EVALUATING OPTIONS OF WIRELESS LOCAL AREA NETWORK (LAN) SECURITY SOLUTIONS: CASE STUDY OF THE WORLD FOOD PROGRAMME – UGANDA

A Thesis

Presented to the

School of Post Graduate Studies

Kampala International University

In Partial Fulfilment

Of the Requirements for the Degree

MASTER OF SCIENCE IN COMPUTER SCIENCE

By:

AMONGI MARY, MSC

MSC-2004-PT-024

July 2006

DECLARATION

I **AMONGI Mary** do hereby declare that this thesis is my original work and that it has never been submitted to any academic institution for award of a degree or the equivalent.

Signature..... Date 1/11/2006

On this 17th day of October of the year 2006, at Kampala International University

This thesis has been submitted for examination and acceptance with my approval as the supervisor.

Mr. Bada Joseph Kizito
School of Computer Studies
Kampala International University

Signature..... Date 1/11/2006

DEDICATION

To my entire family especially, Robert & my Mother, the two closest people to me!

ACKNOWLEDGMENTS

First, I would like to thank God for giving me health, allowing me to reach this stage in my life, and taking me this far in my career. Second, I would like to thank my family, especially my husband for being so caring, supportive, understanding and connecting me to the people in the organization who were key to my data collection exercise. I thank all the staff of World Food Programme, especially the Information & Communication Technology (ICT) unit.

In addition, I would like to thank my mother, all my brothers and sisters, for being good listeners and good friends and my uncle Mr. David Obot, for being so strong and persistent squeezing time to correct my grammar. I would also like to thank all friends especially Wilson, for being there for me, encouraging me to do my best, being a great friend, and for supporting me all through the project duration.

I would like to give special thanks to my supervisor, Mr. Bada Joseph Kizito, for giving me the opportunity to work with him in this project, for being so supportive, and for spending so much time helping me with the development process of this project. I would like to express gratitude to Mr. Alex Mbaziira, for encouraging me to do better each time and for believing in me, giving me time off to carry out my research. I would also like to express gratitude to Mr. Kwezi R, for being the influential point for my interest in wireless networks and wireless network security. Finally, to everyone else that has helped in the development of this project, either directly or indirectly, I am thankful.

ACRONYMS

WLAN	-	Wireless Local Area Network
IEEE	-	Institute of Electrical and Electronic Engineering
WEP	-	Wired Equivalent Privacy,
WPA	-	Wi-Fi Protected Access,
EAP	-	Extensible Authentication Protocol,
TLS	-	Transport Layer Security,
VPN	-	Virtual Private Network
TKIP	-	Temporal Key Integrity Protocol,
LEAP	-	Lightweight Extensible Authentication Protocol
PEAP	-	Protected Extensible Authentication Protocol,
I.T	-	Information Technology
3G	-	Third Generation
4G	-	Fourth Generation
Wi-Fi	-	Wireless Fidelity
wWANs	-	Wireless Wide Area Networks
WFP	-	World Food Programme
PDA	-	Personal Digital Assistant
AP	-	Access Point
WISPs	-	wireless Internet service providers
MAC	-	Media Access Control
OTP	-	One Time Password

TABLE OF CONTENT

Chapter 2: LITERATURE REVIEW

Chapter 3: RESEARCH METHODOLOGY

LIST OF FIGURES

ABSTRACT

This project focuses on wireless network security and in particular it evaluates the security solutions being used by the case study organization, with its major focus on assessing the level of wireless local area network security awareness and procedures of WLAN use. It explores the possible methods of securing IEEE 802.11 based Wireless LANs.

The project frames the WLAN implementation within the context of the overall WLAN security design for organizations. The design solution represents a policy-based approach to security. This type of approach focuses on overall design goals and translates those goals into specific configurations, policy enforcement, procedures for WLAN use and guidelines for management to use when selecting a suitable WLAN security solution. In the context of wireless, it is recommended that organizations should also consider network design elements such as strong policy framework, mobility and quality of service (QoS) when deciding on an overall WLAN design.

This report contains five chapters. Chapter 1 begins with a general Introduction of the project, stating its objectives and scope among other things, and then chapter 2, details the specific WLAN security technologies in the literature review. Chapter 3 explains the methodology used during the study. The findings from the study and results analysis are explained in chapter 4. Finally, chapter 5 then concludes the report with recommendations and future study.

Chapter 1: GENERAL INTRODUCTION

1.0 INTRODUCTION

Evaluation deals with a systematic determination of: merit, worth, and significance of something or someone. It is often used to characterize and appraise subjects of interest in a wide range of human enterprises. Any evaluation tends to look at both qualitative methods and quantitative methods, including case studies, survey research, statistical analysis, and model building among others (Webopedia,2006).

Wireless Local Area Network (WLAN) use electromagnetic waves to communicate from one point to another without relying on a physical connection. Wireless local area networks (WLANs) transmit and receive data over the air, combining data connectivity and user mobility. Erten (2004) argues that it creates greater employee productivity. At the same time, they facilitate remote access to corporate network resources and data transmission to users by using the open air instead of wires, thus making networks more appealing to conventional users (The IEEE Computer Society, 2004). As these functions are performed by the WLAN user, security of information is fundamental.

Security of information may be applied by any given organization by selecting from a variety of options. Depending on security needs, organizations often discover that developing a strong, cost-effective network and information security can be a challenging task.

Known Wireless LAN security solutions include: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Extensible Authentication Protocol (EAP), Transport Layer Security (TLS), Virtual Private Network (VPN), Temporal Key Integrity Protocol (TKIP), Protected Extensible Authentication Protocol (PEAP), Cisco Aironet and security standard for Institute of Electrical and Electronic Engineering (IEEE) 802.11 wireless LANs Known as 802.11i, to mention but a few

1.1 BACKGROUND TO THE STUDY

Compared to personal computers (PCs) in the 1980s and the Internet in the 1990s, wireless local-area networks (WLANs) are proving to be the next major evolution of technology for many organizations (Dave, 2004). In addition, just as organizations are forced to adopt and provide necessary security to keep up with the users of the preceding technologies, WLANs introduce new security concerns while offering similar productivity-boosting opportunities (Arbaugh, 2003). However, the benefits far outweigh the risks when appropriate actions are taken to minimize those risks.

The adoption of personal computers in the 1980s led to the creation of local-area networks that laid the initial roads to allow communication to flow. In the 1990s, the Internet enhanced connectivity among users. Progressively, wireless LAN is introducing the concept of complete connectivity regardless of the infrastructure of wires. The rapid adoption of Wireless Local Area Network (WLAN) technologies, in conjunction with the steady development of cellular technologies, promises to provide high throughput to the user as well as ubiquitous coverage (Carl, 2003). This provides new opportunities and challenges (AirDefense, 2005).

Data privacy is the most common concern with any wireless technology. One of the numerous security concerns when deploying a wireless LAN is clearly a need to protect data from unauthorized interception over the air (Gupta and Gupta, 2001).

It is sometimes perceived that some of the challenges which threaten the introduction of new services on future wireless networks are possibly the lack of thorough and well-defined security solutions that meet the challenges posed by wireless networks (Potter, 2003). It is argued that an integrated approach to security development, which considers both network and application specific issues, is critical to facilitating the ultimate deployment of a secure, pervasive computing infrastructure. In particular, security algorithms and protocols designed

for wireless computing must consider the resource limitations of network nodes, the mobility of network nodes, and the underlying inter-working of wireless networks (Altunbasak and Owen, 2004).

Further, since most wireless devices usually function in open environments, these networks quite often face natural and malicious threats. Therefore, wireless networks must be able to adapt and heal themselves in the presence of active and passive threats. Furthermore, with the proliferation of an underlying communication infrastructure comes increased sharing of digital content, necessitating the development of solutions that enforce digital rights management policies (Feil, 2003).

WLANs have gained popularity over recent years. The popularity is because they are easy to deploy and provide ubiquitous access to organizational resources from anywhere or where access is possible. Lidong and Haas (1999) observed that a surprising number of organizations do not bother to activate wireless security features. For example, *The Wall Street Journal,* April 27, 2001, described two hackers with a laptop and a boom antenna driving around Silicon Valley listening to network after network. The best 'pickups' were outside Fortune 500 enterprises that, according to the hackers, "should know better".

Awareness of the security and management implications of adding wireless technologies to organization's network is important. David Halasz, manager of software development in the Wireless Networking Business Unit at Cisco and chair of the Institute of Electrical and Electronic Engineering (IEEE) security task group, observed, "You can be outside a building or be near an employee's house and still be part of the network". The Institute of Electrical and Electronic Engineering developed a standard for wireless network code named 802.11. Robust wireless security implementations with hassle-free management are mandatory for successful integration of wireless into an enterprise framework" (David Halasz, et

al, 2006). However, even if an organization does activate WLAN security based on the 802.11 standard, that does not mean airwaves are secure, according to a study by researchers at the University of California, Berkeley (Berkeley, 2002).

The researchers' report exposed the vulnerabilities of the static Wired Equivalent Privacy (WEP) standard (Walker, 2000). The report raised questions as to why it was adopted. Arbaugh (2002) observed that, if WEP had been examined by the cryptographic community before it was enacted into an international standard, the flaws would have been eliminated. Widespread perception in the networking community was that the only way to secure a WLAN was to use virtual private network (VPN) technologies at additional expense and management. The University of California Berkeley report (2002) had reservations about any commercial system that had mechanisms to support techniques that effectively defended against attacks via wireless connections. Otherwise the report identified many organizations using security based on IEEE 802.1x draft standard for the 802.11 framework, Cisco Aironet WLAN security provides dynamic, per-user, per session WEP that mitigates many of the concerns identified by the study, and increases the overall 802.11 WEP encryption robustness.

In the quest to provide trusted computing and communication for the broad variety of current and future wireless networks various researches were undertaken. For example, WINLAB initiated several security-related research initiatives over the years: Candolin and Kari, (2002), "The Analysis and Development of Resource-Efficient Authentication and Key Pre-Distribution Schemes for Hierarchical Ad Hoc Networks", in, *Authentication in Hierarchical Ad Hoc Networks;* Lee, et al, (2003), "Protocol Development for Ad Hoc Networks Capable of Repairing Themselves in the Presence of Faults and Adversarial Attacks", in, *Self-Healing Ad Hoc Networks;* Lidong, et al, (1999), "The Evaluation of Current Multicast Security Solutions for the 3G Network, and the Development of Improved Group Key Management and Authentication Protocols for Cellular Networks", in, *Multicast Security for Third*

Generation (3G) Wireless Networks; Chlamtac, et al, (2003), "Authentication and Provably Secure Protocols During Mobile Node Migration Across Coexisting Wireless Networks With Varying Security Policies", in, *Secure Inter-working in fourth Generation (4G);* and Nichols, et al, (2002), Robust Statistical Methods Suitable for Localizing Wireless Devices in the Presence of Malicious Adversaries", in, *Secure Localization and Location-Based Security.*

Otherwise, the early development of WLAN security, much of the focus has been on encryption, authentication, and wireless VPNs. While these are a good start to securing a WLAN, they do not provide a comprehensive solution. The reasons are that they do not assess network vulnerabilities or discover rogue Access Points and ad hoc networks (Lee, et al, 2003); cannot protect the WLAN from intruders and attacks; and have limitations in enforcing WLAN security policies.

In addition, a few WLAN security tools, such as sniffers and scanners, have been introduced to secure WLANs. However, sniffers cannot detect rogue Access Points and require expert 802.11 security analysts to read the data and understand the threats detected (Housley and Arbaugh, 2003). Scanners can identify unauthorized networks, but they offer very limited security because they only scan samples and stationary snapshots of the airwaves. They cannot continuously monitor a WLAN for new threats, wireless attacks, and network abuses.

1.2 THE WORLD FOOD PROGRAMME

1.2.1 History of The World Food Programme (WFP): The First 41 Years

Scheduled to go into operation in 1963 as a three-year experimental program, WFP was up and running before it could walk. (Wfp, 2006)

An earthquake hit Iran in September 1962, followed by a hurricane in Thailand in October. Newly independent Algeria was resettling 5 million refugees. Food aid was urgently needed and WFP supplied it. It has never stopped.

WFP's Mission:

As the food aid arm of the UN, WFP uses its food to:

- meet emergency needs
- support economic & social development

The Agency also provides the logistics support necessary to get food aid to the right people at the right time and in the right place.

WFP works to put hunger at the centre of the international agenda, promoting policies, strategies and operations that directly benefit the poor and hungry.

WFP helps the following categories of people

- Victims of natural disasters
- Displaced People
- The world's hungry poor

WFP's areas of operation

- WFP is the world's largest international food aid mobilization combating hunger in **underdeveloped nations with severe food shortages**. The frontline stretches from sub-Saharan Africa and the Middle East to Latin America and Asia & the Pacific.

- These are places where cabling communication network would be near to impossible if it has to serve its purpose within the shortest time needed. WLANs come in as the most preferred solution in most of these operations.

Methods used by WFP to fight hunger

- Rescue
- Rapid Reaction
- Rehabilitation
- Deterrence

1.2.2 World Food Programme in Uganda

Despite Uganda's fertile soil and favourable climate, five percent of rural households continue to experience food insecurity. This developing country registered increased literacy and life expectancy rates and a reduction in the number of people living in absolute poverty from 56 percent in 1992 to 38 percent in 2004. However, it ranked 144th out of 177 countries in the UNDP Human Development Index for 2005 (UNDP,2005).

WFP Activities

World Food Programme supports the National Food Strategy through its Protracted Relief Recovery Operation 10121.1, which targets drought-affected people, refugees and nearly 1.5 million internally displaced people living in cramped camps to the north of the country. The program, which runs until 2008, also assists displaced people when they return to their farms.

The relief program aims to provide life-saving assistance to the most vulnerable. The recovery and country programs enable vulnerable people to secure food and income by themselves and eventually break out of the poverty trap and build their own sustainable livelihoods. In 2006, WFP plans to reach over 2.7 million people

under the relief and recovery operation and more than 236,000 people under the country program.

1.2.3 WLAN Use by WFP

Out of the 14 WFP sub offices, Tororo and Moroto use WLAN entirely to achieve the organization's goals in their respective regions. The nature of the organization's activities makes Wireless LANs the most convenient network option to implement. Based on the area and nature of organizational operations, and the major advantages of wireless LANs, WFP decided to deploy WLANs in their offices where their operations are anticipated to be temporal, thus the need for a wired network does not seem feasible.

These WFP WLANs are connected to the Internet. Such connections expose the system to risks of attacks from both Internet users and internal authorized LAN users. Risks of attacks usually arise from abuse of rights to access to information critical to the organization's operations.

1.3 PROBLEM STATEMENT

Wireless networks enable organizations to provide employees with the flexibility to work remotely and access critical information, increasing productivity, communication and motivation. However, some of the biggest risks for organizations implementing wireless technology are the improper use of the facility, insufficient policies, procedures to protect the WLAN from; denial-of-service attacks, eaves dropping, encryption and authentication related problems, in some cases placement of rogue, or unauthorized, wireless access points.

The market is flooded with many security solutions to address these WLAN risks. However, even when the organization implements any of these solutions, there is still need for wireless network devices to be securely configured and maintained through properly defined policies and implementation procedures, to protect corporate data and critical organization information.

1.4 OBJECTIVES

This study was guided by general and specific objectives.

1.4.1 General Objectives

The general objective of this research was to evaluate options of Wireless Local Area Network Security options in the World Food Programme in Uganda.

1.4.2 Specific Objectives

The specific objectives were to:

1. Assess organizational awareness of WLAN security and their options
2. Assess the organizational policy of deploying WLAN
3. Assess the organizational procedure for use of WLAN.
4. Assess management guidelines for selection of WLAN security solutions
5. Identify suitable & practical WLAN security configuration solutions that can be effectively used by organizations.

6. Evaluate the security of the wireless local area network and applications including threats to data integrity, confidentiality and availability of services and resources
7. Design and implement a WLAN; which will be used to carryout investigation & assessment procedures on the various security options identified by the researchers.

1.5 SCOPE

There are several Wireless LAN security challenges that face organisations, with several standard based and proprietary security solutions to address these challenges. However, this project sought to evaluate solutions that were currently being used by the case study organization, in a windows (Microsoft) network infrastructure and applications environment as opposed to Linux environment. Hence the evaluation software tools used are those supported by windows environment. Amidst the wireless technologies in the market, the focus of the study is WLAN based on IEEE 802.11standard.

Geographical scope

The research focus was therefore to assess, evaluate and design options for WLAN security solutions with more emphasis on strengthening encryption, authentication and intrusion detection; documenting best practice to reduce losses at organisational level; using World Food Programme Uganda, specifically its sub-office WLAN in Tororo as a case study.

Target respondent

The cross section of the study involved both system administrators and system users of the WLAN system. The total number of respondents was 22 users and 5 system administrators.

1.6 SIGNIFICANCE OF THE STUDY

This study is important to three groups of persons: -

- The Organization
- Academicians
- Software Developers

Wireless networking adoption is exploding. With the proliferation of wireless technology and the increasingly distributed nature of organizations with partners, vendors and extranets, security has never been more crucial to the success of a business or an organization's operations as it is in recent years. Many analysts believe that within a few years, all computers will include wireless technology at the factory.

However, the removal of wires from the communications and network access equation has obvious limitations & benefits. Some of the limitations associated with WLANs are seen in the problem statement of this project (section 1.3.1).

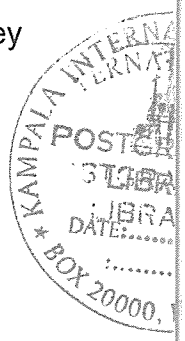
1.6.1 The Organization

The most common reason for deploying a wireless network in the organization is increased employee productivity. In addition to information sharing, numerous new applications are enabled with wireless networks, such as on-line mobile patient/customer records, real-time inventory management, and public internet hotspots.

The study provides the organization with a clear understanding of the current risks due to improper configurations, unauthorized access points, and to appreciate the fact that clear security policies and procedure are important.

This study also recommends configuration changes and other steps that can be taken to improve the organization's wireless network security.

It also enables the organization to address security issues proactively before they are exploited. The following are some of the benefits that the study will offer:



- A clear understanding of current wireless network and information security risks
- Identification of vulnerabilities on the organization's network infrastructure
- More informed decision-making and raised internal awareness of wireless network and information security risks
- Identification of the gaps in organizational security controls, policies and processes
- A specific, actionable plan to improve overall security posture based on organizational goals and needs
- Advanced notice of security issues before they are exploited
- Compliance with national and international regulations that require security risk assessments

For employees who travel regularly, secure wireless access is a tool that represents significant productivity enhancement. The ability to access network resources easily and safely at a hotel, a coffee shop, an airport lounge or the local office means less idle time while waiting to dial in or search out a broadband connection (Henning, 2003).

Secure wireless LAN access can also generate significant operational cost savings by greatly reducing or eliminating the I.T administrative burden associated with employee Moves/Adds/Changes. It is widely accepted that the cost of deploying a LAN at a new office, for example, can be greatly reduced with Wireless Fidelity (WiFi) technology compared to the cost of a purely Ethernet infrastructure. In environments where floor plans may change frequently, such as retail stores, the savings are even greater. Wireless LANs ease network deployment at new facilities since cables do not need to be run, a costly and time consuming task.

