.

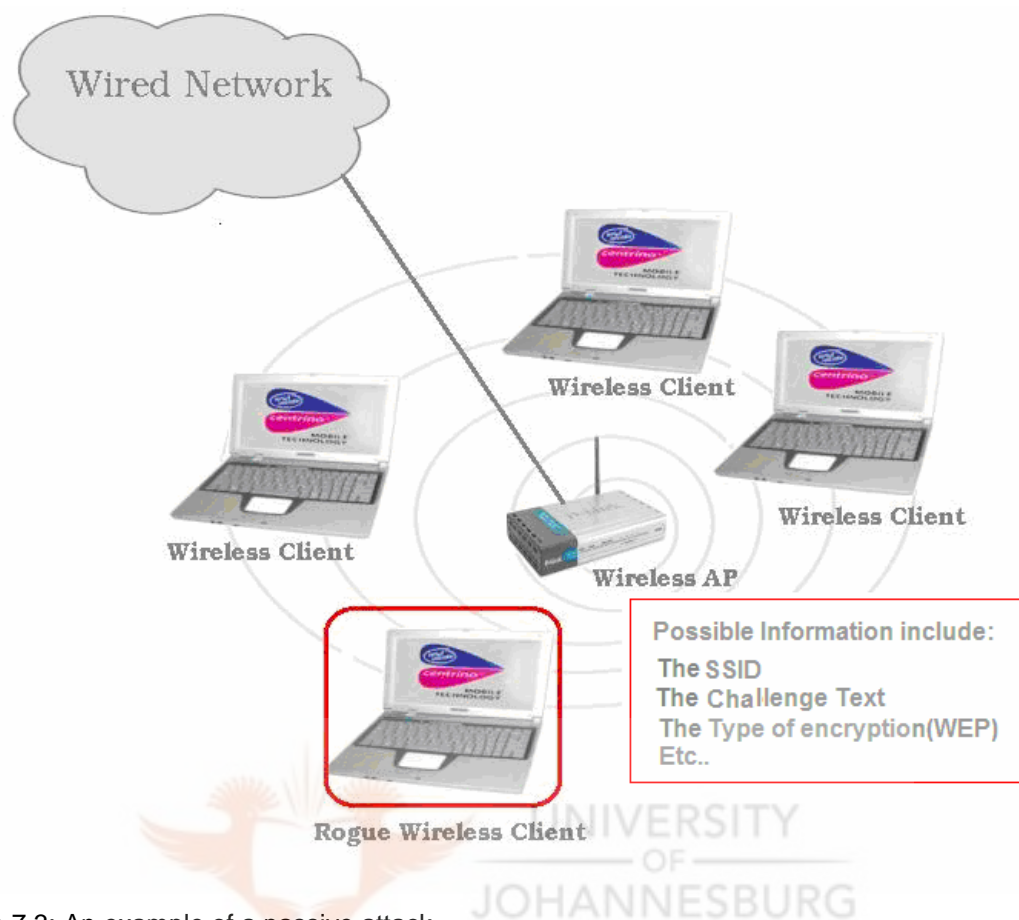


Figure 7.3: An example of a passive attack.

Wireless communication takes place on unlicensed public frequencies. Any one can use these frequencies. This makes protecting a wireless network from passive attacks more difficult [66].

A passive attack occurs when an unauthorized party simply gains access to information (like the SSID) that can later be used to launch an active or insertion attack. Passive attacks include two types of attacks: eavesdropping and traffic analysis [66]. In traffic analysis the attacker goes much deeper and gains intelligence by monitoring the transmission for pattern of communication. The person can use one of the easily obtainable tools such as NetStumbler or AirSnort (discussed in Appendix B) to passively scan for WLAN signals and discover wireless networks. Some wireless cards are capable to sniff network traffic, whereas some do not and may only be useful to discover wireless networks. Hackers generally prefer having both types of cards [65, 67].

Passive attacks can exploit the following wireless security risks discussed in chapter 6:

- Signal Overflow
- Rogue APs

Our next discussion is on active attacks.

7.3 Class 2: Active Attacks

Now that the attacker has gained enough information from the passive attack, he can then produce an active attack. In an active attack, an unauthorized party makes modifications to a message, data stream or file. In contrast to passive attacks, active attacks can be prevented.

The types of active attacks are almost all identical to that of wired networks and include one of the four following types [65, 66, and 67]:

- Masquerading: The attacker impersonates an authorized user and thereby gains unauthorized privileges.
- Replay: The attacker monitors transmission (passive attack) and retransmits messages as a legitimate user.
- Message modification: The attacker alters a legitimate message by deleting, adding to, changing or reordering it.
- Denial of Service (DoS): the attacker prevents or prohibits the normal use or management of communication facilities.

In denial of service attacks, potential attackers who cannot gain access to the wireless LAN can nonetheless pose security threats by flooding the wireless network with static noise that causes wireless signals to collide and produce **cyclic redundancy check** (CRC) errors.

This denial of service (DoS) attack effectively shuts down or severely slows down the wireless network in a similar way that DoS attacks affect wired networks [61].

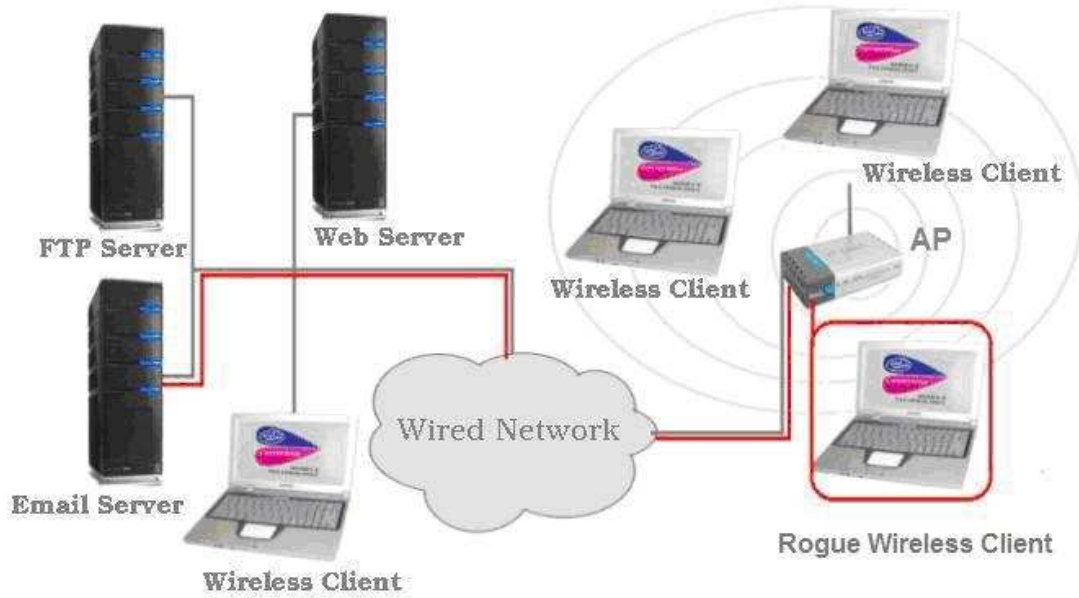


Figure 7.4: An example of an active attack.

Figure 7.4 shows an example of an active attack, where the rogue wireless client attacks the AP, and upon a successful attack the rogue client accesses the email server on the wired network. The attacker can for instance use the email server to send spam or read confidential emails. Active attacks can exploit the following wireless information security risks discussed in chapter 6:

- Rogue APs.
- The lack of using encryption for data transmissions over the wireless channels.

The next section discusses insertion attacks.

7.4 Class 3: Insertion Attacks

Insertion attacks consist of the deployment of unauthorized devices or the creation of new wireless networks without going through security processes and reviews.

The following are two types of insertion attacks [67, 155]

- **Rogue Clients:** The attacker tries to connect to a wireless network using his own laptop, or the attacker may steal corporate equipments, such as a laptop or a PDA that is already linked to the network. If no password is required, the intruder may easily connect to the internal network.
- **Rogue Access Point:** The attacker may try to access information by developing a rogue Access Point (AP). The APs may attract unsuspecting users and trick them into mistaking the rogue APs for legitimate APs.

Furthermore, the organization might be unaware of the presence of rogue Access Points and this may lead to unauthorized clients gaining access to the network. Using a rogue AP, an attacker can gain valuable information about the wireless network, such as authentication requests, the secret key that may be in use, and so on.

Because of their undetectable nature, the only defense against rogue APs is vigilance through frequent site surveys using tools such as NetStumbler or AirSnort (see Appendix B), and physical security [66]. Frequent site surveys also have the advantage of uncovering the unauthorized APs that company staff may have set up in their own work areas, thereby compromising the entire network and completely undoing the hard work that went into securing the network in the first place [66].

Even if the company does not use or plan to use a wireless network, the company should consider doing regular wireless site surveys to see if someone has violated the company security policy by placing an unauthorized AP on the network, regardless of their intent [66]. The portal WISP, discussed in Part III of this dissertation, will provide sample wireless network security policies.

Insertion attacks can exploit the following wireless security risks discussed in chapter 6:

- The lack of monitoring the wireless networks for rogue APs and rogue wireless clients.
- The lack of using an authentication mechanism for wireless networks.

The next section discusses jamming attacks.

7.5 Class 4: Jamming Attacks

Jamming is a special kind of DoS attack. In jamming, legitimate traffic cannot reach clients or the Access Point because illegitimate traffic overwhelms the frequencies. Jamming may be caused by interference whereby fake RF frequencies prevent the wireless network from functioning. Figure 7.6 shows an example of a jamming attack, where a signal jamming device creates interference for the wireless network.

Jamming may not necessarily be malicious [67]. Nevertheless, in case of malicious action, the attacker may jam a particular Access Point or client and then is able to impersonate the disabled device as a rogue client or AP [155].

Jamming attacks can exploit the following wireless information security risks discussed in chapter 6:

- The lack of monitoring the wireless network for interference.

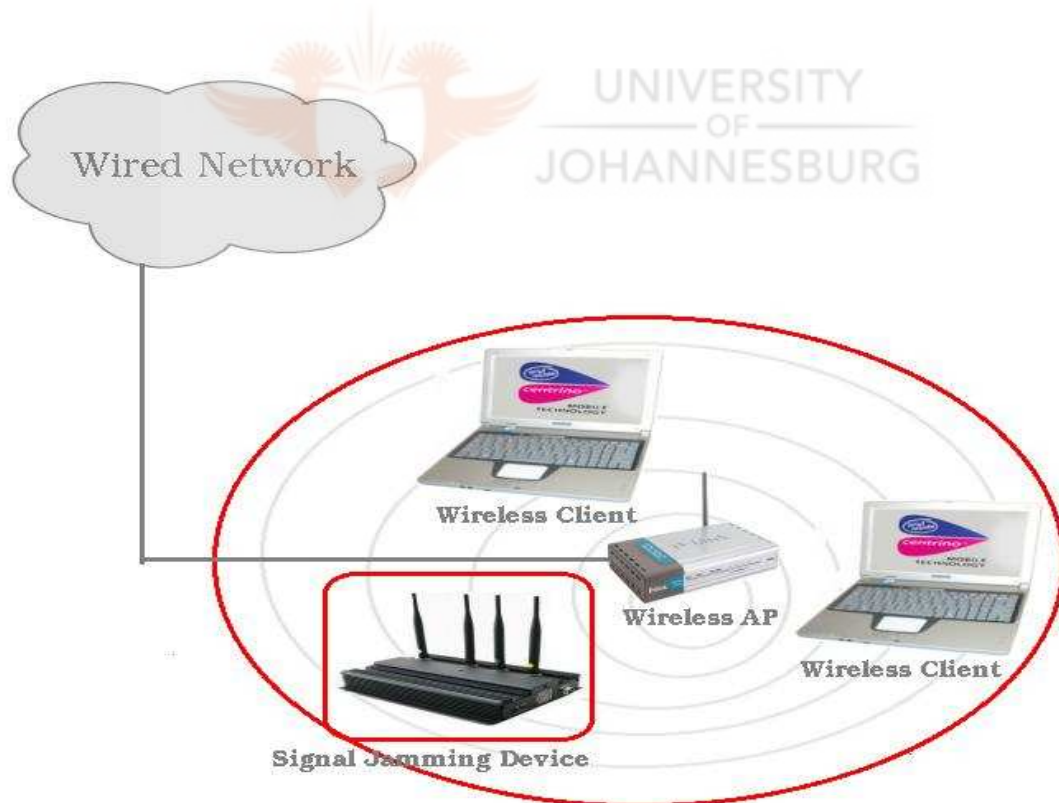


Figure 7.5: An example of a jamming attack.

7.6 Summary

The four basic classes of attacks against WLANs are: Passive attacks, Active attacks, Insertion attacks, and Jamming attacks. Passive attacks are used to collect information, information like the network SSID, the type of authentication, and the type of encryption. Active attacks are used to launch an attack against the wireless network. The types of active attacks are almost all identical to that of wired networks and include one of the four following types: Masquerading, Replay, Message modification, Denial of Service (DoS) [65, 66, and 67].