Wireless LAN mobility allows employees to carry their net-connected laptops to conference rooms and peers' offices, resulting in decisions being made quicker and based on data that are more accurate. Furthermore, with the increasing number of Personal Digital Assistant (PDAs) and mobile phones incorporating Wireless Fidelity (WiFi) technology, demand for a wireless infrastructure will continue to increase. However, wireless networking deployment can be a challenge when faced with the realities of security. A wireless network with weak security and improper device configurations can compromise an entire organization's security posture and create more problems than it solves, hence the importance of this research.

1.6.2 Academicians

Initiation of Future research projects; based on the findings of this study for the benefit of those scholars who would like to contribute to the fast growing wireless technologies.

1.6.3 Software Developers

Adjustments on future security software development projects, with keen emphasis on product architecture which takes into account the various attacks mentioned in the problem statement of this project.

1.7 Research Questions

The research project will seek to answer a number of questions related to the problem of how to best plan and secure WLAN in a large organization. These include: -

1. What is the WFP user awareness level of WLAN security solutions and options?
2. What is the WFP WLAN security solution policy?
3. What is the WFP WLAN security solutions user procedure?
4. What is the WFP WLAN security solution selection management guideline?
5. What are the limitations of some of the WLAN security technologies used by WFP?
6. What are the wireless WLAN security configuration solutions used by the organization?
7. Which WLAN applications, services and resources protect data integrity and confidentiality?

Chapter 2: LITERATURE REVIEW

2.1 INTRODUCTION

This chapter discusses the review of literature concerning wireless local area network security, as researched by several scholars prior to this study.

Section 2.2, clarifies the definitions used in this report, in order to get all readers familiar with the technological terms contained herein.

Section 2.3, contains details of network types in existence, in relation to wireless network security which is the point of focus. Its subsequent subsections, further describes the different standards based wireless technologies in use.

2.2 Clarity of Definitions

In this section, a number of definitions will be clarified purposely to cater for the readers who may not be very familiar with the many technological terms that are used in this report.

The definitions are presented according to different authors' perspective with the intention of bringing out the different perspectives that may explain the particular phrases used.

2.2.1 Computer network

A **computer network** is a group of two or more computers connected to each other. Some basic types of computer networks include:

- A local area network connects two or more computers in a house or an office
- A corporate network enables communication among various offices of the same organization
- An "internet" connects two or more smaller networks together. The largest one is called the Internet.

These network types are not mutually exclusive. (Tanenbaum, 2003). The *local area network* in a department store is usually connected to the *corporate network* of the parent company, and may have privileges with the corporate network of a bank. Any connected machine at any level of the organization may be able to access the *Internet*, through a web server.
(http://simple.wikipedia.org/wiki/Computer_network)

Key Terms:

- A ***threat*** is a potential violation of security. In other words, it is a possible danger that might exploit a vulnerability of the system (Stallings, 2003).
- An ***attack*** is an actual violation of security. In other words, it is a deliberate attempt to evade security services and to violate the security policy of a system (Stallings, 2003).
- **Encryption**; is about transforming data so that only authorized parties can decode it. The encryption process combines some plaintext with a digital key to produce Cipher text. Decryption reverses the process by taking the Cipher text and combining it with the key to reproduce the original plaintext (Arbaugh, 2002).
- **Authentication**; is about proving or disproving someone's or something's claimed identity. Traditionally authentication is a one-way process, for example a user logs onto a computer and proves their identity with a username and password. In wireless networking mutual authentication should be employed where the network authenticates the client and the client authenticates the network. This prevents unauthorized devices from masquerading as network equipment to gain access to sensitive identification data on the wireless client (Arbaugh, 2002).

2.2.2 Access point

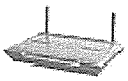


Figure. 2.1 Wireless device - A basic Digital Subscriber Line (DSL) gateway/router

Access points are two-way transceivers that broadcast data into the surrounding environment. Access points act as a mediator between wired and wireless network.

2.3 Types of Computer Network architecture

A group of two or more computer systems linked together. There are many types of computer networks, including: (Webopedia, 2006).

- **Local-area networks (LANs)**: The computers are geographically close together (that is, in the same building).
- **Wide-area networks (WANs)**: The computers are farther apart and are connected by telephone lines or radio waves.
- **Campus-area networks (CANs):** The computers are within a limited geographic area, such as a campus or military base.
- **metropolitan-area networks MANs):** A data network designed for a town or city.
- **Home-area networks (HANs):** A network contained within a user's home that connects a person's digital devices (Tanenbaum, 2003).

In addition to these types, the following characteristics are also used to categorize different types of networks:

- **Topology**: The geometric arrangement of a computer system. Common topologies include a bus, star, and ring.
- **Protocol**: The protocol defines a common set of rules and signals that computers on the network use to communicate. One of the most popular

but otherwise this isn't worth the cost. Watching a DVD while someone else browses the Internet through the network doesn't require 1,000 Mbps of speed.

2.4 WIRELESS LAN

The following sections describe the relevant protocols and techniques used in this Master's Thesis. At first an overview of the standard IEEE 802.11 will be given. Then the principles of WLAN technologies including authentication, encryption and wireless sensor devices used in the security design will be explained briefly.

Overview of IEEE 802.11

The standard IEEE 802.11, (IEEE, 1999), specifies the Media Access Control (MAC) and the physical layer in the Internet protocol stack, Figure 2.2, for wireless connectivity.

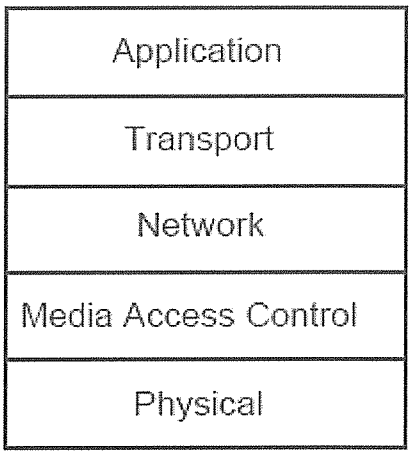


Figure 2.2: The Internet protocol stack

The Need for Wireless

Standard 802.11-based wireless LANs (WLANs) provide mobility to network users while maintaining the requisite connectivity to corporate resources. As laptops become more pervasive in the workplace, users are more prone to use laptops as their primary computing device, allowing greater portability in meetings and

conferences and during business travel. WLANs offer organizations greater productivity per employee by providing constant connectivity to traditional networks in venues where previously unavailable (IEC, 2005).

Wireless network connectivity is not limited to enterprise use. WLANs offer increased productivity not only before and after meetings, but also outside the traditional office environment. Numerous wireless Internet service providers (WISPs) are appearing in airports, coffee shops, hotels, and conference and convention centers, enabling enterprise users to connect in public access venues.

2.4.1 Types of Wireless Technology

Wireless local-area networking has existed for many years, providing connectivity to wired infrastructures where mobility was a requirement to specific working environments. These early networks were based on both frequency-hopping and direct-sequencing radio technologies (described later). These early wireless networks were nonstandard implementations, with speeds ranging between 1 and 2 MB. Without any standards driving WLAN technologies, the early implementations of WLAN were relegated to vendor-specific implementation, with no provision for interoperability, inhibiting the growth of standards-based WLAN technologies. Today, several standards exist for WLAN applications: 802.11, HiperLAN, HomeRF SWAP, and Bluetooth (IEC, 2005).

2.4.2 Functional View

Considering a functional viewpoint, WLANs can be categorized as follows: peer-to-peer wireless LANs, multiple-cell wireless LANs, and building-to-building wireless networks (point to point and point to multipoint). In a peer-to-peer wireless LAN, wireless clients equipped with wireless network interface cards (NICs) communicate with each other without the use of an access point. Coverage area is limited in a peer-to-peer LAN, and wireless clients do not have access to wired resources. A multiple-cell wireless LAN extends the coverage through the use of

overlapping cells. Coverage area of a cell is determined by the characteristics of the access point (a wireless bridge) that coordinates the wireless clients' use of wired resources (IDC, 2005).

Building-to-building wireless networks address the connectivity requirement between LANs (buildings) in a campus-area network. There are two different types of building-to-building wireless networks: point to point and point to multipoint. Point-to-point wireless links between buildings are radio- or laser-based point-to-point links. A radio-based point-to-point bridged link between buildings uses directional antennas to focus the signal power in a narrow beam, maximizing the transmission distance. A laser-based point-to-point bridged link between buildings uses laser light (usually infrared light) as a carrier for data transmission. A radio-based point-to-multipoint bridged network uses antennas with wide beam width to connect multiple buildings (LANs) in a campus-area network (IEC, 2005).

2.4.3 Technology View

Though most of this study focuses on 802.11 WLANs (described below), it is relevant to understand other wireless standards currently in the market (described later in this section).

2.4.4 802.11 Wireless Technology

The IEEE maintains the 802.11-based standard, as well as other 802-based networking standards, such as 802.3 Ethernet (see Section 2.3.1). A nonprofit, vendor-neutral organization known as the Wi-Fi Alliance provides a branding for 802.11-based technology known as Wi-Fi (Wireless Fidelity). A Wi-Fi compliant device must pass interoperability testing in the Wi-Fi laboratory. All vendor products that are Wi-Fi certified are guaranteed to work with all other Wi-Fi certified products—regardless of the vendor (IDC, 2005).

Standard 802.11-based wireless technologies take advantage of the radio spectrum deemed usable by the public. This spectrum is known as the Industrial, Scientific, and Medical (ISM) band. The 802.11 standard specifically takes advantage of two of the three frequency bands, the 2.4 GHz-to-2.4835 GHz UHF band used for 802.11 and 802.11b networks, and the 5.15 GHz-to-5.825 GHz SHF band used for 802.11a-based networks (IDC, 2005).

The spectrum is classed as unlicensed, meaning there is no one owner of the spectrum, and anyone can use it as long as that user's device complies with FCC regulations. Some of the areas the FCC governs include the maximum transmit power of the radios and the type of encoding and frequency modulations that can be used.

2.4.5 Wireless LAN Radio Frequency Methods

The 2.4-GHz ISM band (used by 802.11b) makes use of spread-spectrum technology. Spread spectrum dictates that data transmissions are spread across numerous frequencies. The reason for this is that the 2.4-GHz band has other primary owners. Primary owners are entities who have bought the spectrum for their own use, or have been granted legal access to the spectrum above all else. Common primary owners of the 2.4-GHz band include microwave oven manufacturers. Microwave ovens transmit in the same frequency range, but at far greater power levels (a typical 802.11 network card operates at 100 mW, whereas a microwave oven operates at 600W). With spread-spectrum technology, if there is ever any overlap with the primary owner, the primary owner has what can effectively be called "radio frequency (RF) right of way" (Ray, et al, 2005).

The 802.11 standard specifies two different types of Layer 1 physical interfaces for radio-based devices. One uses a frequency-hopping architecture, whereas the other uses a more straightforward single-frequency approach, known as direct sequencing.

Frequency Hopping

The 2.4-GHz ISM band provides for 83.5 MHz of available frequency spectrum. The frequency-hopping architecture makes use of the available frequency range by creating hopping patterns to transmit on one of 79 1-MHz-wide frequencies for no more than 0.4 seconds at a time. This setup allows for an interference-tolerant network. If any one channel stumbles across interference, it would be for only a small time slice because the frequency-hopping radio quickly hops through the band and retransmits data on another frequency (IEC, 2005).

The major drawback to frequency hopping is that the maximum data rate achievable is 2 Mbps. Although one can place frequency-hopping access points on 79 different hop sets, mitigating the possibility for interference and allowing greater aggregated throughput, scalability of frequency-hopping technologies becomes a deployment issue. Work is being done on wide-band frequency hopping, but this concept is not currently standardized with the IEEE. Wide-band frequency hopping promises data rates as high as 10 Mbps (IEC, 2005).

Direct Sequencing and 802.11b

Direct-sequencing networks take a different approach to data transmission. Direct sequencing provides 11 overlapping channels of 83 MHz within the 2.4-GHz spectrum. Within the 11 overlapping channels, there are 3 22-MHz-wide non-overlapping channels. The large bandwidth along with advanced modulation based on complementary code keying (CCK) provided by direct sequencing is the primary reason why direct sequencing can support higher data rates than frequency hopping. Additionally, because the three channels do not overlap, three access points can be used simultaneously to provide an aggregate data rate of the combination of the three available channels. In 1999, the IEEE ratified the 802.11b standard, which provided newer, enhanced modulation types to allow direct-sequencing networks to achieve data rates as high as 11 Mbps, or 33 Mbps when the three non-overlapping channels are used together. Direct sequencing does

have one disadvantage compared to frequency hopping: interference intolerance. Though both are affected by interference, throughput in a direct-sequencing network falls dramatically when interference is introduced (Ray, et al, 2005).

2.4.6 IEEE 802.11b

This technology is the old reliable for wireless home networking. It's the technology many people mean when they say "wireless" or "Wi-Fi." Do be careful not to confuse Wi-Fi with the newer FireWire; they're different things. For the record, Bluetooth technology is also wireless, but if you hear people say "I run wireless at home," chances are they mean some variant of 802.11 wireless standards. An 802.11 technology is usually easier to install than an Ethernet network, but configuring the equipment can take a little longer (Ray, et al, 2005).

Usually, the promised 11 Mbps speed ends up in the 2.5-4 Mbps range. That's still generally faster than a broadband connection, but may be slow for watching DVDs from another room. Securing an 802.11b network usually slows it down a little as well, but it does the job for sharing printers and Internet connections, and transferring files doesn't take all day. People who bring a laptop home from work often use 802.11b (IDC, 2005).

It's worth noting that 802.11b operates on the 2.4 gigahertz (GHz) frequency, which causes interference with many cordless phones that use the same frequency. Switching to a 900 megahertz (MHz) cordless phone generally solves this problem.

2.4.7 IEEE 802.11a

802.11a is a technology upgrade to 802.11b, but you can't run both of them on the same network. If you enjoyed running an 802.11b network and want to replace it with 802.11a, you'll be an old pro with the new equipment, since they're similar in some ways. 802.11a operates at 5 GHz, so cordless phone interference should not be an issue. And the real clincher for most people; 54 Mbps throughput—five times the data speed that 802.11b delivers (Hao, et al, 2004).

A good rule of thumb with "latest and greatest" high-speed technology of **any** kind is that you should only spend the money for new gadgets if you've already maxed out the potential power of the old stuff. In general, technology comes down in price with time, so don't buy more than you need. If you're setting up your very first network and want to buy wireless, 802.11b is still worth considering. But if you have five power users on your network, take a good look at 802.11a.

2.4.8 IEEE 802.11g

The "a," "b," and "g" designations on wireless networks are not in a helpful order in terms of performance. The first was "b," "a" is fastest, and "g" splits the difference. 802.11g moves data at 54 Mbps, which is significantly faster than 802.11b. Both 802.11g and 802.11b run on the 2.4 GHz frequency (Hao, et al, 2004).

The speed gains and compatibility between "b" and "g" bring up an interesting point. In most 802.11 networks, data moves through a hardware device called an **access point** (also called a **hub**, a **router**, or a **base station**). There are several types of access points. If both 802.11b and 802.11g equipment are used in a network, the access point has to be 802.11g for the network to use all the speed that 802.11g allows. The access point is the conduit between computers, so make sure it's as fast as the fastest computer on your network, if you want the speed. So don't spend the money to upgrade one of your computers without upgrading the access point, too.

Technology	Speed	Wireless	Cost
Ethernet 10/100	100Mbps	No	Low
Gigabit Ethernet	1,000 Mbps	No	Very high
802.11b	11 Mbps	Yes	Low
802.11a	54 Mbps	Yes	High
802.11g	54 Mbps	Yes	Medium

Table 2.1: Network types, speed and cost variations

802.11e, 802.11h and 802.11i

802.11e focuses on establishing Quality of Service (QoS). 802.11h focuses on power usage and transmission interference from 802.11 radio frequencies. Finally, 802.11i is known as the data security protocol (IEEE P802.11 Task Group I, 2004). It considers two encryption algorithms, Temporal Key Integrity Protocol (TKIP) for backward compatibility with WEP and Advanced Encryption Standard (AES) to provide a stronger encryption than WEP (Hao, et al, 2004).

As time goes by, more IEEE 802.11 standards will keep emerging, as well as updates to the ones that are available at this time. In addition, new security solutions and encryption algorithms are being proposed for use with the wireless networks (Jamil, 2004). At the same time, new attacks and threats will have to be taken into account and new security solutions for these will have to be developed (Hao, et al, 2004).

2.4.9 Other Wireless Technology

Some other technologies, old and new, hover around the edges of the home network market. These aren't necessarily technologies that can be recommended for use as the backbone of a home or small office network. But in many ways they're related, and they're often on the shelf next to networking hardware in many computer stores. And, since many people still use them in their personal networks, it's necessary to mention them here.

HiperLAN

HiperLAN is a European Telecommunications Standards Institute (ETSI) standard ratified in 1996. HiperLAN/1 standard operates in the 5-GHz radio band up to 24 Mbps. The ETSI has recently approved HiperLAN/2, which operates in the 5-GHz band at up to 54 Mbps using a connection-oriented protocol for sharing access among end-user devices.

Bluetooth wireless technology

Bluetooth is a personal-area network (PAN) specified by the Bluetooth Special Interest Group for providing low-power and short-range wireless connectivity using frequency-hopping spread spectrum in the 2.4-GHz frequency environment.

Bluetooth wireless technology is slow but in many ways is the most intriguing networking technology. Printers, mice, joysticks, keyboards, personal digital assistants (PDAs), cell phones, digital cameras—anywhere data goes, chances are someone makes a Bluetooth wireless device to move it. At about 1.5 Mbps, it's not really a viable network technology, but it isn't designed to network computers together. Its main function is to connect computers to smaller devices. The range is about 30 feet. For very specific connections between very modern devices, Bluetooth wireless technology is fast gaining in popularity. We won't discuss it in any of the installing or configuring sections here, since it's not often used as the backbone of a network, but Bluetooth wireless technology has many practical uses for home and office.

2.5 Cost Comparison

For the budget conscious, Ethernet technology usually wins. Some people will move computers into a single room to avoid the wiring hassle, but even for small networks that isn't always practical. An Ethernet network should normally cost under $100 per computer, and less if your computers already have network cards (many do). Additional Ethernet hardware should generally total less than $100. On the other end of the cost spectrum, many new buildings and houses come with internal Ethernet wiring, and it's not hard to find stories online from people who incorporate networking into a remodel.

Wireless equipment will probably cost about $100 per computer, in addition to the cost of hardware, which is typically under $100. If a wireless network adapter is already installed in each computer, the cost of the network hardware—called an **access point** (See Figure.2.1)—will be most of the cost, if not all.

Unless there is an Ethernet network with only two computers, maybe more than one of the following will be needed; a router, switch, hub, or access point.

2.6 WLANs Connection Modes:

IEEE 802.11 standard-based WLANs are currently very popular amid Internet and network users (Altunbasak and Owen, 2004).

There are many aspects to wireless networks: from modes of operation, to the attacks performed and their corresponding security solutions. A wireless network consists of a group of computers interconnected between each other through a wireless channel frequency. There are two modes for wireless connections: infrastructure (access point preferred) and ad-hoc (peer-to-peer). The infrastructure mode is characterized for having a centralized access point (AP) to which many computers can connect to and connect through to other computers in the same network.

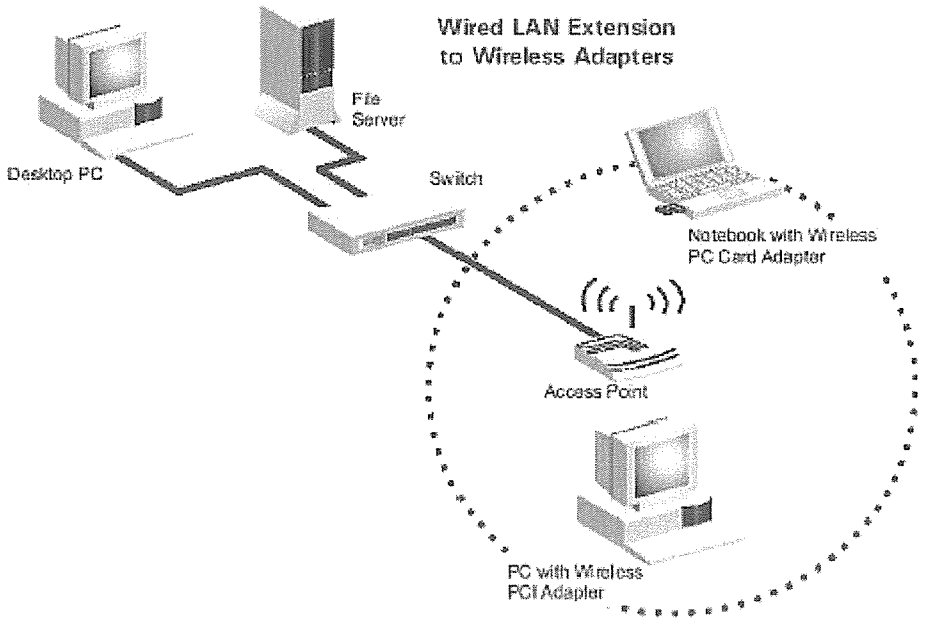


Figure 2.3: Infrastructure (AP) Wireless Network

Contrary to infrastructure AP networks, the ad-hoc mode is designed for having computers interconnect with each other as peers, without the need of a centralized AP. As we can see in Figure 2.4, we see the lack of a centralized AP. Nonetheless, computers are interconnected to each other. This type of wireless network is less common because of many different reasons. One of the reasons is that since there is no centralized AP, authentication from one computer to the other is somewhat more complicated than AP authentication, which resembles authentication in wired networks. In ad-hoc mode, computers are interconnected to each other by performing their own authentications (Candolin and Kari, 2002).

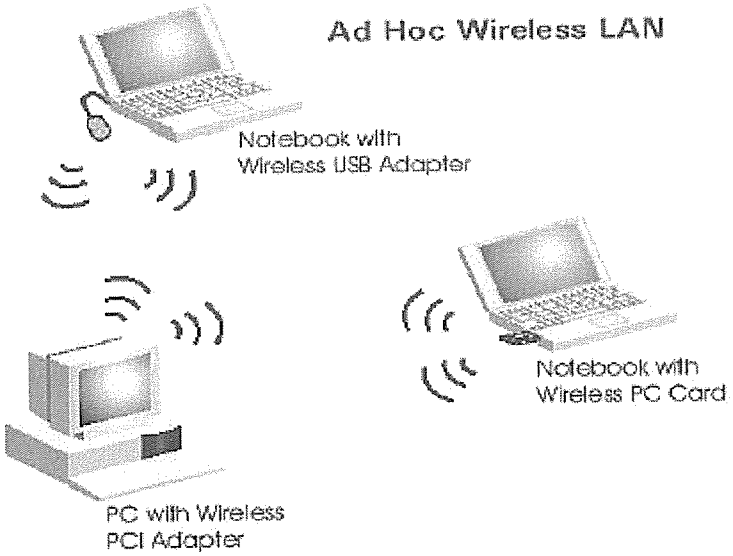


Figure 2.4: Ad Hoc (peer-to-peer) Wireless Network

Wireless Local Area Networks (WLANs) offer a quick and effective extension of a wired network or standard LAN. By simply installing Access Points to the wired network, personal computers and laptops equipped with WLAN cards can connect with the wired network at broadband speeds (Candolin and Kari, 2002).

Over the last few years, most deployments of WLANs have been on the IEEE 802.11b standard that operates over the unregulated 2.4 GHz frequency spectrum. The 802.11b standard offers connectivity of up to 11 Mbps – fast enough to handle large e-mail attachments and run bandwidth-intensive applications like video conferencing. While the 802.11b standard now dominates the WLAN market, other variations of the 802.11 standard, such as 802.11a and 802.11g, have been developed to handle increased speeds. WLAN vendors have committed to supporting a variety of standards (Altunbasak and Owen, 2004).

Benefits of Wireless LANs

Wireless LANs offer users an array of benefits which out weigh the challenges they face. These benefits range from cost efficiency to seamless integration with other networks.

The benefits Wireless LANs include:

1. "CAMP": Convenience, Affordability, Mobility, Productivity
2. Deployment advantages: Installation flexibility, speed and scalability
3. Regions without or with limited wired infrastructure can easily establish wireless communication
4. Wireless networks have a better chance of surviving disasters
5. 802.11 wireless LANs, WiMAX and 3G+ cellular networks promise high bandwidths, global mobility, quality of service and seamless integration with one another.

Problems faced by Wireless LANS

Network security attacks are a major concern in today's networked world. Software hackers and crackers are only part of the online security and privacy problem. Computer security threats can come from within the organizations operations too (Housley and Arbaugh, 2003). There is usually a tendency to believe that the current wireless access points present a larger security problem than the early Internet connections. A large number of organizations, based on vendor literature,

believe that the security provided by their deployed wireless access points is sufficient to prevent unauthorized access and use. Unfortunately, over the years, this has not been the case (Dyce, 2005).

Continuous waves of virus attacks, which cripple corporate networks in the wired world, have pushed security issues to the top of the agendas for organization managers and IT managers. Added to that are more security issues regarding the emergence of wireless networks, including Wireless Fidelity (Wi-Fi) and Wireless Wide Area Networks (wWANs), which provide access to/from corporate information (Berghel and Uecker, 2004).

Further more, WLANs have some shortcomings. These include inability to provide consistent and persistent signal since they are based on radio waves. Signals tend to vary continuously. This means that they are not able to provide ubiquitous coverage. There will always be coverage gaps even with higher-speed wWANs, for example, in buildings, in valleys, shadows of buildings, rural areas, between base stations. Further, WLANs also experience problems with Wi-Fi networks, especially during changing access points and temporary loss of signal (Housley and Arbaugh, 2003). WLANs also experience congestion because they do not have unlimited bandwidth. There is also a tendency to turn off or deactivate users even if the end user is in coverage.

Other security risks for organizations implementing wireless technology are the placement of rogue, or unauthorized, wireless access points on the corporate network, Denial-of-Service attacks, eaves dropping, encryption and authentication related problems (Housley and Arbaugh, 2003). In spite of all the problems mentioned above, it is possible to secure a WLAN network and create a trusted environment for its users.

2.6.1 Wireless LAN Security

At a wired network, one can often, to some degree, restrict the access to the network by physical means. The geographical range of a wireless network will more often than not be significantly greater than the office or home it's meant to cover; (Anonymous, 2003) any neighbor or arbitrary trespasser may be able to sniff on all the traffic and gain unauthorized access to internal network resources as well as to the Internet, possibly sending Spam (unsolicited mail) or doing illegal actions using the owner's IP address, if the security isn't taken seriously. Most equipment is Wi-Fi-certified, IEEE 802.11b or IEEE 802.11g compliant and offers some level of security like Wired Equivalent Privacy (WEP) and/or Wi-Fi Protected Access (WPA) (Arbaugh, 2002).

Security encompasses a number of facets, which is why organizations invest heavily in dedicated security infrastructure and highly trained specialists.

Every network application and infrastructure components have a distinct set of security requirements that must be addressed before managers feel comfortable entrusting it with the organization's mission critical information (Arbaugh, 2003). For wireless LAN, security takes place on two levels:

- The packet level
- The Radio frequency (RF) level

Within this context, organizations' WLAN security requirements essentially fall into three broad categories, with the first two referring to packet-level security and the third dealing with RF-level security.

1. Data Confidentiality and Integrity

The protection of data as it passes along the shared medium. Confidentiality is delivered through the use of encryption algorithms used to encode information in a manner that can only be decoded and read by the parties for which it is intended. Going hand-in-hand with encryption are the concepts of data integrity and non-repudiation, which help to prevent hackers from altering data. This is achieved

through the use of hashing algorithm, which takes a snapshot of each packet's content before it is encrypted (Borisov, et al, 2001). By doing this, even if a packet were to be decrypted; it would not be possible for the hacker to alter data contained within and fraudulently re-send the data. (For instance, changing the source IP address so that it appears that an authorized user is actually coming from the hacker's location) This process is known as spoofing. Strong data confidentiality and integrity are especially critical for wireless traffic, as packets can more easily be intercepted – and potentially compromised – by virtually anyone in the vicinity of the network (Arbaugh, 2003).

2. *Authentication and Access Control*

The mechanism used to grant authorized users access to the wireless network and resources residing on the broader organization's corporate network. More sophisticated implementations also allow for the definition of access control policies that grant different users or groups with unique security settings and access to different network resources. Robust authentication and access control measures are especially vital to WLANs because there is little available in the way of physical separation of authorized users from the network (Arbaugh, et al, 2004). A user can potentially have a laptop outside of the office premises, and without an authentication mechanism to keep them out, they could gain full access to the corporate network.

3. *Intrusion Detection and Prevention*

The aforementioned categories focus on the packet level and borrow heavily form wired network security principles – with unique wireless characteristics. Conversely, intrusion detection and prevention focuses on; the radio frequency (RF) level, and is entirely unique to WLAN. It involves radio scanning to detect rogue access points or ad hoc networks to regulate network access (Chlamtac, et al, 2003).

In the wireless world, overlapping of signal ranges with neighboring networks can often be expected. For this reason, wireless intrusion detection and prevention services must be able to identify and remove threats, but still allow friendly entities to co-exist while preventing them from accessing each other's resources. Advanced implementations are able to visually represent the network area along with potential threats, and have automatic classification capabilities so that threats can be easily identified. This proactive security takes advantage of the unique properties of Wi-Fi technology to deliver capabilities that extend beyond traditional wired security, and helps network managers to maintain control of the WLAN.

2.6.2 Understanding wireless vulnerabilities and threats

At this point it is important to remind ourselves and make a distinction between the terms threat and attack.

A ***threat*** is a potential violation of security. In other words, it is a possible danger that might exploit a vulnerability of the system (Stallings, W, 2003).

An ***attack*** is an actual violation of security. In other words, it is a deliberate attempt to evade security services and to violate the security policy of a system (Stallings, W, 2003).

Attacks on wireless networks fall into four basic categories:

- Passive attacks
- Active attacks
- Man-in-the-middle attacks, and
- Jamming attacks (Shimonski, 2002).

Passive attacks attempt to learn or make use of system information but do not affect system resources (Stallings, 2003). Active attacks attempt to alter system resources or affect their operation.

While security concerns can hold up implementations of wireless networks and technology, most enterprise decision-makers understand that they cannot put off addressing those concerns indefinitely. Whether or not their internal systems are

wirelessly enabled, (Borisov, et al, 2001) Organizations are still subject to threats as employees, customers and partners communicate through networks outside of the enterprise, and then use the same devices, or communicate the same information through the enterprise's wired networks. The boundaries between wired and wireless networks are blurring and so the most viable approach is to adopt a security posture that makes business sense for both wireless and wired networks from a balanced risk-management perspective (see graph Figure: 2.5).

Achieving an Optimal Security Posture

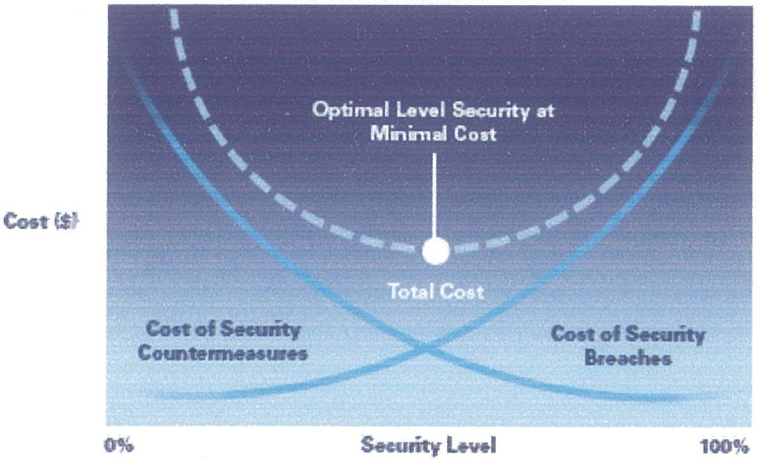


Figure 2.5: Adopted from "WS Building a secure foundation for Enterprise Mobility – Motorola, 2006, May".

Achieving an Optimal Security Posture

An effective risk-management approach to security balances the costs of security measures against the potential costs of the breaches they are designed to prevent.

The good news is that a focused strategy for security is not only accessible, it is good for organizations. Organizations are increasingly adopting security best practices at a strategic level. Rather than treating security as a series of point-issues to be "fixed," they are looking at security as a continuous process that enhances trusted relationships with employees, customers and partners. The

result, in many cases, can be a more transparent and trusted business environment.

To develop a practical wireless security strategy, it is important that those charged with making or approving security decisions first understand the nature of wireless vulnerabilities and the types of threats that can exploit them to cause damage.

The following is a general overview of some of the key vulnerabilities and threats, although they do not represent a complete picture of the risk landscape, they are the most commonly experienced over recent years (Nichols and Lekkas, 2002).

2.6.3 The Unique Challenges to Wireless Network Security

Myths about wireless security

1. Wireless isn't secure.
2. Spending more yields better security.
3. Technology is the answer.

Vulnerabilities mark the beginning of the risk management equation. Every technology, wired or wireless, poses some form of security vulnerability (Motorola, 2006).

For the security decision-maker, the challenge is to identify which vulnerabilities are most susceptible to today's constantly evolving threats and in particular his/her organizational environment. There are several basic sources of vulnerability to wireless networks, including:

• **Proliferation of Devices:** According to a 2004 report by Gartner, "By 2007, more than 50 percent of enterprises with more than 1,000 employees will make use of at least 5 wireless networking technologies." A chief source of vulnerability to a network is the sheer volume and complexity of the wireless environment, with

users relying on portable devices such as PDAs, laptops and smart phones (Arbaugh et al, 2004). In addition to the variety of devices utilizing wireless networks, Organizations must also account for the fact that most devices lend themselves to both business and personal use (Gartner, 2004).

• **Inadequate User Education:** This is perhaps one of the most significant securities vulnerabilities facing many organizations, because it spans all aspects of security. Ultimately, the security of any device, or the network accessed by that device, depends on the awareness of the individual user. Simply put, users cannot be relied upon to act on policies that are unclear or overly intrusive.

• **Converging Networks:** As mentioned earlier, the convergence of wireless and wired networks makes it nearly impossible for Organizations to either ignore wireless networks and technology or look at them in isolation. For example, an employee may email a password to a PDA. Once there, the password, and the security of the wired network, is subject to the security of the wireless PDA device, and to the actions of the employee who owns that device.
Not only does a security strategy have to address wired and wireless networks, but, as mentioned earlier, it must also account for the policies driving the actions of the people who use them (Motorola, 2006).

• **Unauthorized Access and Theft of Data:** Inadequate wireless security measures can result in the loss or theft of vital corporate and customer information. Such incidents, now in the news daily, erode customer and investor confidence and can lead to regulatory compliance problems.

• **Disruption of Service and Network Downtime:** Other vulnerabilities, such as poor isolation between wired and wireless networks and a lack of access management controls, can result in costly downtime for business-critical networks.

• **Viruses, Worms and Other Malicious Attacks:** Wireless devices, applications and networks are now points of entry and propagation for viruses, worms, and other forms of malicious attack. These exploits alone cost businesses nearly $14.2 billion in damages in 2005, according to a 2005 report by Computer Economics (Computer economics, 2005).

2.6.4 Comprehensive Enterprise Security: Local and Wide-Area Vigilance

Most wireless security vulnerabilities cross different network and device types. At the highest level, security and risk management should be technology agnostic. Technologies come and go, but strategic policies remain. Once high level security goals and policies are set, it's necessary to drill down into more granular enterprise security issues within the major networking realms, including Wireless Wide Area Networks (WWAN), Wireless Metropolitan Area Networks (WMAN), and Wireless Local Area Networks (WLAN) (Motorola, 2006).

2.6.5 Network Security Threats

In an "isolated" Ethernet network, threats can only originate from devices that have physical connectivity to the LAN. With WiFi wireless networks, any device in range of the local access point is potentially a threat. As enterprise applications are extended to metropolitan (e.g., 802.16) and wide area (e.g., CDMA, GPRS) cellular networks, the number of potential threat sources increases exponentially. But it would be erroneous to conclude that it's impossible to secure wireless LANs. There is a wealth of security features built into LAN technologies and wireless operator networks.

The real question is: are these features being used and are they united in well-designed security management architecture?

Enterprise users of wireless LANs need to be aware of a number of threats and vulnerabilities that are specific to their environment, including:

• **Compromise of subscriber identities and activities.** Users who run enterprise applications across LANs are not necessarily invisible to other users. If your wireless operator has inadequate security procedures, it's possible that your end-user sessions will be visible to hackers, and in the worst case their session data can be compromised. It is possible for LAN traffic to be snooped, so highly sensitive LAN applications should employ end-to-end encryption and VPN methods (Nichols and Lekkas, 2002).

• **Denial of services.** It may seem that wireless LANs is immune to the type of denial of service (DOS) attacks that are increasingly common on the Internet and corporate IP networks; however, this is not true.

A well-designed network infrastructure will protect against external intruders with a wide range of intrusion detection and intrusion prevention tools, and an architecture that isolates key assets into tightly monitored and authenticated **security zones**. In general, enterprises depend on the operators that serve them to constantly guard against weaknesses in security processes and policies, particularly in these areas (Henning, 2003):

- Unhardened operations management devices and network
- Lack of strong authentication and access control procedures
- Use of poorly trained or unqualified administrative personnel
- Poorly managed software update and patching process
- Lack of security audit and monitoring process
- Lack of security review and vulnerability assessment

• **Theft or loss of handsets and other small wireless devices.** While the chances of theft of an enterprise desktop PC are minimal, the chance of laptop theft is considerable. With handheld devices, the potential for loss or theft is greater still. At first glance, there is not much that can be done to stop corporate users from leaving their handheld devices in taxis and airport lounges, but there are a number of policies that can be put in place to limit the damage caused by this

inevitability. Increasingly, handheld devices will be equipped with biometric protections that will render them inoperative to everyone but their owners (Motorola, 2006). It's also possible to design network applications so that critical data resides inside the corporate data center as much as possible, with the handheld device acting primarily as a remote terminal for viewing this data. In this case, when the device is misplaced or stolen, the account is terminated centrally and no loss of data occurs.

In addition to the deployment of advanced handheld security technologies, it is highly recommended that enterprises conduct a thorough security assessment of all wireless applications that use wireless LAN connectivity (Henning, 2003).

2.6.6 Wireless LAN Security Threats

The very nature of networking means users can exchange information across a distance over a shared medium. The security implication of this is that a hacker doesn't even need to actually walk up to a server or a user's computer in order to gain access to critical files or communications. With wireless LAN, this threat is especially pronounced, because now a hacker doesn't even need to reside on the same physical location (Nichols and Lekkas, 2002).