Insertion attacks consist of the deployment of unauthorized devices or the creation of new wireless networks without going through security processes and reviews. Jamming attacks can effectively shut down or severely slow down the wireless network. There are proven measures to improve the situation for companies, and for individuals. In the next chapter, we will be discussing these measures in detail. Table 7.1 summarizes the types of attacks and the type of risks expected by each type of attack.

Type of Attack	Risk Exploited
Class 1: <i>Passive Attacks</i>	<ul style="list-style-type: none"> • Signal Overflow • Rogue APs
Class 2: <i>Active Attacks</i>	<ul style="list-style-type: none"> • Rogue APs. • The lack of using encryption for data transmissions over the wireless channels.
Class 3: <i>Insertion Attacks</i>	<ul style="list-style-type: none"> • The lack of monitoring the wireless networks for rogue APs and rogue wireless clients. • The lack of using an authentication mechanism for wireless networks.
Class 4: <i>Jamming Attacks</i>	<ul style="list-style-type: none"> • The lack of monitoring the wireless network for interference.

Table 7.1: WLAN Types of Attacks

Now that WLAN security risks and type of attacks have been identified, the next chapter discusses WLANs Security and Countermeasures.

Chapter 8

Wireless LANs Security and Countermeasures



CHAPTER OBJECTIVES

In this chapter, we will discuss:

Countermeasures to Inherent Security Risks of WLANs	Page 76
Countermeasures to WLANs Devices Risks	Page 78
Countermeasures to WLANs Communications Risks	Page 79
Additional Monitoring Suggestion	Page 84

8.1 Introduction

So far, we have discussed three categories of security risks, and four classes of attacks that can be launched against WLANs. In this chapter, WLAN security countermeasures for the three categories of risks will be discussed. We will also look at additional monitoring suggestions.

As stated in chapter 6, the major categories of security risks include:

- Category 1: Inherent Security Risks of WLANs (Chapter 6, 6.2, Page 54).
- Category 2: Security Risks of WLANs Devices (Chapter 6, 6.3, Page 58).
- Category 3: Security Risks of WLANs Communications (Chapter 6, 6.4, Page 62).

Category 1: <i>Inherent Security Risks of Wireless Networks</i>	<ul style="list-style-type: none"> • Signal Overflow • Easy Deployment
Category 2: <i>Security Risks of Wireless Network devices</i>	<ul style="list-style-type: none"> • Rogue AP • Wireless Clients
Category 3: <i>Security Risks of Wireless Networks Communication</i>	<ul style="list-style-type: none"> • Lack of Encryption • Lack of MAC Address Filtering

Table 6.2: WLAN Security Risks

The countermeasures for each one of these categories will now be discussed.

8.2 WLAN Security Countermeasures

Despite the known security risks, wireless environments are being deployed in large numbers. Given this reality, there are a number of practical measures that organizations must take to make the environment as secure as possible [62]. In this section, we will suggest countermeasures to the three categories of the wireless network security risks (discussed in chapter 6) and mentioned above, starting with the inherent security risks of wireless networks.

8.2.1 Countermeasures to Category 1: Inherent Security Risks of WLANs

We have discussed wireless signal overflow and easy deployment in chapter 6. These two risks must be taken into account. However, although it is difficult to control the signal overflow, because that is the way the wireless network operates, there are possible countermeasures. These countermeasures are discussed in the next paragraph.

8.2.1.1 Risk - Signal Overflow

Possible countermeasures include the following:

- **Make a clear policy, stating the organization stand point about wireless networks.**
- **Change the SSID (See paragraph 6.3.1.3) from its default value, and not broadcasting the SSID.**
- **Regularly check Access Point logs for unauthorized MAC addresses.**

8.2.1.2 Risk - Easy Deployment

Possible countermeasures include the following:

- **Regularly monitor for unauthorized deployments. NetStumbler (see Appendix B) can be used to discover unauthorized deployments.**
- **Make a clear policy about wireless network deployments.**
- **Inform employees about the risks involved with unauthorized wireless deployments through awareness programs.**

Even though wireless networks may already exist in unauthorized mode in the some companies, network security policies must address the wireless network issues directly - either by forbidding it totally or providing rules on using it [1]. Organizations must update their security policies to specifically address wireless network policies. The wireless policies must be as consistent as possible with their wired counterparts [62]. Properly securing a wireless environment is not easy but it is not a mystery either. One example of best practices is to prepare a brief 2 to 3 pages document, describing required configuration changes that must be made to an Access Point before it can be attached to the wired network [62].

Security organization and baseline risks assessment are required to protect organizations information assets. We will not discuss these two fully, but it is important to note that security organization is needed for having a secure environment, and facilitates the management of security. Wireless networks security risk assessment should be the first step toward securing wireless networks. The baseline risk assessment is the process of identifying a company's wireless networks assets, threats, and vulnerabilities that could expose the assets to the threats.

The Wireless Information Security Portal (WISP) introduced in Part III, will provide sample wireless network security policies and guidelines for creating awareness programs. Furthermore, employees must be educated through awareness programs about the policies. The next section discusses countermeasures to risks associated with wireless network devices.

8.2.2 Countermeasures to Category 2: WLAN Devices Risks

We have identified Access Points and wireless clients as part of the major risks of WLAN devices in chapter 6. This section discusses countermeasures to mitigate the security risks of WLAN devices.

Like installing a door on a building to keep passers-by from wandering in, enterprises must control the perimeter of their enterprise networks. For the traditional wired LAN, this was accomplished by installing firewalls to control the entry point to the network. However, wireless LANs present greater challenges from the hard-to-control nature of radio transmissions. With data and network connections broadcasting across the air and through windows, walls, floors, and ceilings, the perimeter of a wireless LAN can be as difficult to control as it to define [64]. However, enterprises can control the perimeter of a wireless LAN by securing their WLAN devices that act as the endpoints of the network.

8.2.2.1 Risk – Rogue Wireless Access Points

Possible countermeasures include the following:

- Regularly monitor for unauthorized AP. NetStumbler (see Appendix B) can be used to discover unauthorized APs.
- Make a clear policy about APs deployments.
- All Access Points must be completely locked down and reconfigured from their default settings. The SSID and passwords of the Access Points must be changed from their default values.
- Deployment of enterprise-class APs that offer advanced security and management capabilities.

8.2.2.2 Risk – Rogue Wireless clients

Possible countermeasures include the following:

- Personal firewalls must be deployed on every wireless-equipped laptop.
- Inform every wireless-equipped laptop end user to connect to the company's APs only.
- Inform every wireless-equipped laptop end user about the risks involved with using public WLAN environments through awareness programs.

In fact, Gartner [64] outlined the three “must have” requirements for enterprise wireless networks:

- Install a centrally managed firewall on all laptops that are issued wireless network interface cards or are bought with built-in wireless capabilities.
- Perform wireless intrusion detection to discover rogue Access Points, foreign devices connecting to corporate Access Points and accidental associations to nearby Access Points in use by other companies.
- Turn on some form of encryption and authentication for supported WLAN use.

The portal WISP, introduced in Part III, will provide tips on Access Points configurations, and procedures. WISP will also include the best practices for securing Access Points. The next section discusses countermeasures to risks associated with wireless network communications.

8.2.3 Countermeasures to Category 3: WLAN Communications Risks

Information security controls used to secure network communications include authentication, authorization and encryption. In deploying a secure wireless LANs, IT security and network managers face the most difficult decision in choosing how to secure WLAN communications with multiple forms of authentication and encryption [64].

We have identified the lack of using encryption as a risk, and the countermeasure is to use encryption. We have also identified WEP and lack of MAC address filtering as part of the risks of WLAN communications in chapter 6. This section discusses countermeasures to mitigate the security risks of WLAN communications.

8.2.3.1 Risk – WEP

The standard WEP protocol has been proven to be insecure in several fundamental ways. It requires only a small amount of CPU capability and network traffic to determine the supposedly “secret” WEP encryption keys [62].

Countermeasures - The use of encrypted tunneling protocols like IPSec (see Appendix A), and Secure Shell (see Appendix A) can provide secure data transmission over an insecure network. However, using WEP is better than not using any encryption. Remedies for WEP have been developed with the goal of restoring security to the wireless network itself. WEP remedies include: WEP2, WPA, RADIUS, LEAP, PEAP and VPN. Each one of these remedies will now be discussed.

8.2.3.1.1 WEP2

WEP2 is an enhancement to WEP, implemented on some hardware not able to handle WPA [100]. WEP2 is based on **enlarged IV** value and **enforced 128-bit** encryption. Dynamic WEP is also an enhancement to WEP. It changes WEP keys dynamically.

8.2.3.1.2 WPA (Wi-Fi Protected Access)

In April 2003, the Wi-Fi alliance launched Wi-Fi Protected Access (WPA) as a subset of the future 802.11i security standard based on Temporal Key Integrity Protocol (TKIP) Table 8.1 provides more details about TKIP [101]. WPA is a class of systems to secure wireless (Wi-Fi) computer networks. It was created in response to several serious weaknesses researchers had found in the previous system, Wired Equivalent Privacy (WEP) [80].

WPA implements the majority of the IEEE 802.11i standard, and was intended as an intermediate measure to take the place of WEP while 802.11i was prepared. The most widely recommended solution to WEP security problems is to switch to WPA. It is much more secure than WEP. To add support for WPA, some old Wi-Fi Access Points might need to be replaced or have their firmware upgraded [80].

8.2.3.1.3 RADIUS (Remote Authentication Dial In User Service)

Larger enterprises with more complex wireless LANs with hundreds of stations and dozens of Access Points require more sophisticated access control through incorporating Remote Authentication Dial-In User Service (RADIUS) servers [81]. A RADIUS is an AAA (authentication, authorization and accounting) protocol for applications such as network access or IP mobility. It is intended to work in both local and roaming situations. For more details about RADIUS, refer to Appendix A.

8.2.3.1.4 LEAP (Lightweight Extensible Authentication Protocol)

The Lightweight Extensible Authentication Protocol (LEAP) is a proprietary wireless LAN authentication method developed by Cisco Systems. Important features of LEAP are dynamic WEP keys and mutual authentication (between a wireless client and a RADIUS server). LEAP allows for clients to re-authenticate frequently, upon each successful authentication, the clients acquire a new WEP key [92].

Cisco Systems is a recognized leader in this area. In regards to industry standards, the IEEE introduced 802.1x to provide port-based access control, which incorporates a central authentication server [64]. Cisco introduced Lightweight Extensible Authentication Protocol (LEAP) as a proprietary authentication solution that is based on 802.1x but adds proprietary elements of security [64].

8.2.3.1.5 PEAP (Protected Extensible Authentication Protocol)

Protected Extensible Authentication Protocol (PEAP) is a method to securely transmit authentication information, including passwords, over wired or wireless networks [94]. It was jointly developed by Cisco Systems, Microsoft, and RSA Security. It is important to note that PEAP is not an encryption protocol, as with other EAP types it only authenticates a client into a network [94].

PEAP uses only server-side public key certificates to authenticate clients by creating an encrypted SSL/TLS tunnel between the client and the authentication server. For more details about SSL/TLS refer to Appendix A. The ensuing exchange of authentication information is then encrypted and user credentials are safe from eavesdropping. PEAP is a joint proposal by Cisco Systems, Microsoft and RSA Security as an open standard. It is already widely available in products, and provides very good security. It is similar in design to EAP-TTLS, requiring only a server-side PKI certificate to create a secure TLS tunnel to protect user authentication [94].

New industry standards and proprietary solutions are now being introduced to handle both encryption and authentication. Cisco, RSA Security, and Microsoft developed Protected Extensible Authentication Protocol (PEAP) as one of these proprietary solutions. However, Microsoft and Cisco have separated their PEAP development efforts and introduced their own versions of the protocol [64].

Microsoft's version of PEAP does not work with Cisco's version of PEAP. While Microsoft is bundling its version of PEAP on the desktop, Cisco's version of PEAP requires client software to be installed and managed on each WLAN user stations [64].

8.2.3.1.6 VPN (Virtual Private Networks)

Virtual Private Networks or WLAN gateways provide another alternative to standards-based encryption and authentication [64]. Traditional firewall and VPN gateway vendors, such as Check Point and NetScreen Technologies [64], offer VPNs that funnel all traffic through their existing VPN gateway. These VPN solutions are generally IPSec based and do not work well with wireless LANs where users roam between Access Points or signals may vary and drop off, which forces the user to re-authenticate and begin a new session [64].

Table 8.1 provides a summary of data protection technologies. The next section discusses MAC address filtering.