When looking at technology threats facing an enterprise network, it is appropriate to consider WLANs, the weakest links in traditional IP networks. For example, considering an attack launched against a large retail chain in suburban Detroit. Using inexpensive, available equipment, intruders accessed the chain's local IP network by exploiting an unsecured wireless network. The intruders proceeded to access additional stores around the country. They then modified an in-store application used to process credit card transactions, making customers' account numbers easily accessible for later retrieval (Hao, et al, 2004).

The threats to the WLAN environment provide valuable insight into the types of activities malicious users can employ to compromise wireless networks.
While the three threats described below represent a small sample of the types of issues facing wireless security, they do underscore the need for a focused security policy and strategy. Examples include:

- **Radio Frequency (RF) Eavesdropping:** An intruder can target a specific wireless network with the intent to eavesdrop and capture all over-the-air (wireless) traffic transiting the network. Lack of data encryption yields clear text output for the intruder. Weak data protection can be easily cracked using publicly available tools with little technical experience. Proprietary corporate information and confidential customer data can be collected, stolen, exposed or otherwise compromised (Hao, et al, 2004).

- **Reconnaissance Probes:** Another type of threat occurs when someone looks for open Wi-Fi signals (termed "War driving"), often using a common tool called NetStumbler. This tool, and many others like it, takes advantage of the fact that wireless networks typically broadcast their network name or SSID. Run on handheld device with wireless client, Netstumbler can be used to discover wireless networks in an unobtrusive manner. It is typically a passive tool, but occasionally will broadcast such that an intrusion detection system can pick it.

  The fact that network names can be discovered has been amplified by some vendors as a source of concern in an attempt to help sell dedicated wireless intrusion detection systems. However, a wireless LAN that employs 802.11i (WPA2) or WPA for security can not be breached simply through the discovery of the network name (Buchholz, 2003).

- **Weak Authentication**: Lack of strong authentication protecting the WLAN from unauthorized users substantially increases the risk of accidental or malicious

external use. Unauthorized users can view, steal or otherwise compromise confidential corporate and customer data or launch a variety of attacks against both wireless and core networks. The use of authentication within any environment is a critical step in thwarting unauthorized access and providing auditable information, which, in turn, substantially reduces cycle time for troubleshooting and incident investigation.

- **Rogue Devices:** The relatively low cost and widespread availability of wireless infrastructure equipment and devices can lead to employees bypassing corporate policies and security measures to establish their own connections to corporate WLANs. Unsecured, unauthorized WLAN equipment (infrastructure or client-based) can impact the availability of the production WLAN by introducing RF interference within production air space. This potentially provides open access to any wireless user within range. Frequent war-drivers can detect this vulnerability and publicly advertise it to other potential intruders along with specific instructions for launching an exploit.

  The results; service disruption can yield substantial monetary and operational impacts, including unauthorized network access, network unavailability, loss of productivity during incident investigation and repair, and the exposure of backbone networks and systems.

2.6.7 The "Non-Technical" Threats: Social Engineering

In addition to the technical threats to networks illustrated by the WLAN issues outlined above, organizations must also recognize the growing risk posed by hackers and malicious parties circumventing security technologies altogether by exploiting human vulnerabilities. Over the past five years, attacks themselves have shifted and evolved from being purely technical in nature (such as, denial of service, hacking) to incorporating social engineering techniques (such as, phishing, viruses) that exploit the human perimeter and the policy level:

Traditionally the weakest links in the security framework; for this reason, organizations cannot rely entirely on technology solutions alone to protect their critical enterprise networks.

2.7 A Holistic Approach to Wireless Security: People, Process, Policy And Technology

Given the proliferation of non-technical, social-engineering threats, Organizations cannot count on only technologies such as firewalls and Intrusion Detection Systems (IDS) to safeguard their networks. Much as these technological measures are implemented, in reality, the only way to adequately address security concerns effectively across the enterprise in addition to technology is to embrace a holistic security model that considers the environment in which both wired and wireless technology operates. Such an approach integrates the key environmental considerations of people, process and policy along with technology (Motorola, 2006).

- **People:** The human factor in securing enterprise networks encompasses a variety of issues, ranging from employee awareness and education, to building the business case and gaining support to implement an appropriate security strategy. Once an organization can leverage its most valuable resource, people, the ability to mitigate risks becomes more efficient and less cost-intensive.

- **Process:** Processes that are measurable can streamline operational cost and enhance any organization's security posture. This enhanced posture helps ensure system availability, confidentiality, and integrity.

- **Policy:** A prudent and dynamic policy is critical to informed decision-making processes. When making decisions questions such as these should be asked. Does your organization have policies that address current key issues in network security? Are those policies and processes being communicated clearly, and are

they being enforced? The answers to these questions go a long way toward determining an organization's security posture.

• **Technology:** The technology component of an effective enterprise security strategy encompasses traditional security measures, such as firewalls, authentication and Intrusion Detection Systems (IDS) systems. It must also account for ever-changing vulnerabilities, the interconnectedness of wired and wireless systems, and the need to identify and address emerging threats before they cause damage (Motorola, 2006).

2.7.1 The Value of Vulnerabilities Assessment

For any organization, an effective security approach starts with a measurement and assessment of vulnerabilities within the organization's current information technology environment. This assessment sets the benchmark for the organization and provides an immediate identification of known vulnerabilities
(Peltier, et al, 2003).
A thorough assessment will identify critical system assets, prioritize vulnerabilities and suggest actionable remediation guidelines. Although this is not a formal risk assessment of the entire environment, it does provide a holistic review of the network environment by analyzing the critical network, host and firewall systems that determine the current information security posture (Henning, 2003).

This assessment can give the organization an understanding of the security risks related to its activities and the appropriate actions needed to mitigate those risks/vulnerabilities (Henning, 2003). An organization should have a complete network assessment performed at least annually (or more frequently depending on the sensitivity of information on the network) to identify any new equipment, vulnerabilities or changes to the environment that may have inadvertently increased its security exposure.

Following a vulnerability assessment, a risk management approach is needed to balance security risks against business priorities and limited budgets (Peltier, et al, 2003). Without a thorough, focused understanding and prioritization of a network's risks and vulnerabilities, it becomes extremely difficult to deploy a coherent solution. An ad-hoc approach can place too much focus on non-critical systems, and, as a result, overlook "high impact" threats. This may expose the environment to theft of organization information, waste resources and budget, and provide a false sense of security. Once executives have a thorough understanding of the risks their Organization face, they can make informed investment decisions.

2.7.2 The Trend in WLAN Security over recent years.

The wireless LAN market is expanding year after year along with the rapid spread of broadband infrastructure. Recent advances in technology have made commercial deployments of wireless networks possible, opening up potentially huge opportunities. The WLAN market is set to grow at an annual rate of 30% per year to nearly $5 billion by this year 2006. WLAN equipment sales have jumped 60% from this time last year to the present. WLANs for the home and small offices are projected to grow 103% and WLAN sales to the enterprise will grow at 32% (Carl and Weinschenk, 2003).

Although relatively new, the wireless local area network (WLAN) security market has been experiencing tremendous growth as wireless technology becomes more widespread. Organizations are shifting to WLAN technology as they realize its advantages of huge productivity gains through mobility and instant access to information and standards that ensure interoperability of WLAN equipment. This is expected to drive strong growth in the WLAN security market. Since WLAN technology is used to transmit sensitive data and the possibility of that data going astray exists, the need for a solution to secure it is expected to continue, remarks Carl (Carl and Weinschenk, 2003).

2.8 WLAN Security Technologies:

2.8.1 Wired Equivalent Privacy - (WEP)

WEP, the oldest, most prevalent form of WLAN encryption available, was originally designed to bring the same level of security to a WLAN that was available on a traditional wired LAN. WEP uses a matching encryption key at both the access point and the wireless client to secure wireless communication. These keys can be either 64 or 128 bits in length. Only the first 40 or 104 bits are used as the actual encryption key. WEP keys must be distributed to each WLAN client device.

The 802.11 standards define WEP as a simple mechanism to protect the over-the-air transmission between WLAN access points and network interface cards (NICs). Working at the data link layer, WEP requires that all communicating parties share the same secret key. To avoid conflicting with U.S. export controls that were in effect at the time the standard was developed, 40-bit encryption keys were required by IEEE 802.11b, though many vendors now support the optional 128-bit standard. WEP can be easily cracked in both 40- and 128-bit variants by using off-the-shelf tools readily available on the Internet. On a busy network, 128-bit static WEP keys can be obtained in as little as 15 minutes, according to current estimates http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html, http://www.cs.umd.edu/~waa/wireless.pdf.

WEP has a number of weaknesses as stated by many reports. It has been shown that WEP keys can be deduced in very little time. WEP-encrypted packets can be altered without detection using a “man-in-the-middle” attack. By modern standards, WEP is not considered a cryptographically strong security solution. Organizations concerned with security often use WEP as their preliminary security method to moderately limit access to their WLAN, but use a Virtual Private Network (VPN) as a more secure gatekeeper to the core enterprise network to provide data confidentiality (Berghel and Uecker, 2004).

2.7.2 Wi-Fi Protected Access - (WPA)

The recent 802.11i specification was still being developed to resolve the issues found in WEP, but to expedite the introduction of a more adequate WLAN security scheme for the enterprise market, the Wi-Fi Alliance introduced the WPA specification. Based on a subset of the 802.11i draft standard (which had not yet been released), WPA improved on WEP in the following ways:

- To address WEP's encryption issues, Temporary Key Integrity Protocol (TKIP) was introduced. TKIP utilizes temporal encryption key that is renewed every 10,000 packets, preventing a key from being stolen and subsequently used to decipher a significant amount of information. In addition, data integrity was improved through the use of more robust Michael Message Integrity Check (MMIC) hashing mechanism.
- The use of the 802.1x authentication specification was also incorporated. Based on the Extensible Authentication Protocol (EAP), WPA introduced a more sophisticated mechanism for user authorization and access control by leveraging RADIUS authentication tools (Berghel and Uecker, 2004).

WPA did a great deal to address the concerns associated with WLAN security, and can be hailed as an important step in increasing acceptance of WLAN as an enterprise –ready technology. However, concerns still existed.

While the use of temporal keys by TKIP mitigated some problems, many felt uncomfortable entrusting their critical data to a security mechanism that was inherently flawed. Because of this, many viewed WPA as a temporary measure meant to bridge the gap between WEP and soon-to-be ratified 802.11i standard, and therefore insisted on postponing their deployments.

2.7.3 Temporal Key Integrity Protocol – (TKIP)

The Temporal Key Integrity Protocol (TKIP), which is part of the 802.11i WLAN security standard, addresses the shortcomings in WEP without requiring replacement of the existing WLAN hardware (IEEE P802.11 Task Group I, 2004).

TKIP is more robust than WEP and is not susceptible to the same attacks. TKIP keys are larger than WEP keys (128 bits for the key itself, compared to 40 or 104 for WEP) and are generated dynamically for each session. Where WEP uses a single fixed key for an entire session, TKIP keys are changed automatically for each packet of transmitted data.

To prevent man-in-the-middle attacks, TKIP includes a Message Integrity Check (MIC). Transmitted packets that are captured, altered, and resent fail the MIC and are discarded. Because of the dynamic nature of TKIP keys, a secure method of distributing these keys to a wireless client is required.

2.7.4 Internet Protocol Security - (IPsec)

IPsec is a framework of open standards for ensuring secure private communications over IP networks. IPsec Virtual Private Networks (VPNs) use the services defined within IPsec to ensure confidentiality, integrity, and authenticity of data communications across public networks, such as the Internet. IPsec also has a practical application to secure WLANs by overlaying IPsec on top of clear-text 802.11 wireless traffic.

When deploying IPsec in a WLAN environment, an IPsec client is placed on every PC connected to the wireless network and the user is required to establish an IPsec tunnel to route any traffic to the wired network. Filters are put in place to prevent any wireless traffic from reaching any destination other than the VPN gateway and Dynamic Host Configuration Protocol (DHCP) or Domain Name System (DNS) server. IPsec provides for confidentiality of IP traffic, as well as authentication and anti-replay capabilities. Confidentiality is achieved through encryption using a variant of the Data Encryption Standard (DES), called Triple DES (3DES), or the new Advanced Encryption Standard (AES) (FIPS-197, 2001).

Though IPsec is used primarily for data confidentiality and device authentication, extensions to the standard allow for user authentication and authorization to occur as part of the IPsec process.

2.7.5 VPN-WLAN Integration

After vulnerabilities were revealed in WEP, many organizations' intent on deploying WLAN discounted security measures introduced by the IEEE 802.11 working groups and the Wi-Fi Alliances altogether. The thinking was that the best security solution could be found in the open, standards-based technology delivered by Virtual Private Network (VPN). Internet Protocol Security (IPsec) is the IETF standard for VPN, and it has been through a number of revisions that have resulted in a robust security standard that provides exceptional data confidentiality, authentication and access control for IP-based network traffic, regardless of the physical medium (Carli, et al, 2003). The implementation involved installing VPN client software on each wireless client, which would then establish encrypted tunnels to a VPN gateway located somewhere on the wired network. By integrating wireless LANs into an IPsec infrastructure, network managers allowed the WLAN infrastructure to focus on simply transmitting wireless traffic, while the VPN would secure it.

Using VPN to secure WLANs ostensibly resolved the wireless security issue. However, there were a number of problems that prevented this from being ideal:

- IPsec was designed to provide security within a fundamentally different architecture than a wireless LAN. VPN is meant to give external user's encrypted access to the LAN using firewall policies. With VPN, wireless users are treated as external to the network, even though they are in fact local. Therefore, their application performance and access rights are often very different from wired users. As a result, even if a wireless user is a member of the same team as a wired user and is in the same physical location, the two will be subject to completely different criteria to access the same resources (Carli, et al, 2003).
- Overlaying VPN onto a wireless solution also raises the issue of complexity. Each wireless device must have a VPN client installed and individually configured, and this client – which also can have dramatic impact on system

performance – must be started every time the user wants to access the network. End-users find this process cumbersome, while IT managers are loath to deploy and maintain separate security infrastructure on top of the wireless infrastructure.

- The excessive cost of VPN solutions represents another major issue. VPN solutions involved significantly higher capital and operational per-user costs than wireless LAN equipment does (Ray, et al, 2005). While network managers are able to justify these costs based on the ROI derived from other VPN applications like remote access, few of them are able to see a positive ROI on VPN-secured wireless LANs when their initial WLAN investment is inflated by several hundred percent after incorporating VPN security.

2.7.6 802.1x and the EAP

IEEE 802.11 authentication is offered by three mechanisms:

1. Open system authentication, where only the AP's publicly available network name – also known as Service Set Identifier (SSID) is used;
2. Shared key authentication, where a static, manually preset WEP key on both the AP and the stations is used; and
3. Configuring the AP to only accept selected MAC addresses.

Whether used separately on in combination, these measures are easily over come with widely available hacking tools. Open System Authentication depends on an attacker not learning the SSID – but this can always be learned by using a packet sniffer, even when the SSID broadcast has been disabled. Shared Key Authentication is poorly designed and an attacker with a packet sniffer can reuse information gathered from one valid authentication to authenticate him. Finally, any Wi-Fi card MAC address list is ineffective and not scalable.

In the name of "Plug-and-play", the default authentication is only Open System Authentication, which is why default AP security is said to be off.

However, it is important to note that, the 802.1x standard defines a generic framework that can be used to authenticate users who want to access a wired or wireless network. 802.1x does not perform this authentication itself; instead it defines an Extensible Authentication Protocol (EAP) that enables a number of authentication methods. The main components of an 802.1x environment include.

- **Supplicant: This is the 802.1x/EAP client software running on the WLAN client device.**
- **Authenticator: This is the access point that acts as a mediator, relaying EAP packets between the supplicant and an authentication server.**

The three main elements of an 802.1X and EAP approach follow:

- Mutual authentication between client and authentication (Remote Access Dial-In User Service [RADIUS]) server
- Encryption keys dynamically derived after authentication
- Centralized policy control, where session time-out triggers re-authentication and new encryption key generation

When these features are implemented, a wireless client that associates with an access point cannot gain access to the network until the user performs a network logon. After association, the client and the network (access point or RADIUS server) exchange EAP messages to perform mutual authentication, with the client verifying the RADIUS server credentials, and vice versa. An EAP supplicant is used on the client machine to obtain the user credentials (user ID and password, user ID and one-time password [OTP], or digital certificate). Upon successful client and server mutual authentication, the RADIUS server and client then derive a client-specific WEP key to be used by the client for the current logon session. User passwords and session keys are never transmitted in the clear, over the wireless link.

The sequence of events follows:

- A wireless client associates with an access point.
- The access point blocks all attempts by the client to gain access to network resources until the client logs on to the network.
- The user on the client supplies network login credentials (user ID and password, user ID and OTP, or user ID and digital certificate) via an EAP supplicant.
- Using 802.1X and EAP, the wireless client and a RADIUS server on the wired LAN perform a mutual authentication through the access point in two phases. In the first phase of EAP authentication, the RADIUS server verifies the client credentials, or vice versa. In the second phase, mutual authentication is completed by the client verifying the RADIUS server credential, or vice versa.
- When mutual authentication is successfully completed, the RADIUS server and the client determine a WEP key that is distinct to the client. The client loads this key and prepares to use it for the logon session.
- The RADIUS server sends the WEP key, called a session key, over the wired LAN to the access point.
- The access point encrypts its broadcast key with the session key and sends the encrypted key to the client, which uses the session key to decrypt it.
- The client and access point activate WEP and use the session and broadcast WEP keys for all communications during the remainder of the session or until a time-out is reached and new WEP keys are generated.
- Both the session key and broadcast key are changed at regular intervals. The RADIUS server at the end of EAP authentication specifies session key time-out to the access point and the broadcast key rotation time can be configured on the access point.

2.7.7 Lightweight Extensible Authentication Protocol (LEAP)

LEAP, also known as EAP-Cisco Wireless, was developed by Cisco systems in response to the weaknesses identified in WEP. LEAP uses the 802.1x authentication framework. After authentication, dynamically-generated WEP keys are sent to the WLAN client. To provide added security to basic WEP, these keys change automatically throughout the course of a session.

- **Authentication server:** This is often a Remote Authentication Dial In User Service (RADIUS) server responsible for deciding whether a user should be allowed to access the network. By centralizing authentication with a RADIUS server, access points do not need to be reconfigured each time a new user is added to the WLAN.

When a wireless client first associates itself with an access point enabled for 802.1x security, the only communication allowed by that access point is 802.1x authentication. Using a negotiated EAP method, the supplicant on the wireless client sends its credentials (typically, a user name and password) to the access point (the authenticator), which forwards the information to the authentication server. The authentication server instructs the access point to allow or disallow the particular client access to the WLAN.

After a WLAN client has been authenticated successfully, a special algorithm establishes the encryption keys that the access point and the client use. The keys are WEP or TKIP keys, depending on the EAP method used. After the user is authenticated and WLAN encryption keys are established, the client has encrypted access to the enterprise LAN.

Using 802.1x for authentication simplifies the administration of WLAN security. Granting or revoking WLAN permissions requires updating the central authentication server. It does not require configuration changes at the access point level.

LEAP authentication is based on a user name and password. Passwords are encrypted using a one-way function before being sent to the authentication server. LEAP significantly improves on basic WEP security. However, Cisco announced in 2003 that passwords sent using LEAP are vulnerable to attack, especially when cryptographically weak, or simple, passwords are used.

2.7.8 Protected Extensible Authentication Protocol - (PEAP)

PEAP is an open standard jointly developed by Microsoft, RSA Security and Cisco Systems. It uses the 802.1x framework, and was designed specifically for use with WLANs (Cisco netacad, 2005).

PEAP works in two phases. In the first phase, Transport Layer Security (TLS) creates an encrypted tunnel between the supplicant and the authentication server. In the second phase, the supplicant sends its credentials to the authentication server using the TLS tunnel.

The two versions of PEAP are PEAPv0 (also known as Microsoft PEAP) and PEAPv1 (also known as Cisco PEAP). In addition, there are a number of second-phase protocols that can be used for the credential exchange.

The IEEE has finally done what it should have done long ago: It ratified a workable security standard for 802.11 wireless LANs. Known as 802.11i, (IEEE P802.11 Task Group I, 2004) it's a significant event for the wireless industry and provides momentum for what many expect to be a major ramp up of WLAN implementation in the enterprise. Like most new standards, it will take some time to mature, but the Wi-Fi Alliance's decision to jump the gun in 2003 by rolling out WPA (Wi-Fi Protected Access) will help ease the implementation burden somewhat (Dave, 2004).

As most observers of the WLAN industry are aware, the security features found in the original standard were woefully inadequate. To a certain degree, these deficiencies reflected the perception that security services are normally

implemented at layer 3 and above. After all, Ethernet enjoyed explosive success throughout the 1990s with no inherent security capabilities. However, since Ethernet relied on a guided medium that could be secured easily and was normally implemented using switches that isolated unicast traffic, the need was not so compelling.

The new 802.11i standard is much better, providing two of the three fundamental network security capabilities: authentication and privacy. Authorization services, for which open standards are not so critically important, are already delivered at higher layers by a range of infrastructure products (Cisco netacad, 2005).
802.11i's privacy services are built on top of AES, (IEEE P802.11 Task Group I, 2004) a strong encryption standard that passes muster with even the most paranoid security administrators. While AES is overkill for most environments, there's really no added cost (Sanchez-Avila and Sanchez-Reillol, 2001).That's because leading chipmakers, including Atheros and Broadcom, have been implementing hardware-based AES for a couple years now (Broadbeam, 2004).

Authentication with 802.11i is built around the 802.1X protocol, used in conjunction with EAP (Extensible Authentication Protocol) and implemented using RADIUS authentication servers that have been proven for many years in managing secure dial-up connectivity (IEEE P802.11 Task Group I, 2004). While EAP supports a range of alternate authentication types carried over 802.1X, the lack of a single, universally accepted standard will inevitably lead to implementation and interoperability challenges. Windows shops may be tempted to build their security environment around Transport Layer Security (TLS) or Microsoft PEAP, but these standards are not always supported on non-Microsoft systems.

The 802.11i authentication system is effective in a simple WLAN environment, but roaming introduces significant challenges. When users roam between WLAN cells, they need to re-establish their security credentials (IEEE P802.11 Task Group I, 2004). The entire 802.11i authentication process takes up to about four times

longer for time-sensitive applications. To combat this problem, the 11i committee added two special features, including a client caching mechanism that allows you to quickly re-authenticate to access points with which you have had a previous authentication. Contributed by Trapeze Networks, this system is reported to decrease authentication time to about 25 milliseconds (Dave Molta, 2004).

While caching speeds up the process of re-association, it does nothing to address association with new access points. To address this issue, Cisco and Microsoft contributed a rather crude pre-authentication algorithm that anticipates roaming. While a number of committee members were openly critical of this system, the majority felt that it was better to have a limited pre-authentication standard than none at all. Additional work on this problem will continue under the auspices of the newly formed 802.11k committee (Dave, 2004).

2.7.9 Kerberos

When Kerberos was developed at MIT it was intended to provide authentication and security in the campus computing network at MIT and to other intranets. Today it is used by many organizations, companies and universities
(Coulouris et al., 2001). Kerberos is partly based on the Needham and Schroeder authentication protocol. In their protocol they specify an authentication server which contains a list of users and their passwords. Everybody on the network must therefore trust the authentication server. In Kerberos there are two services on the authentication server, the authentication service and the Ticket Granting Service (TGS). The authentication service authenticates the client and replies to the client with a ticket to the TGS. The TGS receives the ticket from the client and checks its validity and replies to the client with a new ticket to the server the client wishes to make a request to. The hosts on the network are required to be loosely synchronized to handle replay attacks. If the synchronization is performed over the network the synchronization protocol must itself be secure.

Proprietary Alternatives Available Today

Several WLAN vendors provide robust, but proprietary, solutions to address WEP shortcomings.

These solutions combine standards-based 802.1x implementation with a proprietary version of TKIP. Since they address known WEP flaws, these solutions have been shown to be effective at providing a wrapper for WEP and therefore should server as an effective deterrent even for active techniques that may be used in a targeted attack.

The primary tradeoff for this path is that organizations must use WLAN APs and clients that support the same proprietary approach, either from a common vendor, or its licensees.

Generally, vendors offering proprietary options will enable their customers to migrate to standards-based solutions via software/firmware upgrades.

2.8 Management guidelines to WLAN security Solution Selection:

Some of the factors that have influenced Organizational Management Decisions over recent years are discussed below. These are some of the Industry Standards best practices that should be observed in every WLAN environment.

2.8.1 Productivity-Boosting and Cost-Saving Benefits

802.11 WLAN technology allows workers to connect to the corporate network from a conference or board room, the cafeteria, or a bench outside the building at broadband speeds. In developed countries, organizations are quickly deploying new networks without the costs and time of wiring offices and workstations. *"By year-end 2002, 30% of enterprises suffered serious security exposures from deploying WLANs without implementing the proper security"*(Gartner Group, 2002).

WLAN traffic travels over radio waves that cannot be constrained by the walls of a building. While employees might enjoy working on their laptops from a grassy spot outside the building, intruders and would-be hackers can potentially access the network from the parking lot or across the street.

When WLANs are deployed, standard encryption and user authentication features should be implemented within the Access Points and WLAN cards (Buchholz, 2003). While these tools provide the first steps of managing a secure WLAN, the very nature of the airwaves opens a WLAN to unwanted intruders and potential attacks. Security managers must constantly be on guard against intruders attempting to access the corporate network as well as internal activities that weaken security and overall network performance (AirDefense, 2005).

Intruders and hackers pose three main threats to the security of a WLAN.

- Because wireless communication is broadcast over radio waves, eavesdroppers who merely listen to the airwaves can easily pick up unencrypted messages. Additionally, messages encrypted with the Wired Equivalent Privacy (WEP) security protocol can be decrypted with a little time and easily available hacking tools (Burr, 2003). These passive intruders put businesses at risk of exposing sensitive information to corporate espionage.
- The theft of an authorized user's identity poses one the greatest threats. Service Set Identifiers (SSIDs) that act as crude passwords and Media Access Control (MAC) addresses that act as personal identification numbers are often used to verify that clients are authorized to connect with an Access Point. Knowledgeable intruders can pick off approved SSIDs and MAC addresses to connect to a WLAN as an authorized user with the ability to wreak havoc on the entire network, because existing encryption standards are not foolproof (Burr, 2003).

- Finally, outsiders who cannot gain access to a WLAN can none-the-less pose security threats by jamming or flooding the airwaves with static noise that causes WLAN signals to collide or simply force stations to continuously disconnect from Access Points. These Denial-of-Service (DoS) attacks effectively shut down the wireless network in a similar way that DoS attacks affect wired networks.

2.8.2 Internal Vulnerabilities

Careless and deceitful actions by both loyal and disgruntled employees also present security risks and performance issues to wireless networks with unauthorized Access Points, improper security measures, and network abuses. Because a simple WLAN can be easily installed by attaching an Access Point to a wired network and a WLAN card to a laptop, employees deploy unauthorized WLANs when IT departments are slow to adopt the new technology.

Despite the security risks of 802.11 WLANs, Gartner Group declared in February 2002, that WLANs are moving toward becoming "safe enough" to deploy for most organizations. Just as wired networks are secured using several technologies, WLANs require a layered approach to security with five key technologies (Access point, Discovery & Vulnerability Assessment, Authentication & Authorization and Intrusion protection).

2.8.3 Access Point Security:

At the most basic level of security, all Access Points should be configured to enact their imbedded security features, such as MAC filtering where only authorized MAC addresses can associate with the Access point.

Every network client (wired or wireless) is assigned a unique 48-bit MAC address. MAC address filtering involves programming the MAC address of every client device that is allowed to access a specific WLAN into each access point. This is the simplest form of WLAN security.

MAC address filtering is a very weak form of security. It is a rudimentary form of authentication (MAC address spoofing is a well-known weakness) and does not provide any encryption. Additionally, administering a WLAN using MAC address filtering can be labor-intensive, as the MAC address of each new client that wants to access the WLAN must be added to the list of allowed MAC addresses at each access point.

MAC address filtering is used mostly by very simple WLAN client devices that do not support any other form of WLAN security.

While useful for small deployments, MAC filtering is not feasible for enterprise WLANs.

2.8.4 Discovery and Vulnerability Assessment:

Since rogue Access Points and ad hoc networks can pop on and off a WLAN with ease, all WLANs should be monitored 24hours a day, 7 days a week to discover all WLAN deployments and identify network vulnerabilities as they happen. Without effective network discovery and vulnerability assessment, (Candolin and Kari, 2002) a security manager would never know if a rogue Access Point is attached to the network, an access point openly broadcasts its SSID, or a WLAN card is reconfigured to allow ad hoc networks.

2.8.5 Encryption, Authentication & Wireless VPNs:

Although WEP-based can be compromised, it is effective in guarding your data from drive-by hackers who are not willing to devote the time it takes to crack the encryption. Several vendors provide more reliable encryption.

While MAC-based access control is the simplest form of authentication, it's also the easiest to compromise. Numerous vendors offer authentication with session-specific keys and access control servers to only allow authorized users onto the network and limit their access to only designated systems on the network. Many

organizations are deploying wireless virtual private networks to strengthen encryption and authentication. However, this may not be a viable solution for all organizations.

2.8.6 Intrusion Protection & Policy Enforcement:

Security managers rely on intrusion detection and policy enforcement to ensure that all components of a WLAN are secure and are being used within the realm of organization /enterprise specific policies. While many organizations have already deployed intrusion detection systems for their wired networks, only a WLAN-focused intrusion detection system can:

(i) Identify and eliminate Denial-of-Service attacks;

(ii) Identify when a session is hijacked and disconnect the intruder; and

(iii) Determine where and when a security breach happened.

Without a policy enforcement layer of security, a security manager would never know if traffic is unencrypted, stations connect over unauthorized channels, or if confidential files were sent over the wireless network in the middle of the night.

2.9 Hope on the horizon

A new approach to WLAN security is emerging. There are hopes that the wide-scale acceptance of WLANs and the resulting publicity around security issues is making people more aware of the issues and, therefore, less careless. The standard itself is changing as well. In the short term, another standard -- WiFi Protected Access (WPA) -- replaced WEP. Over the long haul, the standard from which WPA is derived, called 802.11i, has also taken over (Research and Consultancy Outsourcing Svcs., 2005).

Clearly, the industry is struggling to get its ducks in a row even as wireless usage increases radically. For the time being, says Clark, "Organizations can be relatively safe by using WEP Weak Key Avoidance." This approach, as the name implies, bypasses the compromised elements of WEP. Also, "A key to implementing WLAN

security is that it has a clear migration path," says Singhal (CTO of wireless security vend). This can be in the form of potential software-based upgrades or the inclusion of a middleware level that handles the complexities of standards transitions independently of the security software itself (Research and Consultancy Outsourcing Svcs., 2005).

WPA has encryption and authentication layers. On the encryption layer, a concept called the temporal key integrity protocol (TKIP) is currently working its way through the IEEE's 802.11i standards committee. "TKIP will initially use RC4 encryption, but later it will implement the more secure advanced encryption standard (AES)," says Sanchez (Sanchez-Avila and Sanchez-Reillol, 2001).

Chapter 3: RESEARCH METHODOLOGY

3.1 INTRODUCTION

This section describes methods and techniques, which were used for data collection and analysis during the study. It also describes the procedure of obtaining samples and the reasons why these particular methods are preferred by the researchers. The tools were chosen as appropriate ones to the study topic.

3.2 Research design

The study was intended to cut across-sections, and describes the nature and pattern in which the study was done and steps followed. In that case, the study employed both qualitative and quantitative research. To cater for all kinds of information that would be relevant to the study, because; most of the problems, which were identified, could be quantified in terms of the loss it caused to the organization, which offered specialized techniques for obtaining the in-depth responses about what the technical experience on the ground is.

3.2.1 General methodology structure:

- **Application Architecture review:** Review of existing wireless security functionality, features and architecture with the organization.
- **Automated detection of access points:** Use of automatic scanning utilities and tools to identify wireless access points on the organization's network.
- **Unauthorized Access point identifiers:** Comparison of the complete list of access point discovered with the actual authorized access points defined by the organization.
- **Network devices & Access point configuration review:** Evaluation of the configurations of a sample of wireless network devices (access points inclusive) in comparison to industry best practices.

- **Review of Wireless Network Management:** Thorough evaluation of the current wireless network management process in place, such as encryption key management and hardware or software maintenance, in comparison to industry best practices.

3.3 Data collection

Five different methods were used for data collection and these included; interviewing key informants in the organization, observation together with experimentation, questionnaires and case study.

Interviewing / key informants' interviews

This method of data collection involved face-to-face interaction with the respondents and asking them questions in line with the study topic; their response were later analyzed & processed. This involved identifying key informants or personalities in the organization. The target group here included among others, both the users who interact very closely with the system & the "technical personnel" – Systems Administrators.

Observation together with experimentation

This method involved the actual use of the eyes to see the conditions prevailing in the current system, doing some experiments on an implemented WLAN and observing the outcome.

3.3.1 Evaluation methods used

- Meeting with the wireless LAN administrators and users; to assess awareness levels, employee expertise, and strength of the security measures in place.
- Performed external scanning of the wireless network to illustrate the ease with which unauthorized persons could intercept wireless signals.

- Performed traffic analysis to see if sensitive data is being transmitted, if transmissions are encrypted and how vulnerable the network is to attacks.
- Performed a complete internal scanning and physical inspection, to verify the source signals.
- Reviewed network topology to assess connectivity to wired network and determine measures to protect the wireless network from the wired network.

3.3.2 Evaluation Tools

- Hardware
  - Laptop
  - Wireless network card
  - Antenna
  - Global Positioning System (GPS) device
- Wireless sniffing software
- WEP encryption cracking software
- Mapping software
- Traffic monitoring software

3.3.3 Security Analysis Tools used for the Experiment

- **AirSnort** is a wireless LAN (WLAN) tool that recovers encryption keys. It operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. AirSnort works for both 40 and 128 bit encryption (http://freshmeat.net/projects/airsnort/; http://www.dachb0den.com/projects/bsd-airtools.html).

- **WEPCrack** is a tool that cracks 802.11 WEP encryption keys using the latest discovered weakness of key scheduling (Fluhrer, et al, 2001; Sourceforge, 2005).

- **Network Stumbler** scans for networks roughly every second and logs all the networks it runs into--including the real SSIDs, the AP's MAC address, the best signal-to-noise ratio encountered, and the time you crossed into the network's space. If you add a GPS receiver to the notebook, it logs the exact latitude and longitude of the AP. Network Stumbler does not use promiscuous mode. Thus, by simply turning off broadcast pings hides the Access Point from NetStumbler (http://www.netstumbler.com/;http://www.netstumbler.com/download.php "Pock etPC MiniStumbler").
- **Internet Scanner** assesses many 802.11b security checks. This is done by doing analyzing via the wired network and contacting the management interface.
- **Wireless Scanner** examines 802.11b security issues via the 802.11b airwaves. Has a penetration testing mode and discovery mode. Uses promiscuous mode, thus capable of capturing the raw 802.11b packets for forensics analysis and replay. Even if broadcast pings are turned off, Wireless Scanner will still catch any Access Points if it sends any kind of traffic due to using promiscuous mode (http://www.iss.net/download/ - "Evaluation copy of Wireless Scanner"; https://iss.custhelp.com/cgi-bin/iss.cfg/php/enduser/home.php "WS Knowledge Base").

- **RealSecure**, monitors many 802.11b attacks. Recommend putting Intrusion Detection and Intrusion Prevention behind the Access Point, directly on any servers and desktops behind the access point, as well as, on any wireless clients.
- **BlackICE PC Protection 3.5**, personal firewall with Intrusion Protection capability, is used on wireless laptops and desktops to protect against client to client attacks.

- **nmap** (which stands for network mapper) supports these scan modes:
  - Vanilla TCP connect scanning

- TCP SYN (half open) scanning
- TCP FIN, Xmas, or NULL (stealth) scanning
- TCP ftp proxy (bounce attack) scanning
- SYN/FIN scanning using IP fragments (bypasses some packet filters)
- TCP ACK and Window scanning
- UDP raw ICMP port unreachable scanning
- ICMP scanning (ping-sweep)
- TCP Ping scanning
- Direct (non port-mapper) RPC scanning
- Remote OS identification by TCP/IP fingerprinting
- Reverse-id scanning

If one way doesn't get any information, another way might. These kinds of port scans are fairly classic, with the exception of Remote OS Identification by TCP/IP Fingerprinting. It identifies the OS of a target through TCP/IP packet analysis (Ray, et al, 2005). This form of attack by scanning may yet make some wide ripples in the security pool.

3.4 Case Study

A big percentage of international organizations carry out their operations over WLANs in recent years. Internet presence for most organizations has posed a high degree of vulnerability to most of these organizations, since they have to link their wireless LAN to the existing wired infrastructure so that those in the field or off the office building, can still gain access to the network.

One such organization was taken during this research as the case study. The United Nations World Food program (UNWFP).

This section presents an evaluation of the existing wireless network. The case study evaluation finding is presented in a parallel manner with the results analysis that was done at the conclusion of this research. This allowed comparisons between the experimental and observational results and all incidents projected in

the problem statement of this project report. W.F.P is a United Nations front line agency in the fight against global hunger. The organization has a UGANDA country office located in Kampala with branch offices found in about 15 districts. One of the branch offices Tororo, served as the study site during this research.

3.5 Handling data collected

Setting a clear policy; In addition to the technical solutions implemented, security policy documentation was done; setting a policy means making security priorities clear to employees. For instance, they must be told clearly that it is not okay to stop by any electronic shop and pick up a wireless access point to plug into the Ethernet port at the office. Doing so creates rogue access points that are outside the realm of the organization /enterprise's security infrastructure and can lead to lost data. The bookend to a clear security policy is enforcement. This means having the right tools on hand to test for the presence of rouge access points.

Another important step to have in place is strong policy control on the network side, and different levels of access must be established for different people using the WLAN.

3.5.1 Data Processing

Statistical Package for Social Scientists (SPSS) statistical data analysis software tool; was used to process quantitative data. Qualitative data which were based on opinions expressed by the respondents, observation and experiments, was analyzed by a method developed by the researcher in order to arrive at a conclusive result.

3.5.2 Content Analysis

- Characterization of data on the network
- View of potential vulnerabilities
- Determine appropriate network use
- Assist in review of policy conformance

Chapter 4: DATA PRESENTATION AND ANALYSIS

4.1 INTRODUCTION

In order to evaluate the security options for WLAN, an experimental test bed was setup. This test bed was implemented to carryout experiments that could allow evaluation of existing security solutions for WLANs and compare the case study WLAN environment to the Industry standards.

An important aspect of this project involves evaluating the case study WLAN security, therefore, a test bed was required to evaluate the WLAN in the presence of conflicting standards.

This chapter presents the analyses from questionnaires, interviews and observation. It also describes the implementation of the experimental test bed which was setup in order to evaluate the various WLAN security solutions in existence (use) and the results that were derived from the experiments.