Data Protection Technology	Description
WEP	Wired Equivalency Privacy – Original security standard for wireless LANs. Flaws were quickly discovered. Freeware, such as WEPCrack (see Appendix B), can break the encryption after capturing traffic and recognizing patterns in the encryption.
802.1X	As the IEEE standard for access control for wireless and wired LANs, 802.1x provides a means of authenticating and authorizing devices to attach to a LAN port. This standard defines the Extensible Authentication Protocol (EAP), which uses a central authentication server to authenticate each user on the network.
LEAP	Lightweight Extensible Authentication Protocol – Based on the 802.1x authentication framework, LEAP mitigates several of the weaknesses by utilizing dynamic WEP and sophisticated key management. LEAP also incorporates MAC address authentication as well. (Developed by Cisco)
PEAP	Protected Extensible Authentication Protocol – Securely transports authentication data, including passwords and encryption keys, by creating an encrypted SSL/TLS tunnel between PEAP clients and an authentication server. PEAP makes it possible to authenticate wireless LAN clients without requiring them to have certificates, simplifying the architecture of secure wireless LANs. (Developed by Cisco, Microsoft, and RSA Security)
WPA	Wi-Fi Protected Access – Subset of the future 802.11i security standard. Designed to replace the existing WEP standard. WPA combines Temporal Key Integrity Protocol (TKIP) and 802.1x for dynamic key encryption and mutual authentication. (Discussed in chapter 6)
TKIP	The Temporal Key Integrity Protocol, pronounced tee-kip, is part of the IEEE 802.11i encryption standard for wireless LANs. TKIP provides per-packet key mixing, a message integrity check and a re-keying mechanism, thus fixing the flaws of WEP. (Industry standard).

Table 8.1: Data protection technologies

8.2.3.2 Risk - MAC Address Filtering

MAC Address Filtering is a feature normally turned off by the manufacturer. The MAC address filtering is turned off, because it requires a bit of effort to set up properly.

Countermeasure – To improve the security of WLAN, strongly consider enabling and using MAC address filtering.

Like installing locks and keys on a door to control who can enter, this layer of wireless LAN security is to control which users can access the wireless LAN. To provide basic authentication, most Access Points support simple MAC address filtering that maintains a list of approved stations' MAC addresses. While this is not foolproof, MAC address filtering provides basic control over which stations can connect to the network [64].

Without MAC address filtering, any wireless client can join (authenticate with) a wireless network if they know the network name (also called the SSID) and perhaps a few other security parameters like encryption keys. When MAC address filtering is enabled, however, the Access Point or router performs an additional check on a different parameter. To set up MAC address filtering, a WLAN administrator must configure a list of clients that will be allowed to join the network. First, obtain the MAC addresses of each client from its operating system or configuration utility. Then, record those addresses into a configuration screen of the wireless Access Point or router. Finally, switch on the filtering option.

Once enabled, whenever the wireless Access Point or router receives a request to join with the WLAN, it compares the MAC address of that client against the administrator's list. Clients on the list authenticate as normal; clients not on the list are denied any access to the WLAN. MAC addresses on wireless clients can't be changed as they are burned into the hardware. However, some wireless clients allow their MAC address to be impersonated or spoofed in software. It's certainly possible for a determined hacker to break into the WLAN by configuring their client to spoof a MAC address. Although MAC address filtering isn't bulletproof, still it remains a helpful additional layer of defense that improves overall wireless network security.

However, it is possible to change the MAC address on most of today's hardware, often referred to as MAC spoofing [87]. Unfortunately, attackers can change the MAC address of most clients to be anything they want it to be [62]. Deploying user authentication mechanisms is essential to secure wireless networks.



By requiring authentication by potential users, unauthorized users can be kept from accessing the network [62]. We have now discussed WLAN security countermeasures for the 3 categories of risks. We will now look at additional monitoring suggestions.

8.3 Additional Monitoring Suggestions

A critical layer of wireless LAN security requires monitoring of the network to identify rogue WLANs, detect intruders and impending threats, incidents reporting and enforce WLAN security policies.

Manual site surveys can help small to medium organizations. However, the manual site surveys are particularly unreasonable for big organizations operating dozens of offices around the country. Even if these organizations could feasibly devote a network administrator's full attention to survey each site on a daily, weekly, or monthly basis. Wireless LAN security experts advocate 24x7 monitoring of the airwaves to secure wireless LANs by identifying rogue WLANs, detecting intruders and impending threats, incidents reporting and enforcing WLAN security policies [62, 63, and 64].



8.4 Summary

The generic security risks of wireless networks consist of **Signal Overflow** and easy deployment. These two risks must be taken into account. However, it is difficult to control the signal overflow of wireless networks. A possible countermeasure for **Easy Deployment** risk is making clear wireless networks security policies. As far as wireless networks devices are concerned, all **Access Points** must be completely locked down and reconfigured from their default settings. Personal firewalls must be deployed on every **Wireless Client**, and also includes a deployment of enterprise-class Access Points that offer advanced security and management capabilities.

Authentication and Encryption must used to secure communication over wireless networks. Furthermore, organizations must update the security policies to specifically address wireless networks. A critical layer of wireless LAN security requires monitoring of the network to identify rogue WLANs, detect intruders and impending threats, incident reporting and enforce WLAN security policies.

Wireless networks can be a significant tool in increasing business productivity, and should be considered by all companies. However, wireless networks bring with it a totally new set of security risks which must be evaluated and countered, although with current technology there is no reason not to trust a well setup wireless network.

Table 8.1 summarizes the discussion in this chapter, it maps the different categories of risk to the suggested countermeasures to mediate the specific risks.

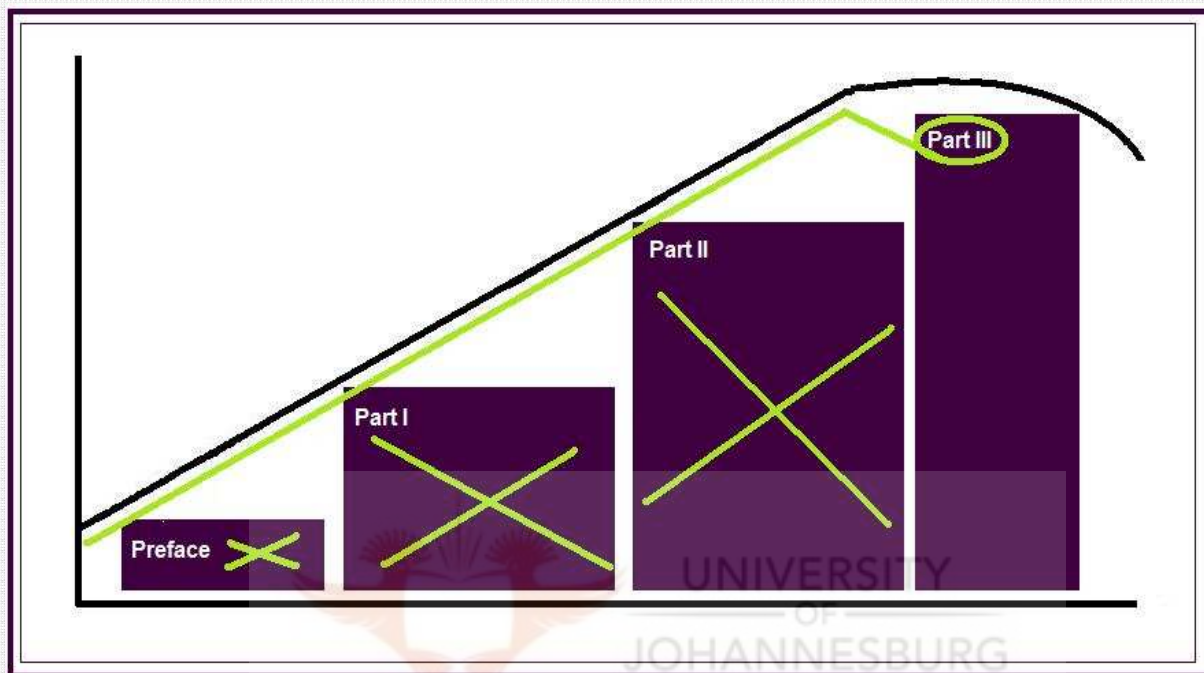
Category 1: <i>Inherent Security Risks</i>	Signal Overflow	<ul style="list-style-type: none"> • Make a clear policy, stating the organization stand point about wireless networks. • Change the SSID (See paragraph 6.3.1.3) from its default value, and not broadcasting the SSID. • Regularly check Access Point logs for unauthorized MAC addresses.
--	------------------------	---

	Easy Deployment	<ul style="list-style-type: none"> Regularly monitor for unauthorized deployments. NetStumbler (see Appendix B) can be used to discover unauthorized deployments. Make a clear policy about wireless network deployments. Inform employees about the risks involved with unauthorized wireless deployments through awareness programs.
Category 2: <i>WLAN Devices Risks</i>	Rogue APs	<ul style="list-style-type: none"> Regularly monitor for unauthorized AP. NetStumbler (see Appendix B) can be used to discover unauthorized APs. Make a clear policy about APs deployments. All Access Points must be completely locked down and reconfigured from their default settings. The SSID and passwords of the Access Points must be changed from their default values. Deployment of enterprise-class APs that offer advanced security and management capabilities.
	Wireless Clients	<ul style="list-style-type: none"> Personal firewalls must be deployed on every wireless-equipped laptop. Inform every wireless-equipped laptop end user to connect to the company's APs only. Inform every wireless-equipped laptop end user about the risks involved with using public WLAN environments through awareness programs.
Category 3: <i>WLAN Communication Risks</i>	Lack of Using Encryption	<ul style="list-style-type: none"> The use of encrypted tunneling protocols like IPSec (see Appendix A), and Secure Shell (see Appendix A) can provide secure data transmission over an insecure network. However, using WEP is better than not using any encryption. Remedies for WEP have been developed with the goal of restoring security to the wireless network itself. WEP remedies include: WEP2, WPA, RADIUS, LEAP, PEAP and VPN.
	Lack of MAC Address Filtering	<ul style="list-style-type: none"> To improve the security of WLAN, strongly consider enabling and using MAC address filtering.

Table 8.2: Countermeasures to WLAN Security Risks.

The next chapter discusses the Wireless Information Security Portal (WISP). WISP will provide security information related to wireless networks security. Furthermore, WISP will provide configuration tips of wireless networks devices, sample wireless network security policies and guidelines for creating awareness programs.

Part III



Part III

Chapter 9 – WISP Overview

Chapter 10 – WISP User Guide

Chapter 11 – WISP Administrator Guide

Chapter 12 – Dissertation Conclusion and Future Research

Chapter 9

WISP Overview



CHAPTER OBJECTIVES

In this chapter, we will discuss:

WISP Introduction	Page 89
WISP Definitions	Page 89
WISP Assessments	Page 91
WISP Solutions	Page 91
System Administration	Page 92

9.1 WISP Introduction

WISP (A Wireless Information Security Portal) is a tool to support the management of a secure wireless network, and helps assure the confidentiality, integrity, and availability of the information systems in a wireless network environment. WISP is a prototype developed to demonstrate the benefit of a centralized place, where all essential support tools for managing wireless networks can be found.

WISP is divided into three main parts. Part 1 is the **WISP Definitions** section consisting of terms and concepts definitions. Part 2 is the **WISP Assessment** section, and Part 3 is the **WISP Solutions** section. Each different part is referred to as an **Application**, and a sub-module of **Application** is referred to as a **Module**, and a sub module of each **Module** is referred to as a **Function**.

We will now briefly discuss each Application. Figure 9.1 Illustrates the WISP navigation links.

9.2 Part 1: WISP Definitions

The definition section describes the computer system, the computer networks, and information security as well as the full dissertation in an electronic format. This section shall help non-specialists in the IT industry with basic terminologies and in understanding the technology.

There are four different modules under the application **WISP Definitions**, namely:

- **Computer Systems**
- **Computer Networks**
- **Information Security**
- **The Dissertation**

1. Computer Systems consists of the following functions:

- Computer Networks
- Hardware
- Software

2. Computer Networks consists of the following functions:

- Wired Networks
- Wireless Networks

WISP Navigation Links:

There are four main categories named APPLICATIONS

1. WISP Definitions
2. WISP Assessment
3. WISP Solutions
4. System Administration

WISP Menu Page

APP: WISP Definitions

No.	Modules	Functions	Citation
1	Computer Systems	Computer Networks	View
2	Computer Systems	Hardware	View
3	Computer Systems	Software	View
4	Computer Networks	Wired Networks	View
5	Computer Networks	Wireless Networks	View
6	Information Security	Info. Sec. Overview	View
7	Information Security	Info. Sec. Pillars	View
8	The Thesis	View Full Thesis	View
9	The Thesis	Download Document	View

APP: WISP Assessment

No.	Modules	Functions	Citation	View
1	Wireless Net. Sec. Risks	Assess Risks	In The Thesis	View
2	Wireless Net. Sec. Risks	View Risks	In The Thesis	View
3	Wireless Net. Type of Attacks	Assess Attack Types	In The Thesis	View
4	Wireless Net. Type of Attacks	View Attack Types	In The Thesis	View

APP: WISP Solutions

No.	Modules	Functions	View
-----	---------	-----------	------

Figure 9.1: WISP Navigation Links

3. Information Security consists of the following functions:

- Information Security (Info. Sec.) Overview
- Information Security (Info. Sec.) Pillars

4. The Dissertation consists of the following functions:

- View Full Dissertation
- Download Document

The next section discusses WISP Assessments.

9.3 Part 2: WISP Assessments

WISP Assessment provides a prototype questionnaire utilized to assess the risks and the types of attack. Every assessment is stored in the Database, so the result can be viewed later.

There are two different modules under the application **WISP Assessments**, namely:

- **Wireless Networks Security Risks (W/less Net. Sec. Risk)**
- **Wireless networks Type of Attacks (W/less Net. Type of Attacks)**

1. W/less Net. Sec. Risk consists of the following functions:
 - Assess Risks
 - View Risks
2. W/less Net. Type of Attacks consists of the following functions:
 - Assess Attack Types
 - View Attack Types

9.4 Part 3: WISP Solutions

WISP Solutions propose two ways of managing the security of wireless networks. The first solution is the strategic solution and the second is the practical solution. In the strategic solution section, the countermeasures to the identified risks are discussed, and sample policies and tips on how to create an awareness programs are provided.

In the practical solution section, a description of the freeware tools available on the internet is provided, and the link to each tool is also provided.

There are two different modules under the application **WISP Solutions**, namely:

- **Strategic Solutions**
- **Practical Solution**

1. Strategic Solutions consists of the following functions:
 - Security Strategy
 - Security Awareness Program
 - Security Policies
2. Practical Solutions consists of the following functions:
 - Technology
 - Non Technological

The next section discusses System Administration.

9.5 System Administration

The system administration provides a mechanism for easy administration of Applications, Modules, and Functions. In the System Administration one can add new topics in a hierarchical manner.

More description of the System Administration is provided in chapter 11.

Figure 9.2 provide a screen dump of the WISP main page.

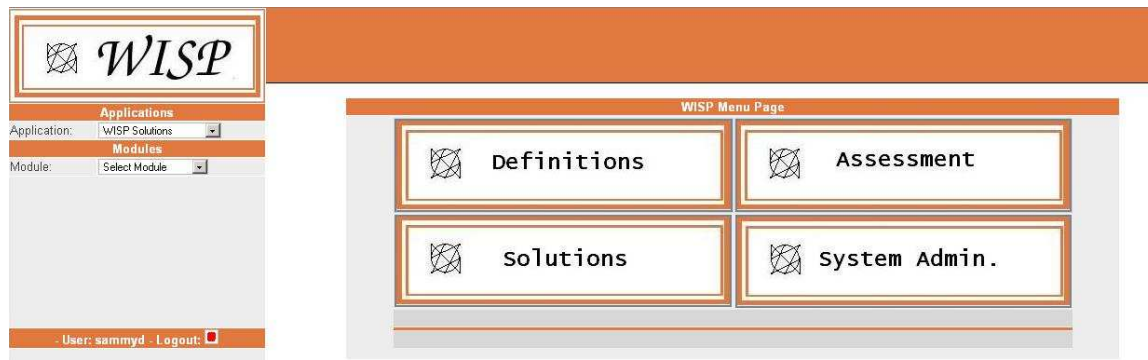


Figure 9.2: WISP Main Page

9.5 Developing WISP

The development of WISP was completed in two phases, the infrastructure development and the content development. The overall effort can be estimated to 280 hours, 180 for infrastructure development and 100 hours for the content development.

The infrastructure development is the first phase, and it provides easy creation of the building blocks of the system, the infrastructure includes WISP System Administration and the platform installation and configuration as well. The platform adopted for WISP is LAMP (Linux, Apache, MYSQL and PHP). The first phase was completed within 6 months.

The content development is the second phase, and it was relatively easy compared to the infrastructure development. The content development consists of developing the following three sections. WISP Definitions, WISP Assessment and WISP Solutions. The second phase was completed within three months. The next chapter discusses the user guide.

Chapter 10

WISP User Guide



CHAPTER OBJECTIVES

In this chapter, we will discuss:

WISP Definitions

Page 94

WISP Assessments

Page 95

WISP Solutions

Page 97


10.1 WISP Definitions

As mentioned earlier, WISP is divided into three main parts. Part 1 is the **WISP Definitions** section consisting of terms and concepts definitions. Part 2 is the **WISP Assessment** section, and Part 3 is the **WISP Solutions** section. The discussion in this chapter does not cover the full functionality of WISP. For that, a live demonstration of Wisp will be provided. Each of the three section is discussed below using screenshots from WISP.

In the **WISP Definitions**, depending on which function chosen, there is only one option, which is the “view” option. The whole definition section is to provide description used in the dissertation on the portal. The example below illustrates a possible scenario.

WISP Menu Page			
APP: WISP Definitions			
No.	Modules	Functions	Citation
1	Computer Systems	Computer Networks	View
2	Computer Systems	Hardware	View
3	Computer Systems	Software	View
4	Computer Networks	Wired Networks	View
5	Computer Networks	Wireless Networks	View
6	Information Security	Info. Sec. Overview	View
7	Information Security	Info. Sec. Pillars	View
8	The Thesis	View Full Thesis	View
9	The Thesis	Download Document	View

When the highlighted “view” link is clicked, the next screen will appear, displaying the introductory part about “Computer Networks”.



Applications

Application: WISP Definitions

Modules

Module: Computer Systems

Functions

Function: Computer Networks

User: sammyd Logout: ☐

2.3 Computer Networks

A computer network is composed of multiple connected computers that communicate over a wired or wireless medium to share resources. For instance, a home computer network may consist of two or more computers that share files and a printer using the network. The next section discusses the Computer Network Types.

2.3.1 Computer Network Types

Some types of computer networks are Local Area Networks (LAN), Metropolitan Area Networks (MAN) and Wide Area Networks (WAN). The main difference among these classifications is their area of coverage [40].

2.3.1.1 LANs

A local area network (LAN) is a network connecting computers in a relatively small area such as a building. Because the network is known to cover only a small area, optimizations can be made in the network signal protocols that permit data rates up to 1000Mb/s. LANs are communications network connecting computers by wire, or wireless link. LANs serve as parts of an organization located close to one another, generally in the same building. LANs allow users to share software, hardware and data [40]. Figure 2.2 shows an example of a LAN.

10.2 WISP Assessment

About the WISP Assessment, there two types of assessments, namely: **Assess Risks** and **Assess Attack Types**. When the highlighted “In The Dissertation” link is clicked, the next screen will appear, displaying the part about “Wireless Risks” in the dissertation.

APP: WISP Assessment				
No.	Modules	Functions	Citation	View
1	W/less Net. Sec. Risks	Assess Risks	In The Thesis	View
2	W/less Net. Sec. Risks	View Risks	In The Thesis	View
3	W/less Net. Type of Attacks	Assess Attack Types	In The Thesis	View
4	W/less Net. Type of Attacks	View Attack Types	In The Thesis	View

However, when the highlighted “View” link is clicked, the next screen will appear, displaying the questionnaire that is used to get input from user.

APP: WISP Assessment				
No.	Modules	Functions	Citation	View
1	W/less Net. Sec. Risks	Assess Risks	In The Thesis	View
2	W/less Net. Sec. Risks	View Risks	In The Thesis	View
3	W/less Net. Type of Attacks	Assess Attack Types	In The Thesis	View
4	W/less Net. Type of Attacks	View Attack Types	In The Thesis	View

WISP Assessment > W/less Net. Sec. Risks > Assess Risks

Company Name:

Company Description:

Category 1: Inherent Security Risks

Signal Overflow:

Is the boundaries of the Wireless LAN defined?

How many APs are attached to the network?

Is there an awareness program about the security issues of W/Less Networks?

Easy Deployment:

What is the company stand point about the W/Less Network usage?

Is there a policy enforcing the company view about W/Less Networks?

Is there incidents reporting mechanism in place?

Category 2: Security Risks of W/Less Devices

Rogue APs:

Do you monitor for rogue APs around the work place?

Is there a procedure in place to deal with rogue APs?

Is there a step by step configuration applied to all APs?

Is the default setting changed before attaching an AP to the network?

Wireless Clients:

how many wireless clients use the W/Less network?

Is there training program for wireless users?

Do you regularly check the access log to check connections to the AP?

Category 3: Security Risks of Wireless Networks Communication

Lack of encryption:

Do you use encryption?

Which encryption do you use?

Lack of MAC Address Filtering:

Do you use Mac Address filtering?

After getting inputs from the user, WISP will display appropriate result to the user based on the inputs supplied. The result will look like the following:

WISP Assessment > W/less Net. Sec. Risks > Risk Assessment Result	
Category 1: Inherent Security Risks	Low
Category 2: Security Risks of W/Less Devices	Low
Category 3: Security Risks of Wireless Networks Communication	Low
Overall Security Risks	Low

The “Assess Attack Types” works in similar manner.



10.3 WISP Solutions

The **WISP Solutions** section, also provide static information on how a specific solution could be adopted, and by referring to the screen below:

APP: WISP Solutions			
No.	Modules	Functions	View
1	Strategic Solutions	Security Strategy	View
2	Strategic Solutions	Security Awareness Program	View
3	Strategic Solutions	Security Policies	View
4	Practical Solution	Technology	View
5	Practical Solution	Non Technological	View

When the highlighted “view” link is clicked, the next screen will appear, displaying the information about “Security Strategy”.

UNIVERSITY
OF
JOHANNESBURG

Strategic Solution, Security Strategy

A possible strategy for securing wireless network includes:

- ♦ Risk Assessment
 1. Risk Assessment
 2. Types of Attacks Assessment
- ♦ Review and Development
 1. Policy Documents
 2. Awareness Programs
 3. Integrate W/Less Network Security Solution with the overall IT Security Strategy
- ♦ Monitor and Control
 1. Routine Checks
 1. Monitor W/Less Boundaries
 2. Monitor for Rogue APs
 2. Incident Reports



Created by : S Diakite

Examples of a security strategy

The next chapter discusses the administrator guide.

Chapter 11

WISP Administrator Guide



CHAPTER OBJECTIVES

In this chapter, we will discuss:

System Requirements

Page 100

Installation Guide

Page 100

Administration Structure

Page 101

11.1 System Requirement

The minimum hardware requirement specification for WISP as follow:

- 32-bit x86 processor (386, 486, Pentium, Pentium MMX, Pentium Pro and Pentium II. Also supported clones such as Cyrix, AMD and TI)
- ISA, EISA, PCI or VLB Bus.
- 4MB or more of RAM
- VGA Compatible video card
- 40MB of Hard Disk Space (after installing all modules)
- CD-ROM drive, in case you installing from a WISP CD-ROM.

The software requirement specification for WISP as follow:

- PHP: PHP Version 4.3.x
- Apache: Version Apache/2.0.x
- MySQL: mysql Ver 14.7 Distrib 4.1.10a
- OS: Linux kernel 2.6.x

11.2 Installation Guide

The installation step would first require the installation of Linux, Apache, MySQL and PHP (LAMP).

For LINUX installations guide refer to: <http://www.linux.org/docs/beginner/install.html>

For PHP installations refer to: <http://www.php.net/install>

For Apache installations refer to: <http://httpd.apache.org/docs/2.0/install.html>

For MySQL installations refer to: <http://dev.mysql.com/doc/refman/4.1/en/installing.html>

Upon a successful installation of the LAMP platform, the following steps must be carried out:

- 1) Run the following command to create the WISP DB named "wisp"
 - a. `mysqladmin -u root -p create wisp`
 - b. then, type in the password for root@localhost
- 2) Copy the "wisp" folder to "/var/www/html/." So that the files can accessed
 - a. The following command shall do the copying, after inserting the cd-rom containing wisp files:
 - b. `"cp -vr /media/cdrom/wisp /var/www/html/."`

- 3) Run the following command as root to import the wisp DB
 - a. `"cat /var/www/html/wisp/wisp.sql | mysql -u root -p"`
 - b. Then, type in the password for root@localhost
- 4) Edit the file `/var/www/html/wisp/inc/db.php` to set the following values:
 - a. `var $dbHost = "localhost";` // the IP of the host can work as well
 - b. `var $dbUser = "mysql";` // The user for mysql DB -
 - c. `var $dbPasswd = "mysql123";` // mysql user password
- 5) Go to this url: <http://localhost/wisp/index.php>
- 6) If all the steps have followed correctly the installation is completed.

11.3 Administration Structure

WISP is organized in a hierarchical manner, every functionality within WISP falls under a specific Module, and each module is under an application. This section discusses how to manage each of these topics.