It also presents the information extracted from data collected during the study and the analysis that was derived from the various findings.

Section (4.2), describes results from the site observation, Section (4.3) describes the statistical analysis derived from questionnaire, section (4.4), explains the experimental wireless network test-bed setup to assess security options such as WEP with an illustration on how easy it is to crack some of the wireless LAN security options currently used by the organization, section (4.5), presents findings from the interview session with systems administrators and lastly a description of a security design solution is in section (4.6).

Wireless Network Test-bed Setup

A test network was setup in order to perform experiments to compare WLAN security solutions with industry standards.

The main components of this network were therefore wireless stations with wireless network cards, and a wireless access point. (See section 4.4).

4.2 Site Observation Results.

In carrying out the survey methodology of topology review, an observation session was done. An assessment of the current infrastructure and security precaution being used was completed.

This section sought to address the following objectives:

- Assess the organizational procedure for use of WLAN.
- To investigate security needs for the organization's wireless network as well as applications used over the network.

4.2.1 WFP Tororo WLAN general network structure

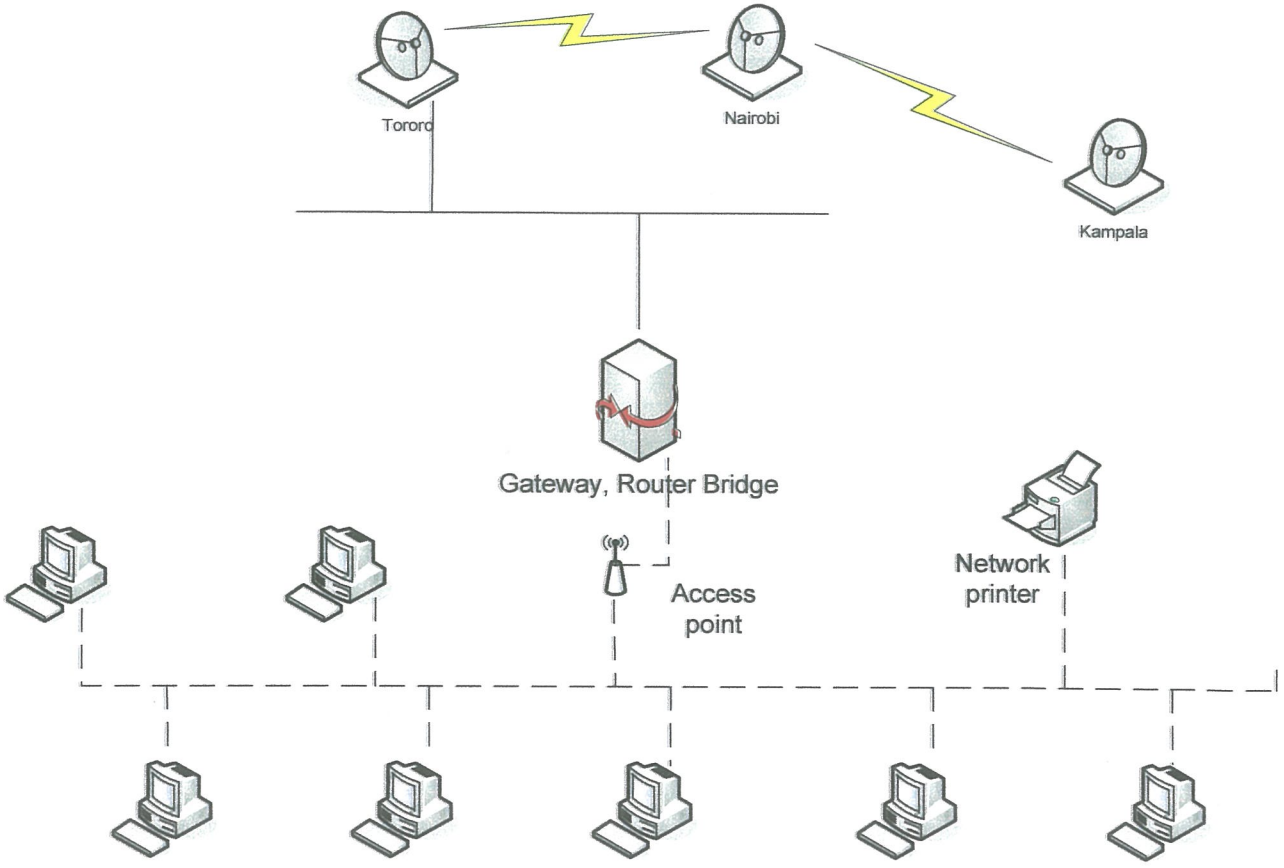


Figure 4.1: Tororo wireless network layout

Figure 4.2: Office setup on Wireless connectivity.

Site survey of the Tororo WFP logistics office reveals the wireless LAN connectivity shown above. This is just a cross-section of the entire wireless local area network in that particular office.

Other WLAN details observed:

- Very Small Aperture Terminal (VSAT) OUTDOOR UNIT - **(See Appendix A)**
- Very Small Aperture Terminal (VSAT) INDOOR UNIT - **(See Appendix A)**
- UUPLUS Server - **(See Appendix B)**
- Linksys Wireless-G Access Point Connected To Power - **(See Appendix C)**
- Linksys Wireless-G PCI Adapter on a Workstation - **(See Appendix C)**
- A Typical Office Setup - **(See Appendix D)**

4.3 Case Study Findings:

The wireless LAN currently being used by the organization is LINKSYS. The wireless LAN products provided by LINKSYS are of high quality, reliable and in general provide stable operating software.

Nevertheless it is often suggested to upgrade the new devices such as; Access points, the PC card, and all other Wireless LAN products involved; as they come available, in order to take advantage of the latest features the product can offer Devices.

This section seeks to answer the following research questions and objectives:

What is the WFP user awareness level of WLAN security solutions and options?
What is the WFP WLAN security solution policy?
What is the WFP WLAN security solutions user procedure?

- Assess organizational awareness of WLAN security and their options
- Assess the organizational policy of deploying WLAN

In order to answer the above research questions, questionnaires were design for the different categories of respondents. Below are the findings of the questionnaires.

4.3.1 Users' Questionnaire Results

This section presents the analysis derived from the questionnaires that were filled by WFP WLAN users and system administrators. It seeks to solve the following research objective:

- To assess organizational awareness level of WLAN security and their options
- Assess the organizational policy of deploying WLAN
- Assess the organizational procedure for use of WLAN.

Users' Questionnaire Results

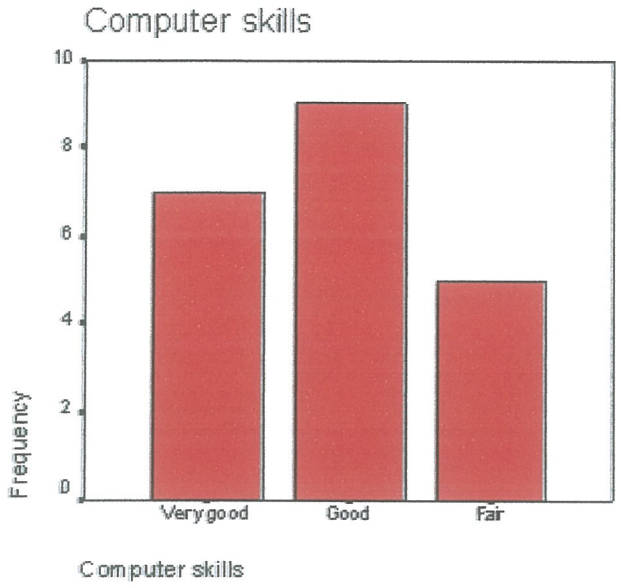


Figure 4.3: Assessment of WLAN Users' computer skills

Computer skill is crucial in assessing user awareness level of WLAN security options and therefore it is one of the parameters that were deemed to affect security of the WLAN. Statistics showed that a big percentage (40.9%) of the users have good computer skills, hence pointing to a high positive response to security policies that may need to be put in place concerning their activity on the WLAN. Studies have shown that, a user with good computer skills is more likely to follow procedure than one without.

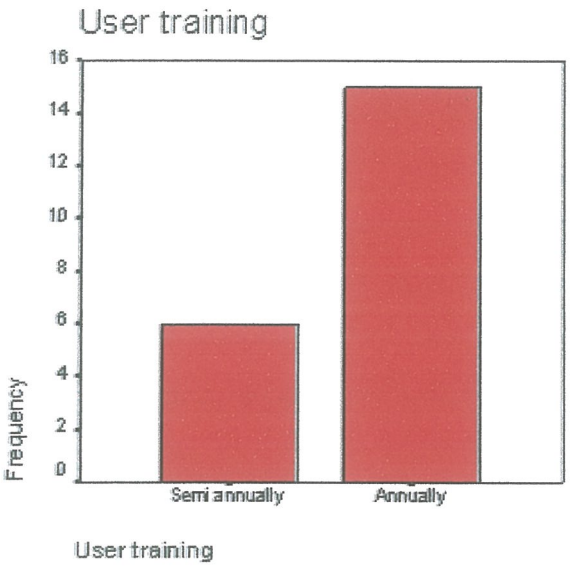


Figure 4.4: Level of User Training

Gauging from the graph, user training is done annually for most of the respondents whereas semi annual training is done for cases when there is a change in the system that users need to be trained in order to use.

This case implies that with a high level of user training the organization is likely to attain a secure WLAN environment, since users are trained regularly; it is easier to deduce that trained user would find it easier to follow the security policies and procedures put in place.

This increase the chances that most of the users are aware of the security implications of these training sessions, and may put its content to good use.

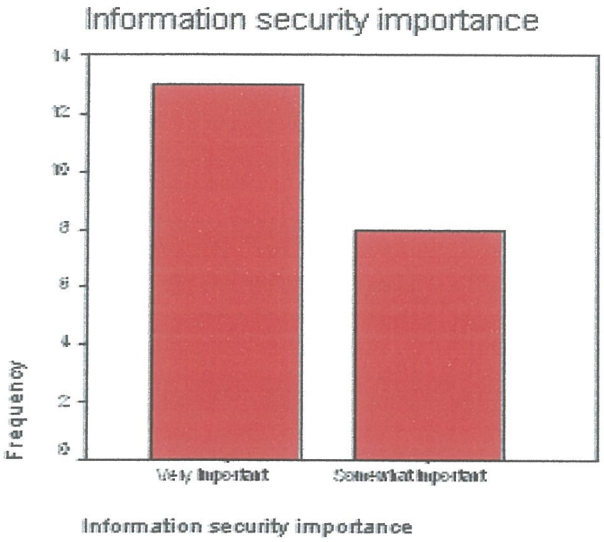


Figure 4.5: Importance of Information Security

Deducing from the users' response, regarding the level of information security importance, more than half of the respondents (59.1%) deem information security to be very important. Therefore, as system users, they would be careful not to expose the organization's information. This also means that the user activity will be in a manner that safeguards information transmitted on the WLAN.

This show a high level of security awareness with regard to information held or transmitted over the WLAN.

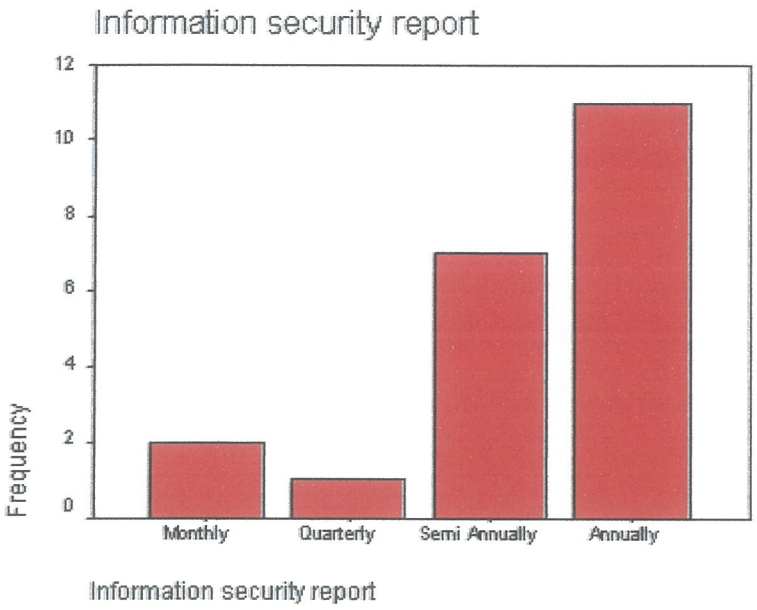


Figure 4.6: Review of Information Security Reports

Frequent review of overall information security status is very important for purposes of monitoring and improvement of a security system, hence information reports would be very necessary for a more structured mode of security status evaluation, and in the long run, these reports act as a tool to guide management decisions concerning the entire system security. Logically, a fairly frequent security assessment helps the organization to be able to identify any irregularities or anomalies that have to be dealt with before they become intrusion points for any attacker.

Data collected suggests that from 50% of users' point of view, information security reports are usually submitted by systems Administrators annually.

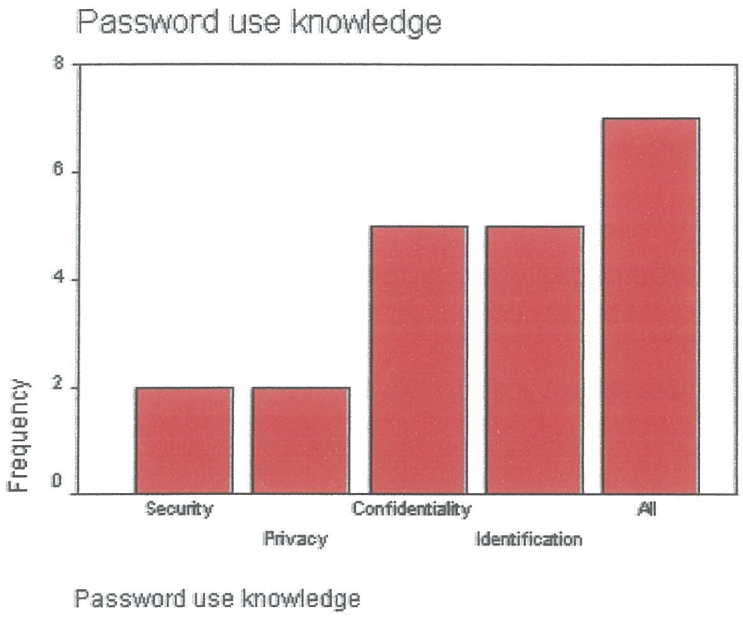


Figure 4:7: Awareness level in password use

Password being the most basic security a system can have, the knowledge of it's use is security awareness at the most basic level. A user must know its use to be able to safe guard it from password theft. It is more likely that a user, who is aware of the dangers and implication of loosing or exposing their password to any other person whether s/he is an authorized system user or not, will be more careful with it.

The findings show that 32% of respondents use their passwords for all (Security, privacy, confidentiality and Identification) purposes. The rest of them use their passwords for each of the individual purpose as mentioned above.

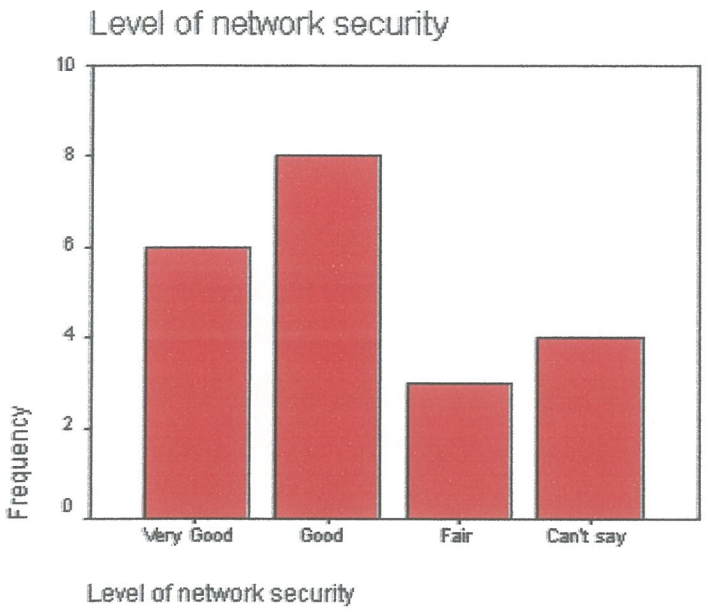


Figure 4.8: Level of Network Security

Statistics show that more than half of the users esteem the level of security of the network to be very good (27.3%) and good (36.4%) respectively. They believe that the current security solution is secure enough for them to store their personal confidential data.

Some had undisclosed reasons to think the network is secure to a satisfactory level, and have never considered an intrusion incident or any attack.

This shows some degree of awareness about network security and its importance to their activities and organizational missions.

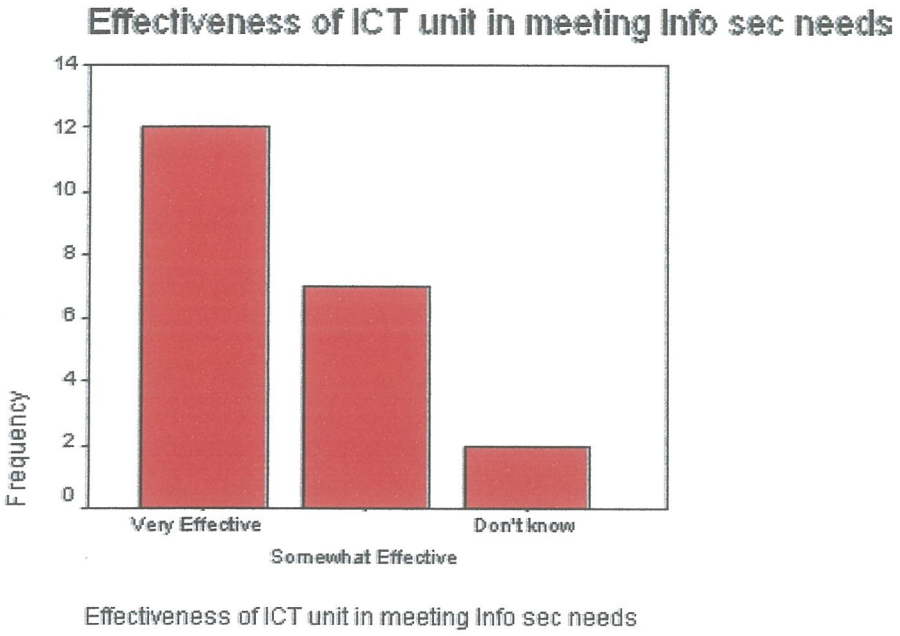


Figure 4:9: Effectiveness of ICT unit in meeting Information Security Needs

54.5% of the respondents think ICT unit is very effective in meeting their information security needs. Whereas 31.8% seemed to think that the unit in charge of network and information security is somewhat effective in meeting their information security. This could be due to a number of reasons ranging from personal to experience and level of technical knowledge about the issues surrounding WLAN security. Most respondents who had good computer skills do not entirely trust the network security. Indicating a moderate degree of level of awareness of how the ideal security should really be.