11.3.1 Application Management

There are three possible options for application management. The options are as follow:

- 1) Add Application
 - 2) Edit Application
 - 3) Delete Application
-
- 1) For Add Application
 - a. Use the navigation bar on the left and select "System Administration"



The screenshot shows the WISP Administrator interface. At the top is the WISP logo, which consists of a geometric wireframe cube icon followed by the text "WISP" in a stylized serif font. Below the logo is an orange header bar with the word "Applications" in white. Underneath this bar, there is a label "Application:" followed by a dropdown menu. The dropdown menu is open, showing a list of options: "Select Application", "WISP Definitions", "WISP Assessment", "WISP Solutions", and "System Administration". The "System Administration" option is highlighted with a blue background. At the bottom of the interface, there is an orange bar containing the text "- User: sammyd - Logout:" followed by a small red square icon.

b. Then select "Application Management"



This screenshot shows the WISP Administrator interface after the "System Administration" application has been selected. The "Application:" dropdown now displays "System Administration". Below the orange "Applications" header bar is another orange header bar labeled "Modules". Underneath, there is a label "Module:" followed by a dropdown menu. This menu is open, showing a list of options: "Select Module", "User Management", "Application Management", "Module Management", and "Function Management". The "Application Management" option is highlighted with a blue background. The bottom of the interface features the same orange bar with the text "- User: sammyd - Logout:" and a red square icon.

c. The select "List Applications"

WISP

Applications

Application:

Modules

Module:

Functions

Function:

Select Function
List Application
Add Application

User: sammyd - Logout:

d. A list of all application would then be displayed

System Administration > Application Management > List Applications			
Application ID	Application Short Name	Application Full Name	Functions
13	WSD	WISP Definitions	Edit Delete
12	WSA	WISP Assessment	Edit Delete
11	WSS	WISP Solutions	Edit Delete
6	ADM	System Administration	Edit Delete

e. To add a new select “Add Application” from the navigation bar



The screenshot shows the WISP Administrator Interface. At the top is the WISP logo, which includes a geometric icon and the text "WISP". Below the logo are three sections: "Applications", "Modules", and "Functions". Each section has a dropdown menu. The "Applications" dropdown is set to "System Administration". The "Modules" dropdown is set to "Application Management". The "Functions" dropdown is open, showing options: "List Application", "Select Function", "List Application", and "Add Application". At the bottom of the interface, it says "User: sammyd - Logout:" followed by a red square icon. A faint watermark of a university logo and the text "UNIVERSITY OF JOHANNESBURG" is visible in the background.

- f. Fill in the "Application Name" and "Application Description" then click on "Add>>"

The screenshot shows the "Add Application" form. The breadcrumb navigation at the top reads "System Administration > Application Management > Add Application". The form has two input fields: "Application Name" with the value "WST" and "Application Description" with the value "WISP Test". Both fields have a red asterisk indicating a required field. Below the input fields are two buttons: "Add>>" and "Reset".

- g. A confirmation screen will display the result of the operation

Application Added
Application Added Successfully

System Administration > Application Management > List Applications			
Application ID	Application Short Name	Application Full Name	Functions
29	WST	WISP Test	Edit Delete
13	WSD	WISP Definitions	Edit Delete
12	WSA	WISP Assessment	Edit Delete
11	WSS	WISP Solutions	Edit Delete
6	ADM	System Administration	Edit Delete

As for **Module Management** and **Function Management** similar procedures are followed to add new topics. However, it is important to note that **Application** must be added first, and then **Module** for the **Application** can be added. In the same fashion, **Module** must be added first, and then **Function** for the **Module** can be added.

The example below illustrates how to add a function “References” under Application “WISP Definitions” and Module “The Dissertation”.

Navigate to list Functions, and then select “Add Function”. As shown below:

System Administration > Function Management > Add Function	
Function Name:	WSREFS *
Function Description:	References *
Application:	System Administration ▼
<input type="button" value="Next>>"/> <input type="button" value="Reset"/>	<ul style="list-style-type: none"> System Administration WISP Solutions WISP Assessment WISP Definitions WISP Test

After selecting WISP Definitions as the Application, click on the “Next>>” button, which will display the following screen:

System Administration > Function Management > Add Function

Function Name:	WSREFS
Function Description:	References
Application:	WISP Definitions
Module:	The Thesis
File Path:	files/references.php
Display:	No
<input type="button" value="Add>>"/> <input type="button" value="Reset"/>	

As it can be observed, the module “The Dissertation” must be selected, and the file path must always be in the following format: “files/{file_name}” in this case the file path is: “files/references.php”.

The display option must be set “yes” for the function to appear in the navigation bar.

At this stage the file “references.php” is inserted in hierarchy database of WISP. However the file must still be created and edited, then copied over to wisp server. It must go under the following directory: “/var/www/html/wisp/files/.”.

11.3.2 Edit and Delete

The edit and delete function operate in similar fashion. For instance, to edit a module, one must use the navigation bar to list the module, as displayed below



Applications

Application: System Administration

Modules

Module: Module Management

Functions

Function: List Module

- User: sammyd - Logout:

System Administration > Module Management > List Modules				
Module ID	Module Short Name	Module Full Name	Module Application Name	Functions
4	USRMGT	User Management	System Administration	Edit Delete
5	APPMGT	Application Management	System Administration	Edit Delete
6	MODMGT	Module Management	System Administration	Edit Delete
7	FUNMGT	Function Management	System Administration	Edit Delete
8	STRSOL	Strategic Solutions	WISP Solutions	Edit Delete
9	PRCSOL	Practical Solution	WISP Solutions	Edit Delete
14	WSD	Definitions	WISP Introduction	Edit Delete
13	WES	Executive Summary	WISP Introduction	Edit Delete
15	WSSR	W/less Net. Sec. Risks	WISP Assessment	Edit Delete
16	WST	W/less Net. Type of Attacks	WISP Assessment	Edit Delete
17	WOGSSC	Sanity Check List	WISP OGS (OnGoing Support)	Edit Delete
18	WOGSOC	Operational Check List	WISP OGS (OnGoing Support)	Edit Delete
21	WSCOMP	Computer Systems	WISP Definitions	Edit Delete
22	WSNET	Computer Networks	WISP Definitions	Edit Delete
23	WSSEC	Information Security	WISP Definitions	Edit Delete
26	WSTH	The Thesis	WISP Definitions	Edit Delete

Then click on either of the links to the right, to Edit or Delete. The rest is self explanatory.

Chapter 12

Dissertation Conclusion and Future Research



CHAPTER OBJECTIVES

In this chapter, we will discuss:

The Problem Statement

Page 108

The Objectives

Page 109

Future Research

Page 111

12.1 Introduction

This chapter is the final chapter of this dissertation. The aim here is to show that the research objectives set at the beginning of this document were achieved.

The chapter begins with a review of the problem statement and the research objectives. It also demonstrates how these research objectives were achieved by referring back to the previous chapters. This is followed by a discussion of topics for further research. The chapter concludes with a word from the author, describing the lessons learnt in this research.

The next section reviews the research problem and discusses how the objectives of this dissertation were achieved.

12.2 The Problem Statement

The problem identified in Chapter 1 was that:

It is challenging for managers to introduce wireless networks and properly manage the security of wireless networks. Security problems of wireless networks are the main reason for wireless networks not being rolled out optimally [1]. Tools to support such management are available, but spread over many books, papers and websites. No real centralized place exists where all essential support can be found.

The dissertation centralizes the tools to support the management of security problems of wireless networks. This was achieved by **WISP (A Wireless Information Security Portal)**, a prototype that was developed at the end of this dissertation, to demonstrate how a web based application can be used to centralize the information needed to properly manage the security of wireless networks.

To solve the research problem, it was necessary to develop a prototype that would centralize relevant information. Such a solution was the goal of this research, and the goal was achieved through the completion of the research objectives. The dissertation was structured in a logical manner following the research objectives (see Chapter 1). All the research objectives were achieved and are discussed in the following paragraphs.

12.3 The Objectives

By referring to what was stated as the objectives of this research in chapter 1, the objectives are as follow:

- 1) **Review of computers and computer networks including both wired and wireless networks.**
- 2) **Introduce the concept of Information Security emphasizing Network Security.**
- 3) **Understand how the wireless LANs work and investigate the security risks of wireless LANs.**
- 4) **Propose a solution for securing wireless LANs.**
- 5) **Demonstrate how a web portal (WISP) can be used to consolidate support tools and manage the information security requirements of a wireless LAN.**

12.3.1 Objective 1

The first objective was to discuss a review of computers and computer networks including both wired and wireless networks. In Part I, chapter 2, we have introduced the computer system discussing the hardware, as well as the software components of the computer system. Furthermore, chapter 3 discussed the wired networks and chapter 4 discussed wireless networks. It was discovered that wireless networks devices inherently presented extra security risks for the wireless network, and the security mechanism for securing wireless networks communication is weak compared to wired networks. This achieved the first objective.

12.3.2 Objective 2

The second objective was to introduce the concept of Information Security. In chapter 5, we had a discussion of Information Security, and the Information Security Pillars, namely: Identification and Authentication, Authorization, Confidentiality, Integrity, Non-repudiation. We have discovered that Information Security is the process of protecting data from unauthorized access, use, disclosure, destruction, modification, or disruption. If we can enforce the five pillars of Information Security, we have gone a long way in ensuring that the information resources of the company are secure. This achieved the second objective.

12.3.3 Objective 3

The third objective was to understand how the wireless LANs work and investigate the security risks of wireless LANs. To understand how wireless LANs work, it was beneficial to categorize wireless LAN security risks based on the type of risks. Hence, we had three different categories, namely: the inherent risks, risks associated with the devices, and the risks associated with the



communication. Each of these categories was discussed in chapter 6. In chapter 7, we have also classified the type of attacks that can be launched against wireless LANs. This achieved the third objective.

12.3.4 Objective 4

The fourth objective was to propose a solution for securing wireless LANs. After categorizing the risks and classifying the type of attacks it was easy to study each category and propose a countermeasure for each risk under all the three different categories. This achieved the fourth objective, and it was done in chapter 8.

12.3.5 Objective 5

The fifth objective was to demonstrate how a web portal (WISP) can be used to consolidate support tools and manage the information security requirements of a wireless LAN. A prototype was required for that demonstration, and WISP was developed and documented. Chapter 9 gives an overview of WISP. Chapter 10 and 11 provides user guide and administrator guide. This achieved the fifth objective. Figure 12.1 on the following page provides an overview of the research objectives in relation to the dissertation layout.



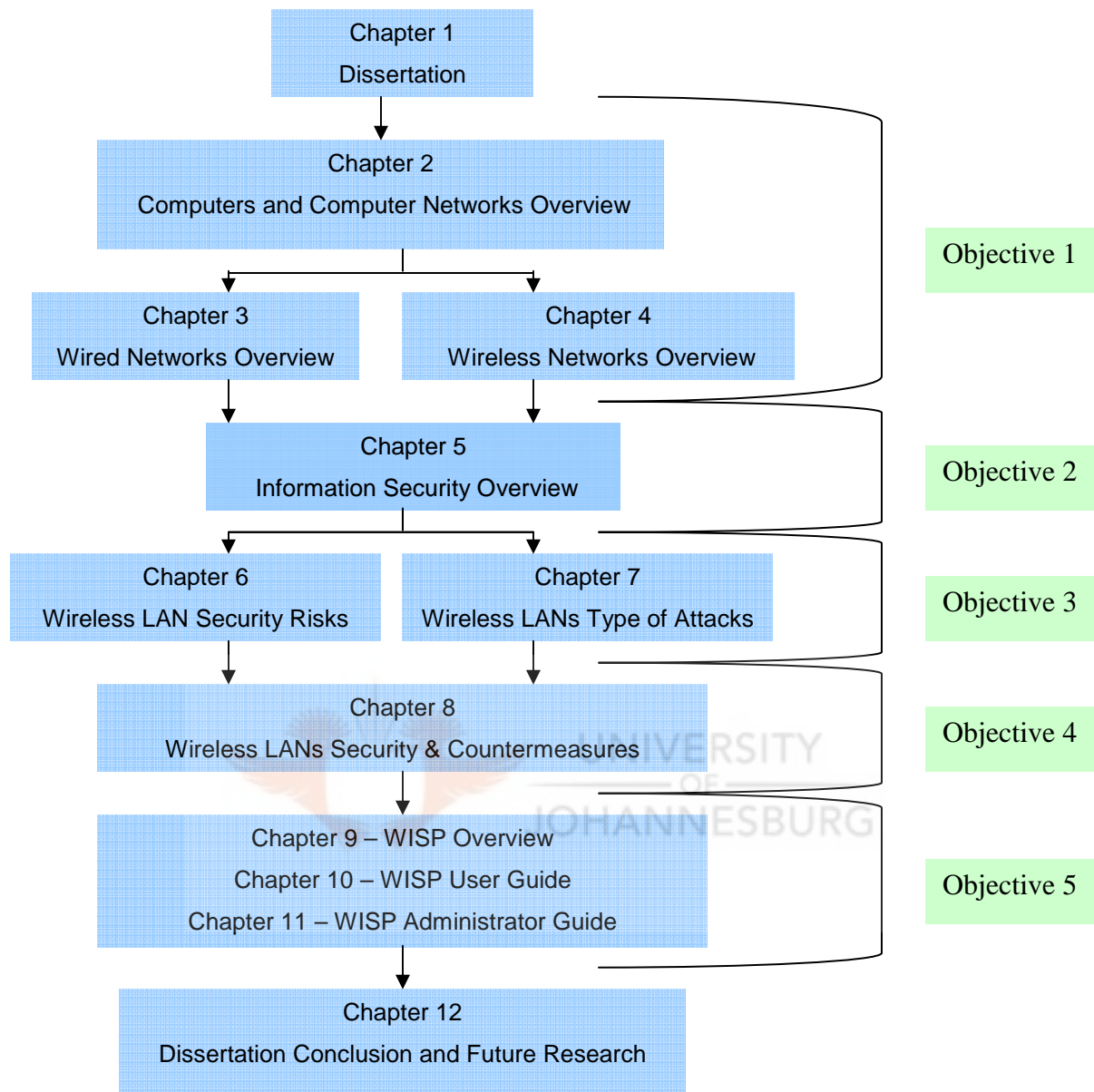


Figure 12.1 Research objectives relative to dissertation layout

12.4 Future Research

The development of WISP has brought about a number of areas that can be investigated further:

- Integration of the assessment result to indicate possible countermeasures
- A reporting mechanism can be added to WISP to generate reports about the security status
- A platform to edit the concepts defined in WISP
- Extending the measurement criteria for assessment to get more accurate result



12.5 Final Word

Through this research, the author has developed skills such as the ability to collect, evaluate and analyze research material, articulate abstract thoughts, and introduce concepts in a structured manner, and to make use of ideas and concepts regarding problem solving. The development of the prototype (WISP), helped the author in making use of programming skills learned in previous work environments. These skills will prove invaluable in all facets of life. The author is extremely proud of being able to compile this dissertation. The successful completion of this dissertation has allowed the author to grow as a researcher.



Appendix A – Detailed Description

A.1 Computer Systems Hardware Components

A.1.1 System Unit	<p>The system unit of the computer system consists of two main components, the CPU (Central processing Unit) and RAM (Random Access Memory).</p> <p>CPU - The central processing unit (CPU) is also known as the processor. The processor is the electronic component that interprets and carries out the basic instructions that operate the computer [13].</p> <p>The CPU contains an arithmetic logic unit (ALU). The ALU performs arithmetic and logical operations on binary code in the computer. The CPU also contains other processing elements and functions, including program counters, control logic, registers, and accumulators [13].</p> <p>Memory or Random access memory (RAM) is used for primary memory storage. This is the high speed memory directly addressable by the CPU. The RAM consists of components that store instructions waiting to be executed and data needed by those instructions [7].</p>
A.1.2 Input devices	<p>An input device is any hardware component that allows you to enter data and instructions into a computer. Some widely used input devices include the keyboards, mouse, microphone, scanner, and video camera [13].</p>
A.1.3 Output Devices	<p>An output device is any hardware component that conveys information to one or more people. Some widely used output devices include the monitor or screen, printers, and speakers [13].</p>
A.1.4 Storage Devices	<p>The storage device is a secondary memory that store data. It is larger, slower memory storage area, and consists of the hard disk drives, floppy disk drive, USB flash drives, CDs, DVDs, and tapes.</p>
A.1.5 Communication Devices	<p>A communication device is a hardware component that enables a computer to send and receive data, instructions and information to and from one or more computers [13]. Some widely used communication devices include Network Interface Card (NIC), modem, wireless router, and wireless client.</p>

A.2 Definitions

A.2.1

File sharing

File sharing is the practice of making files available for other users to download over the Internet and smaller networks. Usually file sharing follows the peer-to-peer (P2P) model, where the files are stored on and served by personal computers of the users. Most people who engage in file sharing are also downloading files that other users share [79].

A.2.2

Dynamic Host Configuration Protocol (DHCP)

Dynamic Host Configuration Protocol (DHCP) is a protocol used by networked computers (*clients*) to obtain IP addresses and other parameters such as the default gateway, subnet mask, and IP addresses of DNS servers from a DHCP server. The DHCP server ensures that all IP addresses are unique, e.g., no IP address is assigned to a second client while the first client's assignment is valid (its *lease* has not expired). Thus IP address pool management is done by the server and not by a human network administrator.

A.2.3

RADIUS

Remote Authentication Dial In User Service (RADIUS) is an AAA (authentication, authorization and accounting) protocol for applications such as network access or IP mobility. It is intended to work in both local and roaming situations. Many networks services (including corporate networks and public ISPs using modem, DSL, or wireless 802.11 technologies) require users to present security credentials (such as a username and password or security certificate) in order to connect on to the network [81].

Before access to the network is granted, this information is passed to a Network Access Server (NAS) device over the link-layer protocol (for example, Point-to-Point Protocol (PPP) in the case of many dialup or DSL providers), then to a RADIUS server over the RADIUS protocol.

The RADIUS server checks that the information is correct. If accepted, the server will then indicate to the NAS that the user is authorized to access the network. RADIUS also allows the authentication server to supply the NAS with additional parameters, such as

- The specific IP address to be assigned to the user
- The address pool from which the user's IP should be chosen
- The maximum length that the user may remain connected
- An access list, priority queue or other restrictions on a user's access
- L2TP parameters

The RADIUS protocol does not transmit passwords in clear text between the NAS and RADIUS server, but in hidden, using a rather complex operation instead, which involves MD5 hashing and shared secret [81].

RADIUS is also commonly used for accounting purposes. The NAS can use RADIUS accounting packets to notify the RADIUS server of events such as

- The user's session start
- The user's session end
- Total packets transferred during the session
- Volume of data transferred during the session
- Reason for session ending

The primary purpose of this data is so that the user can be billed accordingly; the data is also commonly used for statistical purposes and for general network monitoring.

Additionally RADIUS is widely used by VoIP service providers. It is used to pass login credentials of a SIP end point (like a broadband phone) to a SIP Registrar using digest authentication, and then to RADIUS server using RADIUS. Sometimes it is also used to collect call detail records (CDRs) later used, for instance, to bill customers for international long distance [81].

A.2.4 IPsec

IPsec (IP security) is a suite of protocols for securing Internet Protocol (IP) communications by authenticating and/or encrypting each IP packet in a data stream. IPsec also includes protocols for cryptographic key establishment [91].

IPsec protocols operate at the network layer, layer 3 of the OSI model. Other

	<p>Internet security protocols in widespread use, such as SSL, TLS and SSH, operates from the transport layer up (OSI layers 4 - 7). This makes IPsec more flexible, as it can be used for protecting layer 4 protocols, including both TCP and UDP, the most commonly used transport layer protocols [91]. IPsec has an advantage over SSL and other methods that operate at higher layers. For an application to use IPsec no code change in the applications is required whereas to use SSL and other higher level protocols, applications must undergo code changes [91].</p>
A.2.5 Secure Shell	<p>Secure Shell or SSH is a network protocol that allows data to be exchanged over a secure channel between two computers. Encryption provides confidentiality and integrity of data. SSH uses public-key cryptography to authenticate the remote computer and allow the remote computer to authenticate the user, if necessary [90]. SSH is typically used to log into a remote machine and execute commands, but it also supports tunneling, forwarding arbitrary TCP ports and X11 connections; it can transfer files using the associated SFTP or SCP protocols [91].</p> <p>An SSH server, by default, listens on the standard TCP port 22. An ssh client program is typically used for establishing connections to an sshd daemon accepting remote connections. Both are commonly present on most modern operating systems, including Mac OS X, Linux, Solaris and OpenVMS. Proprietary, freeware and open source versions of various levels of complexity and completeness exist [90].</p>
TLS and SSL	<p>Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide secure communications on the Internet for such things as web browsing, e-mail, Internet faxing, instant messaging and other data transfers. There are slight differences between SSL and TLS, but the protocol remains substantially the same [93].</p> <p>The TLS protocol allows applications to communicate across a network in a way designed to prevent eavesdropping, tampering, and message forgery. TLS provides endpoint authentication and communications privacy over the Internet using cryptography [93].</p>

Typically, only the server is authenticated (i.e., its identity is ensured) while the client remains unauthenticated; this means that the end user (whether an individual or an application, such as a Web browser) can be sure with whom they are communicating. The next level of security—in which both ends of the "conversation" are sure with whom they are communicating—is known as mutual authentication. Mutual authentication requires public key infrastructure (PKI) deployment to clients unless TLS-PSK or TLS-SRP are used, which provide strong mutual authentication without needing to deploy a PKI [93].

TLS involves three basic phases:

1. Peer negotiation for algorithm support
2. Public key exchange and certificate-based authentication
3. Symmetric cipher encryption

During the first phase, the client and server negotiate cipher suites, which combine one cipher from each of the following:

- * Public-key cryptography: RSA, Diffie-Hellman, DSA
- * Symmetric ciphers: RC2, RC4, IDEA, DES, Triple DES, AES or Camellia
- * Cryptographic hash function: MD2, MD4, MD5 or SHA

A.3 OSI Model

A.3.1 Layer 7:

The Application layer

The application layer is the seventh level of the seven-layer OSI model. It interfaces directly to and performs common application services for the application processes. It also issues requests to the presentation layer. The common application services sub layer provides functional elements including the Remote Operations Service Element (comparable to Internet Remote Procedure Call), Association Control, and Transaction Processing.

A.3.2 Layer 6:

The Presentation layer

The Presentation layer transforms the data to provide a standard interface for the Application layer. MIME encoding, data encryption and similar manipulation of the presentation are done at this layer to present the data as a service or protocol developer sees fit.

Examples of this layer are converting an EBCDIC-coded text file to an ASCII-coded file, or serializing objects and other data structures into and out of XML [49].

A.3.3 Layer 5:

The Session layer

The Session layer controls the dialogues/connections (sessions) between computers. It establishes, manages and terminates the connections between the local and remote application. It provides for either full-duplex or half-duplex operation, and establishes check pointing, adjournment, termination, and restart procedures [49].

<p>A.3.4 Layer 4:</p> <p>The Transport layer</p>	<p>The Transport layer provides transparent transfer of data between end users, providing reliable data transfer while relieving the upper layers of it. The transport layer controls the reliability of a given link through flow control, segmentation/de-segmentation, and error control.</p> <p>Some protocols are state and connection oriented. This means that the transport layer can keep track of the segments and retransmit those that fail. The best known example of a layer 4 protocol is the Transmission Control Protocol (TCP). The transport layer is the layer that converts messages into TCP segments or User Datagram Protocol (UDP), etc.</p> <p>Perhaps an easy way to visualize the Transport Layer is to compare it with a Post Office, which deals with the dispatch and classification of mail and parcels sent [49].</p>
<p>Layer 3:</p> <p>The Network layer</p>	<p>The Network layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks while maintaining the quality of service requested by the Transport layer.</p> <p>The Network layer performs network routing functions, and might also perform fragmentation and reassembly, and report delivery errors. Routers operate at this layer—sending data throughout the extended network and making the Internet possible. The best known example of a layer 3 protocol is the Internet Protocol (IP) [9].</p>

<p>A.3.6 Layer 2:</p> <p>The Data Link layer</p>	<p>The Data Link layer provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical layer. The best known example of this is Ethernet. This layer may be split into a Media Access Control (MAC) layer and the IEEE 802.2 Logical Link Control (LLC) layer. It arranges bits from the physical layer into logical chunks of data, known as frames [9].</p> <p>This is the layer at which the bridges and switches operate. Connectivity is provided only among locally attached network nodes forming layer 2 domains for broadcast forwarding [9].</p>
<p>A.3.7 Layer 1:</p> <p>The Physical layer</p>	<p>The Physical layer defines all the electrical and physical specifications for devices. In particular, it defines the relationship between a device and a physical medium. This includes the layout of pins, voltages, and cable specifications, hubs, repeaters, and network adapters.</p> <p>These seven layers summarize the Open System Interconnection (OSI) paradigm that was established by the International Standard Organization (ISO) for communications worldwide. It divides the networking process into seven logical layers, starting at operating system level and descending to the cable and interface card level. The layers are: Application, Presentation, Session, Transport, Network, Data link and Physical.</p>

A.4 Wardriving

A.4.1

Description

The informal expression used more often for searching for a signal is wardriving.

Because there is no means to limit who receives the signal, unapproved wireless device can pick up the beaconing RF transmission. Wireless location mapping is the formal expression used to refer to this passive wireless discovery, or the process of finding a WLAN signal and recording information about it.