4.3.2 Systems Administrators' Questionnaire results

Out of the seven questionnaires given to the administrators, five of them were answered and returned. The results analyses from the five respondents are presented as follows:

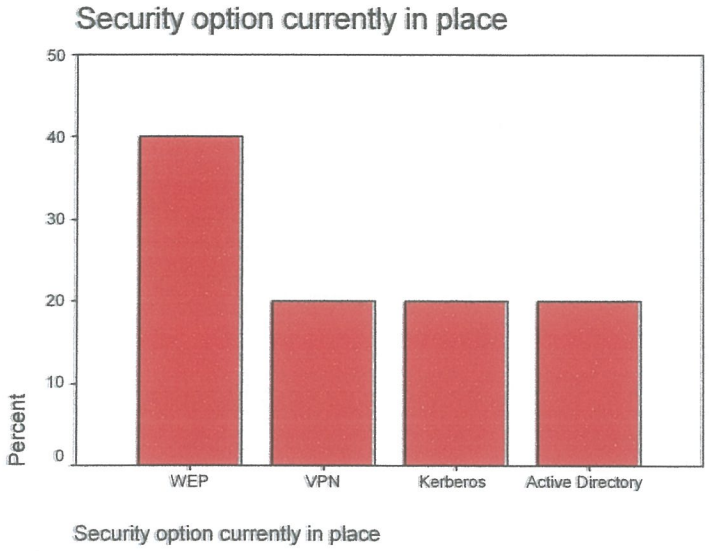


Figure 4.10: WLAN Security solution currently in place

40% of the respondents say the security solution mostly used is WEP in combination with other security solutions that come to play from the network operating system software being used by the organization. Active Directory is used in this context as a result of Windows 2000 server network infrastructure implementation. Virtual network connection is implemented for users who login to the network remotely, for a secure network access.

The use of the different security solutions indicate that the systems administrators are well aware of the various wireless LAN security options that can be implemented in the organization's WLAN.

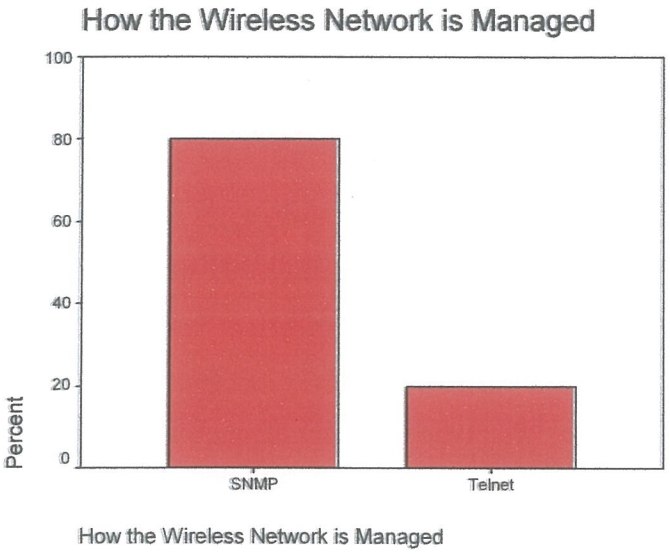


Figure 4.11: Wireless Network Management Procedure

80% say the network is managed using simple network management protocol (SNMP); whereas 20% say remote administration is done using Telnet protocol. This implies that the major management tasks are done using SNMP rather than telnet. This shows that there is probably no consideration for a possibility of SNMP session hijack that could occur. For high levels of security precautions, telnet should not be used at any one time for administration to avoid the session hijack attacks.

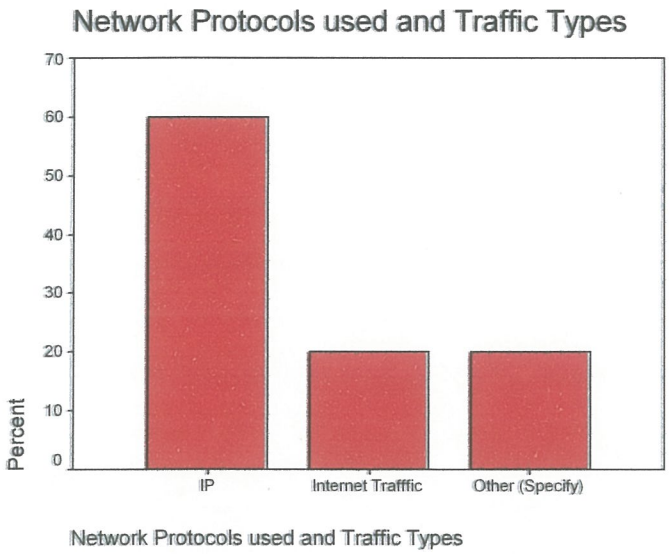


Figure 4.12: Types of Network traffic and Protocols used

60% said Internet protocol is mostly used and 40% said, nature of network traffic include among others, Internet traffic. This implies that the level of security used should be high enough to counter block the degree of exposure the network is subjected to through the Internet. With IP being used, there is very little done in terms of use of security related protocols.

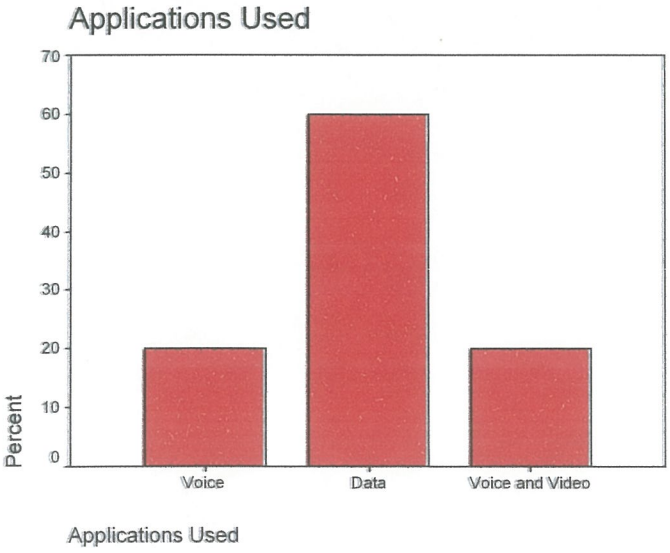


Figure 4.13: Types of Applications used on the WLAN

The type of application used on the network is one of the factors that dictate the type of security solution to be used. In this case, 60% of the applications used a basically for data processing or transfer. 40% is for voice, voice and video collectively. This shows that the administrators are aware that the application used over the WLAN can be successfully secured by the particular security solutions currently being used.

4.4 EXPERIMENTAL TEST-BED RESULTS

In order to evaluate the security options for WLAN, an experimental test bed was setup. This test bed was built to carryout experiments that could allow evaluation of existing security solutions for WLANs and compare the case study WLAN environment to the Industry standards.

An important aspect of this project involves evaluating the case study WLAN security, therefore, a test bed was required to evaluate the WLAN in the presence of conflicting standards.

This section describes the creation of the experimental test bed which was setup in order to evaluate the various WLAN security solutions in existence (use).

It also presents the information extracted from data collected during the study and the analysis that was derived from the findings.

Section (4.4.1) describes the experimental wireless network setup, the subsequent sub-sections (4.4.2, 4.4.3) present the various screen shots from the experiments and their respective explanations, for the external and internal network scans done in order to evaluate the level of security for the test-bed WLAN acting as the simulation of a basic wireless network infrastructure. (See Appendix F)

4.4.1 Wireless Network Test-bed Setup

A test network was setup in order to perform experiments to compare WLAN security solutions with industry standards. This lab experiment was done to address the following objectives and answer the under mentioned research questions respectively;

Objectives:

- Identify suitable & practical WLAN security configuration solutions that can be effectively used by organizations.
- Design and implement a WLAN; which will be used to carryout investigation & assessment procedures on the various security options identified by the researchers.

- To evaluate the security of the wireless local area network and applications including threats to
    - Data integrity
    - Confidentiality
    - Availability of services and resources

Question addressed:

1. What are the limitations of some of the WLAN security technologies used by WFP?

The main components of this network were therefore wireless stations (3 laptops) with wireless network cards, wireless access points, desktop (1). (See Appendix F)

4.4.2 External network scan

Results from an external scanning of the wireless network performed using "AirSnort" and "aircrack" respectively to illustrate the ease with which unauthorized persons could intercept wireless signals. The out come of the experiment is displayed in the figures below (Figure. 4.14 and Figure. 4.15)

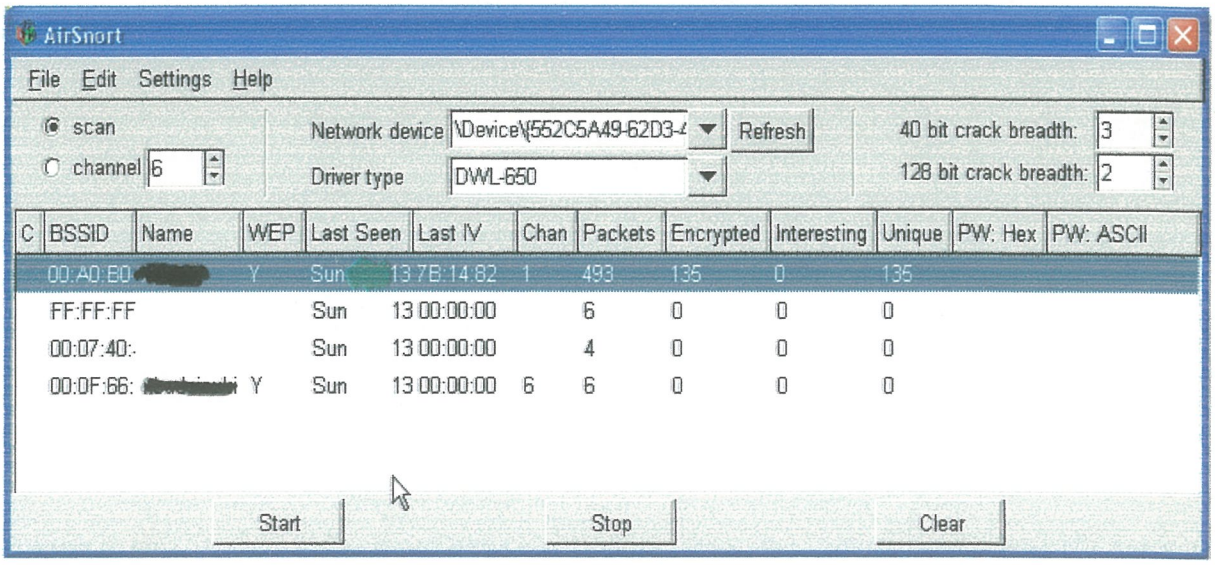


Figure 4.14: Encryption key recovery from a network scan using "AirSnort"

Figure 4.14; shows an illustration of "AirSnort" wireless LAN (WLAN) tool that recovers WEP encryption keys. It operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered.

If a device that uses static WEP keys is lost or stolen, the possessor of the stolen device can access the WLAN. An administrator will not be able to detect that an unauthorized user has infiltrated the WLAN until and unless the theft is reported. The administrator must then change the WEP key on every device that uses the same static WEP key used by the missing device. In a large enterprise WLAN with hundreds or even thousands of users, this can be a daunting task. Worse still, if a static WEP key is deciphered through a tool such as AirSnort (as illustrated above), the administrator has no way of knowing that the key has been compromised by a hacker. Thereby affecting the WLAN security through exposure to vulnerabilities such as;

- Data integrity
- Confidentiality
- Availability of services and resources

This network scan illustrates one of the limitations of WEP WLAN security solution, however it is better than no security at all.

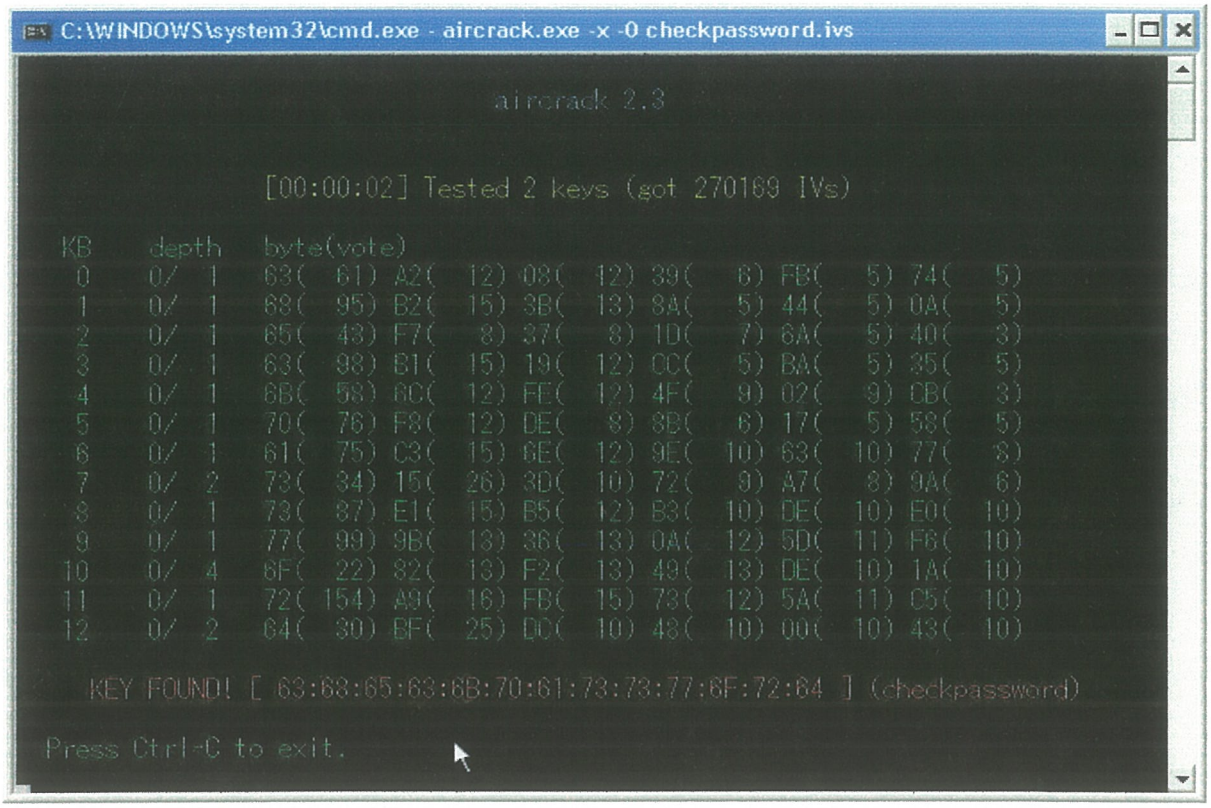


Figure 4.15: Password "Cracking" using aircrack version 2.3

Figure 4.15; illustrates the processing of several keys by any unauthorized intruder using "aircrack" software to try and obtain an authentic password in order to gain access into the network. After running a few trials, the characters in the red line in the figure shows that an authentic key has been found that can be used to gain access into the WLAN.

This experiment illustrated the ease with which an unauthorized user can gain access to valid authentication details such as password belonging to an authorized user in order to gain access to network resources without physically being in the building. Therefore compromising the network and opening it to attacks towards;

- Data integrity
- Confidentiality

4.5 INTERVIEW RESULTS

This section seeks to address the following research objectives:

- Assess the organizational policy of deploying WLAN
- Assess the organizational procedure for use of WLAN.
- Assess management guidelines for selection of WLAN security solutions
- Identify suitable & practical WLAN security configuration solutions that can be effectively used by organizations.

In order to answer the research questions stated below, an interview schedule (See Appendix G) was designed.

What is the WFP WLAN security solution policy?

What is the WFP WLAN security solutions user procedure?

What is the WFP WLAN security solution selection management guideline?

The target respondents for this interview were the systems administrators.

4.5.1 Interview Findings

Table 4.1: Interview findings

Parameter being Evaluated	**Findings**
WEP key, SSID key change schedule	Done yearly
Administrator password change schedule	Not done as frequent as recommended by Industry standards
Separation mechanism of Wireless network from Wired network	Internet service provider (ISP) Firewall
Network scan performed	Not done as recommended by Industry standards

Table 4.1: Con't	
Limiting network access network monitoring	Access is limited by means of username and passwords, enforcing domain related policies, Monitoring is done using SolarWinds network monitoring tool
Security mechanism for data transmission	WEP encryption, MAC filtering
Wireless station operating system	Windows XP, Windows 2000
Access point antenna type	Directional
Antenna transmission power	Moderately powerful
Number of bits supported by the access point	128bits
Users' categories and access rights	Domain security groups – users without administrator rights
Power solutions	UEDCL supply, generators and UPS power backups
Physical security	Security guards, keys and locks, seals
Protection of portable devices from theft	Not yet in place
Access and safety of configuration details	All ICT unit staff have access
Incidents of Information hijack, virus attacks	None, Strong and reliable anti virus software used
Prior assessment done before WLAN installation	Not done, the network was expected to be operational within a very short time for an assessment to be done.
Security management	Centralized
Management decisions	Made based on ICT reports

Table 4.1: Con't	
Monitoring Procedures and policies	Done by none dedicated personnel but developed jointly by all the administrators, documentation of the same is stored in a central server

4.6 WLAN SECURITY DESIGN SOLUTION

The design-solution consists of distributed sensors and server appliances. The remote sensors sit near 802.11 Access Points to monitor all WLAN activities and report back to the server appliance, which analyzes the traffic in real time.

The remote sensors: -

- Are deployed near Access Points;
- Provide round the clock (24x7) monitoring of all WLAN activities;
- Capture wireless traffic from Access Points and stations;
- Report to a back-end server; and
- Are centrally managed.

The sever appliances: -

- Analyze traffic in real time;
- Discover WLANs and rouge deployments;
- Detect intrusions and impending threats;
- Disconnect intruders and protect against attacks;
- Enforce WLAN policies;
- Monitor WLAN performance and troubleshoot network issues;
- Offer a secure web-based interface; and
- Provide comprehensive reporting

4.6.1 Design-solution for wireless LAN security

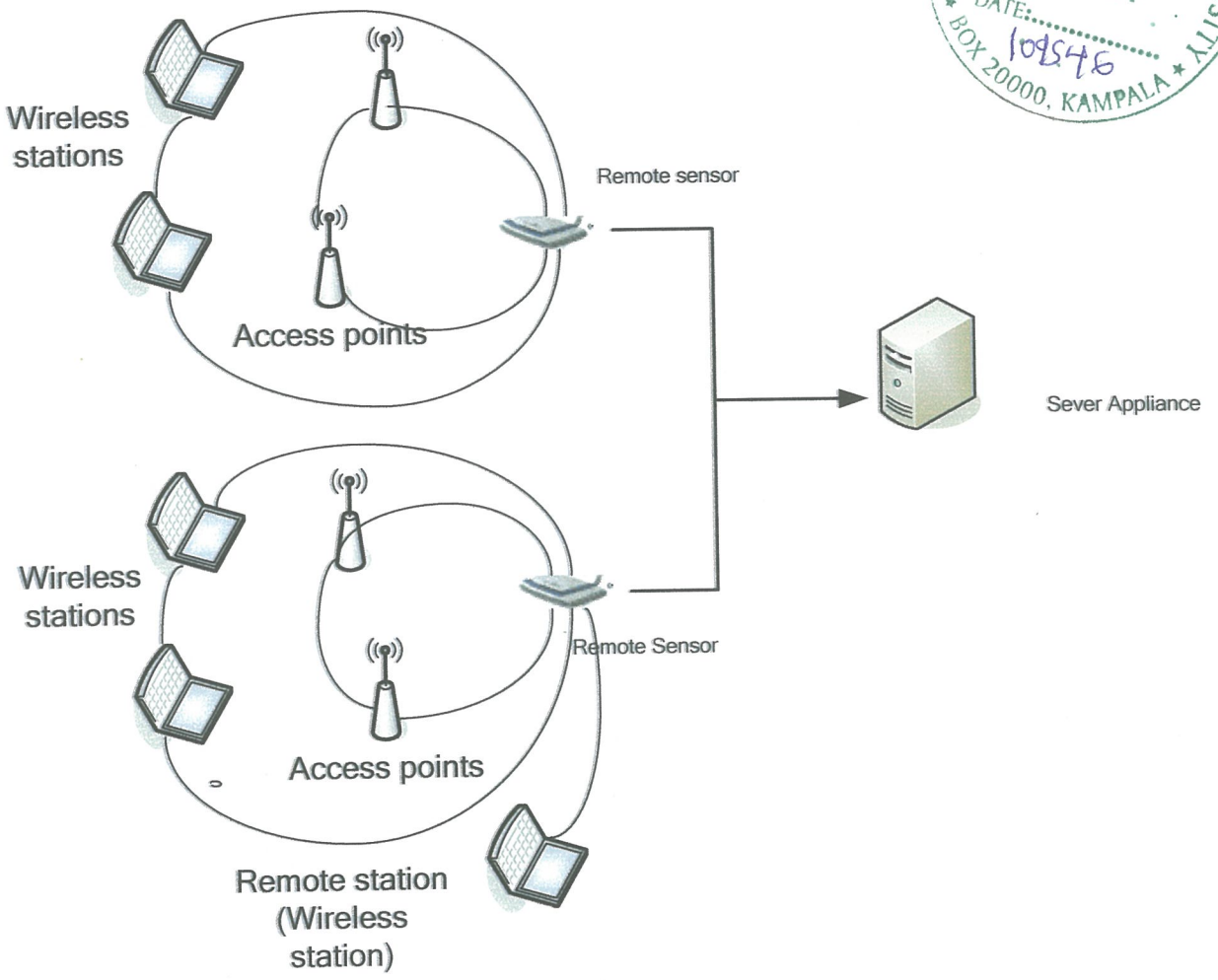


Figure 4.16: WLAN Security solution Design

Chapter 5: CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter contains the conclusion and recommendations for the study.