A.4.2

Techniques used by wardrivers

Some of the techniques used by wardrivers include:

- Driving at a slower speed - The general consensus is that a speed of about 35 MPH is the best for wardriving. Some of the software used to pick up the signal requires time to identify and log the transmission. Driving too fast will not allow the signal to be within range for a long enough period of time.
- Using surface streets - On most freeways the road is farther away from buildings than on surface streets. Being closer to the source allows more RF signals to be identified.
- Creating a plan - Many wardrivers start with street map of the area and block it out into sectors. Starting with the first sector, they drive up and down every street on the map within that sector and record the signal received.
- Repeating over time - Defining a route and then wardriving it on a weekly or monthly basis, helps to identify new WLANs as they are installed.

Knowing the techniques of wardriving is important if you want to limit your exposure. For example, knowing that wardrivers typically repeat their route regularly means that just because your WLAN does not appear today on a public map of wireless hotspots does not mean it won't be found tomorrow.

<p>A.4.3</p> <p>Mobile Computing Devices</p>	<p>A mobile computing device used for wardriving can be a standard portable computer, of which there are two types. One is laptop computer, which contains the traditional features of a desktop computer (screen, keyboard, hard drive, etc.) but in smaller package to allow for mobility.</p> <p>The other type of standard portable computing device is a tablet computer. The key element of a tablet computer is the ability to navigate and enter data using a stylus instead of a keyboard.</p> <p>Tablet computers have several advantages:</p> <ul style="list-style-type: none"> • Users can write rather than type on keyboard. • Handwritten notes are immediately digitized, which makes them easier to amend and share with others. • Drawings, formulas, signature, and other graphical objects can be easily used and manipulated on a tablet computer. <p>Even smaller than a laptop or tablet computer is handheld PC. A handheld PC is small enough to be held in a single hand yet has many of the features of a laptop computer.</p> <p>These features include a screen supporting a resolution of greater than 480 x 240, keyboard, an infrared (IrDA) port, and Universal Serial Bus (USB) connectivity.</p>
<p>A.4.4</p> <p>Wireless Network Interface Card (NIC)</p>	<p>The hardware that allows the mobile computing device to detect a wireless signal is a wireless network interface card (or wireless network adapter). Unlike their desktop counterparts, wireless NICs for mobile devices are available in variety of shapes and styles.</p> <p>For laptop, tablet, and handheld PCs, an external wireless NIC can plug into the USB port.</p> <p>In addition, PC card wireless Instead of being a separate device, most laptops and tablet has the wireless NIC built in as a Mini PCI. A Mini PCI is a small card that is functionally equivalent to a standard PCI expansion card. It was specifically developed for integrating communications peripherals such as modems and network interface cards onto a laptop computer.</p>

A.4.5**Antennas**

Although all wireless NIC adapters have embedded antennas, attaching an external antenna will significantly increase the ability to detect a wireless signal. There are two fundamental characteristics of antennas. First, as the frequency gets higher the wavelength becomes smaller. This means that the size of the antenna is smaller.

There are three basic categories of antennas: Omni-directional, semi-directional, and highly directional. The most common type of antenna for WLAN, whether wardriving or in standard use, is an Omni-directional antenna. An Omni-directional antenna detects signals from all directions equally.

A.4.6**Global Positioning System**

The final piece of hardware used for wardriving is a global positioning system (GPS) receiver, which is one part of the entire GPS system. The GPS system, which was originally developed by the U.S military in the late 1970s as a navigation system but was later opened to civilian use, is used to precisely identify the location of the receiver.

GPS is composed of 27 earth-orbiting satellites, each of which circles the globe twice each day at a height of 19,300 km (12,000 miles). Of the 27 GPS satellites in space only 24 are in operation. The remaining three are spares in case a satellite fails.

A.4.7**Software Tools**

In addition to wardriving hardware, software is also necessary to detect a WLAN signal. Wardriving software can be divided into three categories: client utilities, integrated operating system tools, and freeware discovery applications.

Client Utilities - When WLANs first appeared, operating systems were not equipped to be aware of their presence. Wireless NIC adapter manufacturers include client software utilities that were used to detect a wireless signal and then connect to that network. These client utilities also provided the ability to adjust client parameters, report statistics, and show signal strength. **Integrated Operating System Tools** - One reason why NIC adapter manufacturers stopped distributing client utilities is because operating systems have become wireless aware. This integration of wireless networking into the operating system has made it much easier to use WLANs. **Freeware Discovery Applications** see appendix B.

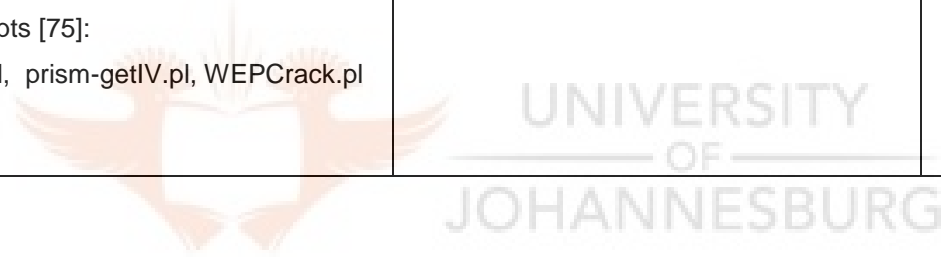


Appendix B – Freeware Applications

Name	Description	Positive Use	Negative Use
B.1 NetStumbler	<p>NetStumbler (also known as Network Stumbler) is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards. It runs on Microsoft Windows operating systems from Windows 98 on up to Windows Vista. A trimmed-down version called MiniStumbler is available for the handheld Windows CE operating system [96].</p> <p>NetStumbler is also available for Apple computers in the form of an application known as MacStumbler.</p>	<p>NetStumbler can be used to [69]:</p> <ul style="list-style-type: none"> * Verify that your network is set up and configured properly. * Find locations with poor coverage in the WLAN. * Detect other networks that may be causing interference on the network. * Detect unauthorized “rogue” Access Points. * Help aim directional antennas for long-haul WLAN links. 	<p>NetStumbler can be used by attackers to collect secret pieces of information as the following [61]:</p> <ul style="list-style-type: none"> * Wireless Access Point's SSID (Service Set Identification, the unique name you can assign to your WAP). * Signal strength of the discovered Wireless Access Point (WAP) and whether the WAP is using encryption. * What channel the WAP is transmitting on.
B.2 Nmap "Network Mapper"	<p>Nmap ("Network Mapper") is a free open source utility for network exploration or security auditing [68].</p> <p>Nmap is designed to allow system administrators and curious individuals to scan large networks to determine which hosts are</p>	<p>Nmap can be used for [70]:</p> <ul style="list-style-type: none"> * Auditing the security of a computer, by identifying the network connections which can be made to it. * Identifying open ports on a target computer in preparation for attacking it. 	<p>Nmap can be used by attackers for [70]:</p> <ul style="list-style-type: none"> * Host Discovery - Identifying computers on a network, for example listing the computers which respond to pings, or which have a particular

	<p>up and what services they are offering [70].</p> <p>Nmap runs on most types of computers and both console and graphical versions are available [68].</p>	<p>* Network inventory, maintenance, and asset management.</p> <p>* Auditing the security of a network, by identifying unexpected new servers.</p>	<p>port open.</p> <p>* Port Scanning - Enumerating the open ports on one or more target computers</p> <p>* OS Detection - Remotely determining the operating system and some hardware characteristics of network devices.</p>
B.3 AirSnort	<p>AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys, it operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered [73].</p> <p>It is estimated that AirSnort needs to capture only five or six million packets and chew on them for as little as a minute, or as long as a couple of hours, before it can chew through the encryption and reveal the WEP key.</p> <p>Those time estimates were unbelievable in 2001. Imagine how much faster today's 2- and 3-gigahertz machines can mow through the same amount of data [61].</p>	<p>AirSnort can be used for [61]:</p> <p>* Auditing the strength of a WEP encryption key.</p>	<p>AirSnort can be used by attackers to [61]:</p> <p>* Discover the network encryption key.</p>

B.4 WEP Crack	<p>WEPCrack is an open source tool for breaking 802.11 WEP secret keys. This tool is an implementation of the attack described in the paper "Weaknesses in the Key Scheduling Algorithm of RC4". This paper was released by Scott Fluhrer, Itsik Mantin and Adi Shamir (who was one of the inventors of the RSA encryption algorithm) [74].</p> <p>WEPCrack actually consists of the following three Perl scripts [75]: WeakIVGen.pl, prism-getIV.pl, WEPCrack.pl</p>	<p>WEPCrack can be used for [61]:</p> <ul style="list-style-type: none"> * Auditing the strength of a WEP encryption key. 	<p>WEPCrack can be used by attackers to [61]:</p> <ul style="list-style-type: none"> * Discover the network encryption key.
----------------------	---	--	--



Appendix C – Sample Security Solutions

C.1 Security Strategy

A possible strategy for securing wireless network includes:

Risk Assessment

1. Risk Assessment
2. Types of Attacks Assessment

Review and Development

1. Policy Documents
2. Awareness Programs
3. Integrate W/Less Network Security Solution with the overall IT Security Strategy

Monitor and Control

1. Routine Checks
 1. Monitor W/Less Boundaries
 2. Monitor for Rogue APs
2. Incident Reports



Created by : S Diakite

Examples of a security strategy

C.2 Security Awareness Program

Selecting awareness program topics. A significant number of topics can be mentioned and briefly discussed in any awareness session.

Topics may include:

- Wireless network signal overflow
- Wireless rogue access point
- Wireless network boundary issues
- Password usage and management – including creation, frequency of changes, and protection
- Protection from viruses, worms, Trojan horses, and other malicious code – scanning, updating definitions
- Policy – implications of noncompliance
- Unknown e-mail/attachments
- Web usage – allowed versus prohibited; monitoring of user activity
- Spam
- Data backup and storage – centralized or decentralized approach
- Social engineering
- Incident response – contact whom? “What do I do?”
- Shoulder surfing
- Changes in system environment – increases in risks to systems and data (e.g., water, fire, dust or dirt, physical access)
- Inventory and property transfer – identify responsible organization and user responsibilities (e.g., media sanitization)
- Personal use and gain issues – systems at work and home
- Handheld device security issues – address both physical and wireless security issues
- Use of encryption and the transmission of sensitive/confidential information over the Internet – address agency policy, procedures, and technical contact for assistance
- Laptop security while on travel – address both physical and information security issues
- Personally owned systems and software at work – state whether allowed or not (e.g., copyrights)
- Timely application of system patches – part of configuration management
- Software license restriction issues – address when copies are allowed and not allowed
- Supported/allowed software on organization systems – part of configuration management

C.3 Sample Security Policy

Sample Wireless Communication Policy for COMPANY_NAME

1 Overview

The purpose of this policy is to secure and protect the information assets owned by COMPANY_NAME. COMPANY_NAME provides computer devices, networks, and other electronic information systems to meet missions, goals, and initiatives. COMPANY_NAME grants access to these resources as a privilege and must manage them responsibly to maintain the confidentiality, integrity, and availability of all information assets.

This policy specifies the conditions that wireless infrastructure devices must satisfy to connect to COMPANY_NAME network. Only those wireless infrastructure devices that meet the standards specified in this policy or are granted an exception by the Information Security Department are approved for connectivity to a network.

2 Scope

All employees, contractors, consultants, temporary and other workers at COMPANY_NAME, including all personnel affiliated with third parties that maintain a wireless infrastructure device on behalf of COMPANY_NAME must adhere to this policy. This policy applies to all wireless infrastructure devices that connect to a COMPANY_NAME network or reside on a COMPANY_NAME site that provide wireless connectivity to endpoint devices including, but not limited to, laptops, desktops, cellular phones, and personal digital assistants (PDAs). This includes any form of wireless communication device capable of transmitting packet data. The Information Security Department must approve exceptions to this policy in advance.

3 Policy Statement

3.1 General Network Access Requirements

All wireless infrastructure devices that reside at a COMPANY_NAME site and connect to a COMPANY_NAME network, or provide access to information classified as COMPANY_NAME Confidential, COMPANY_NAME Highly Confidential, or

COMPANY_NAME Restricted must:

- 3.1.1 Abide by the standards specified in the Wireless Communication Standard.
- 3.1.2 Be installed, supported, and maintained by a approved support team.
- 3.1.3 Use COMPANY_NAME approved authentication protocols and infrastructure.
- 3.1.4 Use COMPANY_NAME approved encryption protocols.
- 3.1.5 Maintain a hardware address (MAC address) that can be registered and tracked.
- 3.1.6 Not interfere with wireless access deployments maintained by other support organizations.

3.2 Lab and Isolated Wireless Device Requirements

All lab wireless infrastructure devices that provide access to COMPANY_NAME Confidential, COMPANY_NAME Highly Confidential, or COMPANY_NAME Restricted information must adhere to section 3.1. Lab and isolated wireless devices that do not provide general network connectivity to the COMPANY_NAME network must:

- 3.2.1 Be isolated from the corporate network (that is it must not provide any corporate connectivity) and comply with the DMZ Lab Security Policy or the Internal Lab Security Policy.
- 3.2.2 Not interfere with wireless access deployments maintained by other support organizations.

3.3 Home Wireless Device Requirements

- 3.3.1 Wireless infrastructure devices that provide direct access to the COMPANY_NAME corporate network,
must conform to the Home Wireless Device Requirements as detailed in the Wireless Communication Standard.
- 3.3.2 Wireless infrastructure devices that fail to conform to the Home Wireless Device Requirements must be
installed in a manner that prohibits direct access to the COMPANY_NAME corporate network. Access to the
COMPANY_NAME corporate network through this device must use standard remote access authentication.

4 Enforcement

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment. A violation of this policy by

a temporary worker, contractor or vendor may result in the termination of their contract or assignment with COMPANY_NAME.

5 Definitions

Term Definition

COMPANY_NAME network

A wired or wireless network including indoor, outdoor, and alpha networks that provide connectivity to corporate services.

Corporate connectivity

A connection that provides access to a COMPANY_NAME network.

Enterprise Class Teleworker (ECT)

An end-to-end hardware VPN solution for teleworker access to the COMPANY_NAME network.

Information assets

Information that is collected or produced and the underlying hardware, software, services, systems, and technology that is necessary for obtaining, storing, using, and securing that information which is recognized as important and valuable to an organization.

MAC address

The MAC address is a hardware number that uniquely identifies each node on a network and is required for every port or device that connects to the network.

6 Revision History

Date of Change

Responsible

Summary of Change

References

References used for background reading

References used in the document

- [1] - Sebastian H von Solms, Emil Marais - From secure wired network to secure wireless networks (what are extra risks?) - Computers & Security 2004 - RAU-Standard Bank Academy for Information Technology, RAU University, Johannesburg, South Africa**
- [2] - Sebastian H von Solms, Jan HP Eloff - Information Security - 2003 - Rand Afrikaans University**
- [3] - Charles P. Pfleeger - Security in computing 2nd edition - Prentice Hall – 2000 Publication Date: October 2006 Publisher: Prentice Hall ISBN-10: 0132390779 ISBN-13: 9780132390774
- [4] - Charles P. Pfleeger, Shari Lawrence Fleeter - Security in computing 4th edition - Prentice Hall - 2006
- [5] - Albert Dorofee - Managing Information security Risks - Addison-Wesley 2003. The octave approach, New York, USA: Addison-Wesley, 2002.
- [6] - Jan Kill Meyer Tudor - Information Security Architecture - AUERBACH 2001 **Publisher:** Auerbach Publications; 1 edition (2001) **ISBN-10:** 0849399882 **ISBN-13:** 978-0849399886
- [7] - Russell Dean Vines - Wireless Security Essentials - Willey 2002 A Russell Dean Vines 5353 Dundas Street West, 4th Floor, Etobicoke, 2002 John Wiley & Sons, Inc.**
- [8] - Douglas E. Comer - Computer networks And Internet - Prentice-Hall 1999**
- [9] - William A. SHAY - Understanding DATA Communication & Networks - ITP. (2nd Edition). *ITP*. Stallings, *William*. (1999).
- [10] - William D. Sheaf - How to Write a Master's Dissertation in Computer Science - Department of Computer Sciences Florida Institute of Technology Melbourne, Florida 32901 August 21, 2001
- [11] - Mark Camp - CWSP Guide to Wireless Security - Thomson 2007**
- [12] - Ross Anderson - Security Engineering - WILEY 2001
- [13] - Shelly - Cushman - Fermat - Discovering computers - Thomson - 2007**
- [14] - Haag - Cummings - Philips - Management Information System for the Information Age - McGraw-Hill - 2007
- [15] - Terry Callings, Kurt Wall - Red Hat Linux Networking and System Administration - Willey 2005
- [16] - Hue Due, PhD., and Chen Zhang, Ph.D. - Risks and Risks Control of Wife Network systems Volume 4, 2006 Information Systems Control Journal**
- [17] - George Reynolds - Ethics in Information Technology - Thomson 2003**
- [18] - William S. Davis, David C. Yen - The Information System Consultant's Handbook - CRC press 1999
- [19] - <http://www.shop-script.com/glossary.html> Retrieved on 13/04/2008

- [20] - <http://www.webasyst.net/glossary.htm> Retrieved on 13/04/2007
- [21] - <http://largebande.gc.ca/pub/technologies/bbdictionary.html> Retrieved on 13/04/2008
- [22] - <http://www.wlana.org/> Retrieved on 13/04/2008
- [23] - <http://www.google.co.za/search?q=wireless+WAN> Retrieved on 13/04/2008
- [24] - <http://www.bitpipe.com/tlist/Wireless-WAN.html> Retrieved on 13/04/2008
- [25] - <http://compnetworking.about.com/cs/homenetworking/a/homewiredless.htm> Retrieved on 13/04/2008
- [26] - http://www.tcpipguide.com/free/t_NetworkStandardsandStandardsOrganizations.htm Retrieved on 13/04/2008
- [27] - <http://www.microsoft.com/technet/network/wifi/default.mspx> Retrieved on 13/04/2008
- [28] - <http://www.answers.com/topic/packet-switching> Retrieved on 13/04/2008
- [29] - <http://www.answers.com/topic/packet> Retrieved on 13/04/2008
- [30] - <http://www.microsoft.com/technet/network/default.mspx> Retrieved on 13/04/2008
- [31] - <http://www.microsoft.com/technet/network/nap/default.mspx> Retrieved on 13/04/2008
- [32] - <http://www.nist.gov/> Retrieved on 13/04/2008
- [33] - <http://w3.antd.nist.gov/wireadhocnet.shtml> Retrieved on 13/04/2008
- [34] - <http://www.ieee.org/web/publications/journmag/index.html> Retrieved on 13/04/2008
- [35] - <http://www.airdefense.net/> Retrieved on 13/04/2008
- [36] - <http://www.cert.org/stats/> Retrieved on 13/04/2008
- [37] - <http://www.google.co.za/search?q=define%3A+OSI+model> Retrieved on 13/04/2008
- [38] - <http://www.google.co.za/search?q=define%3A+ethernet> Retrieved on 13/04/2008
- [39] - http://nsgn.net/osi_reference_model/ Retrieved on 13/04/2008
- [40] - http://en.wikipedia.org/wiki/Computer_networking Retrieved on 13/04/2008
- [41] - http://en.wikipedia.org/wiki/Information_security Retrieved on 13/04/2008
- [42] - http://en.wikipedia.org/wiki/Advanced_Encryption_Standard Retrieved on 13/04/2008
- [43] - http://en.wikipedia.org/wiki/Risk_Management Retrieved on 13/04/2008
- [44] - http://en.wikipedia.org/wiki/Common_Body_of_Knowledge Retrieved on 13/04/2008
- [45] - http://en.wikipedia.org/wiki/Transmission_Control_Protocol Retrieved on 13/04/2008
- [46] - http://en.wikipedia.org/wiki/TCP/IP_model Retrieved on 13/04/2008
- [47] - <http://en.wikipedia.org/wiki/Networking> Retrieved on 13/04/2008
- [48] - http://en.wikipedia.org/wiki/Network_engineering Retrieved on 13/04/2008
- [49] - http://en.wikipedia.org/wiki/OSI_protocols Retrieved on 13/04/2008
- [50] - http://en.wikipedia.org/wiki/History_of_the_Internet Retrieved on 13/04/2008
- [51] - <http://en.wikipedia.org/wiki/Ethernet> Retrieved on 13/04/2008
- [52] - http://en.wikipedia.org/wiki/Wireless_LAN Retrieved on 13/04/2008
- [53] - http://en.wikipedia.org/wiki/Wide_area_network Retrieved on 13/04/2008
- [54] - http://en.wikipedia.org/wiki/UETS/Universal_Ethernet_Telecommunications_Service
Retrieved on 13/04/2008

- [55] - http://en.wikipedia.org/wiki/Wireless_network Retrieved on 13/04/2008
- [56] - http://en.wikipedia.org/wiki/Peer_to_peer Retrieved on 13/04/2008
- [57] - <http://webmaster.lycos.co.uk/glossary/> Retrieved on 13/04/2008
- [58] - http://en.wikipedia.org/wiki/Wireless_LAN Retrieved on 13/04/2008
- [59] - http://en.wikipedia.org/wiki/Wireless_MAN Retrieved on 13/04/2008
- [60] - <http://www.orafaq.com/glossary/fagglosl.htm> Retrieved on 13/04/2008
- [61] - Thomas M. Thomas. Network Security First-Step Published by Cisco Press. 2004
- [62] - Brad C. Johnson. Wireless 802.11 LAN Security: Understanding the Key Issues
SystemExperts Corporation 2002
- [63] - Matthew Gast, Seven Security Problems of 802.11 Wireless.
<http://www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html> Retrieved on 13/04/2008
- [64] - Air Defense, Three Steps for Bullet-proof Wireless LAN Security & Management 2006
- [65] - Anonymous Article, Overview of wireless threats and risks
- [66] - Robert J. Shimonski, Wireless Attacks Primer, 2004
- [67] - Internet Security Sytems, Wireless LAN Security
- [68] - Top 15 Security/Hacking Tools & Utilities, Darknet spilled these bits on April 17th 2006
- [69] - <http://www.stumbler.net/> Retrieved on 13/04/2008
- [70] - LINUX Manual Pages - command "man nmap"
- [71] - <http://en.wikipedia.org/wiki/Nmap> Retrieved on 13/04/2008
- [72] - <http://www.kismetwireless.net> Retrieved on 13/04/2008
- [73] - <http://airsnort.shmoo.com/> Retrieved on 13/04/2008
- [74] - <http://wepcrack.sourceforge.net/> Retrieved on 13/04/2008
- [75] - <http://www.wirelessve.org/entries/show/WVE-2005-0022> Retrieved on 13/04/2008
- [76] - www.tecrime.com/0gloss.htm Retrieved on 13/04/2008
- [77] - Guide to the implementation and auditing of BS 7799 contraols - business information
- [78] - Guide to BS 7799 Risk Assessment.
- [79] - http://en.wikipedia.org/wiki/Wired_equivalent_Privacy Retrieved on 13/04/2008
- [80] - http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access Retrieved on 13/04/2008
- [81] - <http://en.wikipedia.org/wiki/RADUIS> Retrieved on 13/04/2008
- [82] - http://en.wikipedia.org/wiki/File_sharing Retrieved on 13/04/2008
- [83] - http://en.wikipedia.org/wiki/Beacon_frame Retrieved on 13/04/2008
- [84] - <http://en.wikipedia.org/wiki/SSID> Retrieved on 13/04/2008
- [85] - <http://documentation.netgear.com/reference/sve/wireless/WirelessNetworkingBasics-3-08.html>
Retrieved on 13/04/2007
- [86] - <http://documentation.netgear.com/reference/sve/wireless/WirelessNetworkingBasics-3-09.html>
Retrieved on 13/04/2007
- [87] - http://en.wikipedia.org/wiki/MAC_address Retrieved on 13/04/2008

- [88] – <http://compnetworking.about.com/cs/wirelessproducts/qt/macaddress.htm> Retrieved on 13/04/2008
- [89] - http://en.wikipedia.org/wiki/Cyclic_redundancy_check Retrieved on 13/04/2008
- [90] - http://en.wikipedia.org/wiki/Secure_Shell Retrieved on 13/04/2008
- [91] - <http://en.wikipedia.org/wiki/IPSec> Retrieved on 13/04/2008
- [92] - http://en.wikipedia.org/wiki/Lightweight_Extensible_Authentication_Protocol Retrieved on 13/04/2008
- [93] - http://en.wikipedia.org/wiki/Secure_Sockets_Layer Retrieved on 13/04/2008
- [94] - http://en.wikipedia.org/wiki/Protected_Extensible_Authentication_Protocol Retrieved on 13/04/2008
- [95] - <http://www.us-cert.gov/cas/tips/ST05-003.html> Retrieved on 13/04/2008
- [96] - <http://www.microsoft.com/athome/moredone/wirelesssetup.mspix> Retrieved on 13/04/2008
- [97] - <http://compnetworking.about.com/cs/wirelessproducts/qt/changessid.htm> Retrieved on 13/04/2008
- [98] - **Network Security First-Step By Thomas M. Thomas - Published 2004 Cisco Press**
- [99] - http://books.google.com/books?id=0QV_UbgFXhIC Retrieved on 13/04/2008
- [100]- <http://en.wikipedia.org/wiki/WEP2> Retrieved on 13/04/2008
- [101] - http://en.wikipedia.org/wiki/IEEE_802.11i Retrieved on 13/04/2008
- [102] - **An Analysis of Wireless Systems, Hugh Reeves¹, Saud Al Shamsi², computer Science Department, Duke University December 11, 2003.**