Section 5.2 concludes the study, Section 5.3, describes the various specific security configuration recommendations that would secure WLANs. Section 5.4, elaborates the various research limitations that were experienced during the study.

5.2 Conclusion

There are many options that organizations can use today to put proper security protection around their wireless strategy and technology. These include putting in place and enforcing security policies, observing WLAN implementation procedures and having clear management guidelines in security solution selection. All these must be properly documented for easy access by concerned persons.

The major problems identified, that affects security of the organizational WLAN are; insufficient security policies enforced and in operation, insufficient practical procedure of WLAN operation. Instead users concentrate on following certain protocols that only work in a wired network environment. Observation revealed good physical security. However, it was also observed that most WLAN device security features are not enabled to serve their purpose.

5.3 General Recommendations

The organization should;

- Develop stronger wireless network policies
- Enforce the developed wireless network policies and procedures
- Conduct risk assessments to determine required level of security
- Limit access to wireless networks through the use of security measures like (802.11i or WPA) as compared to only WEP

- Maintain logical separation between wireless and wired networks using a dedicated firewall rather than ISP firewall
- Perform regular internal and external wireless scans to identify wireless networks devices and applications
- System administrators should change default passwords, network names (e.g. SSIDs) and SNMP community strings that are preconfigured in the factory.
- All system users should change their passwords regularly, and use "difficult to crack" or strong passwords that are not susceptible to "dictionary attacks". Enable "BIOS" passwords and screen saver passwords to prevent unauthorized people accessing wireless LAN configuration parameters such as static WEP keys (if used).
- Use device authorization (dynamic MAC filtering access control) to exclude unwanted wireless stations.
- Change static WEP keys frequently rather than using dynamic keys. Deploy security management products that simplify this process.

5.3.1 Wireless Security Policy and Architecture Design

The Organization needs to develop a wireless security policy to define what is and what is not allowed with wireless technology. From a holistic view, the wireless network should be designed with the proper architecture to minimize risk.

Though establishing policies to govern wireless networks would appear to be a basic requirement, organizations often fail to take this step or to inform employees of the risk associated with not using a wireless network in accordance with the policies. Once policies are implemented, it's critical to communicate them to increase user's awareness and understanding. In turn they can surely take responsibility for their actions.

Organizations should develop institution-wide policies with detailed procedures regarding wireless devices and usage. Maintaining these policies and procedures to keep current with and changing technological trends. While the organization has specific requirements, at the minimum requires the registration of all WLANs as part of overall security strategy. Since a policy is not effective if users are not in compliance, the network should be monitored to ensure that users are following the policy as intended.

Regular security awareness and training sessions should be conducted for both systems administrators and system users. It is very important to keep systems administrators informed of technical advances and protocols, but it is also equally important for system users to understand the reasons for the protocols. An educated user will more likely be a compliant one, without as much protest as one who is not educated. The importance of vigilance should be highly stressed during these education or training sessions.

5.3.2 Basic Field Coverage

Due to wireless signal leakage, one of the first principals to basic field coverage is to only provide coverage for the areas that need to have access. By using directional antennas and lowering the transmit power (on commercial class equipment - i.e., Cisco and Lucent), 85% (or higher) of the typical 802.11 signal leakage can be effectively eliminated.

5.3.3 Treat Base Stations (AP) as Un-trusted

Judging from the case study's network security architecture, the base stations should be evaluated and determined if it should be treated as an untrusted device and need to be quarantined before the wireless clients can gain access to the internal network. The architecture design may include a Wireless DMZ. This WDMZ includes appropriately placing firewalls, VPNs, IDSes, vulnerability assessments, authentication requirements between access point and the Intranet.

5.3.4 Base Station (AP) Configuration Policy

The wireless policy being developed may need to define the standard security settings for any 802.11 base station being deployed. It should cover security issues like the Server Set ID, WEP keys and encryption, and Simple Network Management Protocol (SNMP) community words. Turning off broadcast pings on the Access Point makes it invisible to 802.11b analysis tools like NetStumbler.

The NetGear Access Point uses the following 4 WEP sequences as default keys.

- 10 11 12 13 14
- 21 22 23 24 25
- 31 32 33 34 35
- 41 42 43 44 45

It is recommended that you do not use the default WEP keys.

Each of the base station models come with default SSIDs. Attackers can use these default SSIDs to attempt to penetrate base stations that are still in their default configuration. Listed below are some default SSIDs:

- "tsunami" - Cisco
- "101" – 3Com
- "RoamAbout Default Network Name" - Lucent/Cabletron
- "Default SSID"
- "Compaq" - Compaq
- "WLAN" – Addtron, a popular AP
- "intel" - Intel
- "linksys" – Linksys
- "Wireless"

Access point security recommendations:

- Enable centralized user authentication for the management interface.
- Choose strong community strings for Simple Network Management Protocol (SNMP) and change them often.

- Consider using SNMP Read Only if the management infrastructure allows it.
- Disable any insecure and nonessential management protocol provided by the manufacturer.
- Utilize secure management protocols, such as Secure Shell Protocol (SSH).
- Limit management traffic to a dedicated wired subnet.
- Isolate management traffic from user traffic and encrypt all management traffic where possible.
- Enable wireless frame encryption where available.
- Physically secure the access point.

5.3.5 802.1X Security

Windows XP and many hardware vendors are building in 802.1X security standards into their Access Points. This provides a higher level of security than the typical WEP security. The 802.1x standard has a key management protocol built into its specification which provides keys automatically. Keys can also be changed rapidly at set intervals. Checks to see if the Access Points support 802.1X.

There have been some security flaws noted by security researches in 802.1X standard. These point out the need for good VPN technology despite this new standard.

5.3.6 MAC Address Filtering

Some Access Points have the ability to filter only trusted MAC addresses. MAC addresses are supposed to be unique addresses on the network. This feature is usually very difficult to implement in a dynamic environment due to the tedious nature of trying to configure AP for each and every trusted client. The MAC address is transmitted in the clear text, so any intruder can sniff authorized MAC addresses, and with proper tools, configure and masquerade their MAC address

as a legitimate MAC address and by-pass this security mechanism. Enabling this security feature can be more effort than the actual security benefit that it provides.

5.3.7 Base Station (AP) Discovery

- From a wired network search, an organization could identify unknown and rogue base stations by searching for Simple Network Management Protocol (SNMP) agents. The rogue base stations are identified as 802.11 devices through SNMP queries for host id.
- Some base stations have a web and telnet interface. By looking at the banner strings of these interfaces, this provides another method of identifying some 802.11 devices.
- An additional means is by using unique TCP/IP attributes like a fingerprint, it can help identify devices as base stations. Most TCP/IP implementations have a unique set of characteristics and many OS fingerprinting technologies use this method for identifying the OS type. This concept can be applied to the base stations.
- From a wireless network search, an organization should identify these rogue base stations by simply setting up a 2.4 GHz sniffers that identifies 802.11 packets in the air. By looking at the packets, you may find the IP addresses to help identify which network they are on. In a densely populated area with many businesses close together, running a sniffer may pick up more than the intended organization's traffic, but a close neighboring company.

5.3.8 Base Station Security Assessments

The organization should examine and analyze the base station configuration. A security audit and assessment determines whether the passwords and community words are still default (see section 5.2.3) or easily guessed and if better security modes have been enabled like encryption.

With the use of router Access Control Lists (ACLs) and firewall rules, the organization can minimize access to the SNMP agents and other interfaces on the base station. A security assessment determines how widely accessible the configuration interfaces to the base stations are allowed to within the organization.

5.3.9 Wireless Client/Station Protection

The wireless clients/stations should be assessed for having the following security technologies:

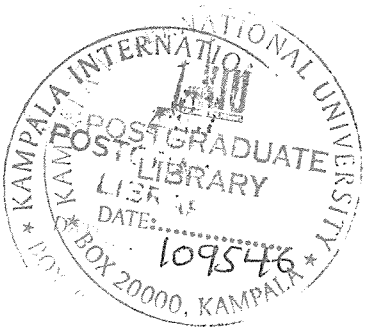
- Fire-cell (distributed personal firewalls) - lock down who can gain access to the client.
- VPN - adds another layer of encryption and authentication beyond what 802.11 can provide.
- Intrusion detection - identifies and minimizes attacks from intruders, worms, viruses, Trojans and backdoors.
- Desktop scanning - identify security misconfigurations on the client.

Client security recommendations:

- Disable ad hoc mode.
- Enable wireless frame encryption where available.

5.4 Research Limitations

- Shortage in evaluation resources due to insufficient facilitation.
- Organization's inability to avail information to the researcher due to the sensitivity of the research topic
- Limited time availed to the interviewer by the organization (contact time between interviewer & respondent due to work schedules and organization's restrictions)



REFERENCE

[1] Altunbasak, H. Owen, H. (2004, March). *Alternative Pair-wise Key Exchange Protocols for Robust Security Networks (IEEE 802.11i) in Wireless LANs.* SoutheastCon,.Proceedings. IEEE, pp 26-29, pp 77 – 83.

[2] Anonymous, (2003, March). 'Wireless networks grow dramatically, but security remains a problem, report says', *Electronic Commerce News*, **8**.

[3] Arbaugh, W. A., (2002, Dec). *An Inductive Chosen Plaintext Attack Against WEP and WEP2.*IEEE 802.11 Working Group, Task Group I (Security).

[4] Arbaugh, W.A. (2003, Aug). *Wireless security is different.* Computer, (Volume: 36), Issue: 8, pp 99 – 101.

[5] Arbaugh, W.A., Shankar, N., Wan, Y.C.J. and Zhang, K. (2004). *Your 802.11 Wireless Network Has No Clothes.* IEEE Wireless Communications, pp 44-51.

[6] Berghel, H., and Uecker J. (2004). 'Wireless Infidelity I: War Driving', *Communications of the ACM*, **47** (9), pp 21-26.

[7] Borisov, N., Goldberg, I. and Wagner, D. (2001). *Intercepting Mobile Communications: The Insecurity of 802.11.* 7th Annual International Conference on Mobile Computing and Networks, Rome, Italy.

[8] Buchholz, J. (2003). *Mathlab Implementation of the Advanced Encryption Standard.* http://buchholz.hs-bremen.de/aes/aes.htm

[9] Burr, W.E. *(*2003, Mar-Apr), *Selecting the Advanced Encryption Standard.* Security & Privacy Magazine, IEEE. Volume 1, Issue 2, pp 43 – 52.

[10] Candolin, C., and Kari, H.H. (2002, Oct). *A security architecture for wireless ad hoc networks.* MILCOM 2002 Proceedings, (Volume: 2). pp1095 – 1100.

[11] Carl, Weinschenk, (2003, March). "*Keep pace with WLAN security developments" TechRepublic*

[12] Carli, M., Rosetti, A., and Neri, A. (2003, 23 Feb.-1 Mar) *Integrated security architecture for WLAN.* Telecommunications, ICT, (Volume: 2), pp 943 – 947.

[13] Chlamtac, I., Conti, M., and Liu, J. (2003) *Mobile Ah hoc networking: imperatives and challenges.* Ad Hoc Networks I, Elsevier BV, pp 13-64.

[14] Coulouris, G., Dollimore, J., and Kindberg, T. (2001). Distributed Systems, Concepts and Design. Addison Wesley, Harlow England, third edition, pp 41-47.

[15] Dave Molta, (2004). *Networking Computing, pp 41-43.*

[16] David Halasz, Sean Convery (CCIE #4232), Darrin Miller (CCIE #6447), and Sri Sundaralingam. (2005, September). *Cisco SAFE: Wireless LAN Security in Depth.* http://www.cisco.com/go/safe, http://www.cisco.netacad.net, Accessed on March 2006.

[17] Dyce, K. (2005). *A Wireless Vulnerability Assessment Framework: A developed prototype wireless vulnerability assessment framework and a study into their use in the real world.* Unpublished Honors thesis, University of Wollongong.

[18] Erten, Y.M. (2004, May). *A layered security architecture for corporate 802.11 wireless networks.* Wireless Telecommunications Symposium, 2004, pp 123-128.

[19] Feil, H. (2003). *802.11 Wireless Network Policy Recommendation For Usage Within Unclassified Government Networks.* The Aerospace Corporation, pp 832-838.

[20] FIPS-197. (2001). *Advanced Encryption Standard (AES).* http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

[21] Fluhrer, S., Shamir, A. and Mantin, I. (2001). *Weaknesses in the Key Scheduling Algorithm of RC4.* Selected Areas of Cryptography, Toronto, Canada.

[22] Gupta, V. and Gupta, S. (2001, Dec). *Securing the wireless internet.* Communications Magazine, IEEE , Volume: 39 , Issue: 12, pp 68 – 74.

[23] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, Lixia Zhang. (2004, Feb). *Security in mobile adhoc networks: challenges and solution.*, Wireless Communications, IEEE, Volume: 11, Issue: 1, pp 38 – 47.

[24] Henning, R. R. (2003), *Vulnerability Assessment in Wireless Networks*, Harris Corporation, [Available Online: http://www.cs.nmt.edu/~cs553/paper15.pdf], Accessed 5 January 2006.

[25] Housley, R., and Arbaugh, W. (2003, May). 'Security Problems in 802.11-based Networks', *Communications of the ACM*, **46** (5), pp 31-34.

[26] *IDC, (2005)* "The Basics of 802.11 Wireless LANs" *Published Aug*

[27] *IEC, (2005),* "Worldwide WLAN Management 2005-2009 Forecast and Analysis" *Published Aug*

[28] IEEE P802.11 Task Group I, (2004). *Status of Project IEEE 802.11i.* http://grouper.ieee.org/groups/802/11/Reports/tgi_update.htm

[29] Jamil, T. (2004, April-May). *The Rijndael algorithm.* Potentials, IEEE Volume 23, Issue 2, pp 36 – 38.

[30] Lee, C.K.L., Xiao-Hu, L., and Yu-Kwong, K. (2003, 11-15 May). *A multipath ad hoc routing approach to combat wireless link insecurity.* Communications, 2003. ICC '03. IEEE International Conference, Volume: 1, pp 448 – 452.

[31] Lidong Zhou, Haas, Z.J. (1999, Nov.-Dec). *Securing ad hoc networks.* Network, IEEE, Volume: 13, Issue: 6, pp 24 – 30.

[32] Light Reading Wireless Oracle, (2003, March). *802.11 Security Checkpoint.*, Vol.2, No.3.

[33] Motorola, (2006, May). *WS Building a secure foundation for Enterprise Mobility, pp 4 – 11.*

[34] Nichols, R. K., and Lekkas, P. C. (2002). *Wireless Security: Models, Threats and Solutions*, New York: McGraw-Hill.

[35] Peltier, T. R., Peltier, J. and Blackley, J. A. (2003) *Managing a Network Vulnerability Assessment*, Auerbach Publications, USA.

[36] Potter, B. (2003, July-Aug). *Wireless security's future.* Security & Privacy Magazine, IEEE, Volume: 1, Issue: 4, pp 68-72.

[37] Ray Zeisz, Matt Keil, & Jae Lee, (2005). "Secure Wireless Networks for Distributed Remote Sites" Juniper Networks, http://www.juniper.net, Accessed on March 2006

[38] Research & Consultancy Outsourcing Svcs. (2005) *"Wireless LAN Security-An Industry Outlook"*

[39] Sanchez-Avila, C., and Sanchez-Reillol, R. (2001). *The Rijndael block cipher (AES proposal): a comparison with DES.* Security Technology, 2001 IEEE 35th International Carnahan Conference. pp 229 – 234.

[40] Shimonski, R. (2002). *Security+ Study Guide and DVD Training System.* Syngress Publishing, MA, First Edition, pp 159-219.

[41] Stallings, W. (2003). *Cryptography and Network Security: Principles and Practices*. Pearson Education, Inc., NJ, Third Edition.

[42] Sun Microsystems, Inc. (2005). *Crypto-Politics: Decoding the New Encryption Standard*. http://research.sun.com/features/encryption/

[43] Tanenbaum, A.S. (2003). *Computer Networks.* Prentice Hall, NJ, Fourth Edition, pp 738-741.

[44] The IEEE Computer Society. *Part 11: (*2004). *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications.* IEEE Standard 802.11i.

[45] *The Wall Street Journal,* (2001 April 27), Accessed on Dec. 2005.

[46] Tiller, J. S. (2005). The Ethical Hack: A Framework for Business Value Penetration Testing, Auerbach Publications, USA.

[47] Walker, J. (2000). *Unsafe at Any Key Size: An Analysis of the WEP Encapsulation.* IEEE 802.11 Task Group E.

[48] Wang Shunman, Tao Ran, Wang Yue, and Zhang Ji. (2003, 27-29 Aug). *WLAN and its security problems.* Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003. Proceedings of the Fourth International Conference on, pp 241 – 244.

Internet Resources

[49] http://www.AirDefense.net, 2005

[50] (http://www.blackalchemy.to/Projects/fakeap/fake-ap.html)

[51] http://www.broadbeam.com, September 2004.

[52] http://www.computereconomics.com/

[53] http://www.dachb0den.com/projects/bsd-airtools.html

[54] http://freshmeat.net/projects/airsnort/,

[55] http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html

[56] http://www.iss.net/download/ "Evaluation copy of Wireless Scanner"

[57] https://iss.custhelp.com/cgi-bin/iss.cfg/php/enduser/home.php "WS Knowledge Base"

[58] http://www.netstumbler.com/, http://www.netstumbler.com/download.php PocketPC MiniStumbler

[59] http://sourceforge.net/projects/wepcrack

[60] http://www.webopedia.com/TERM/n/network.html

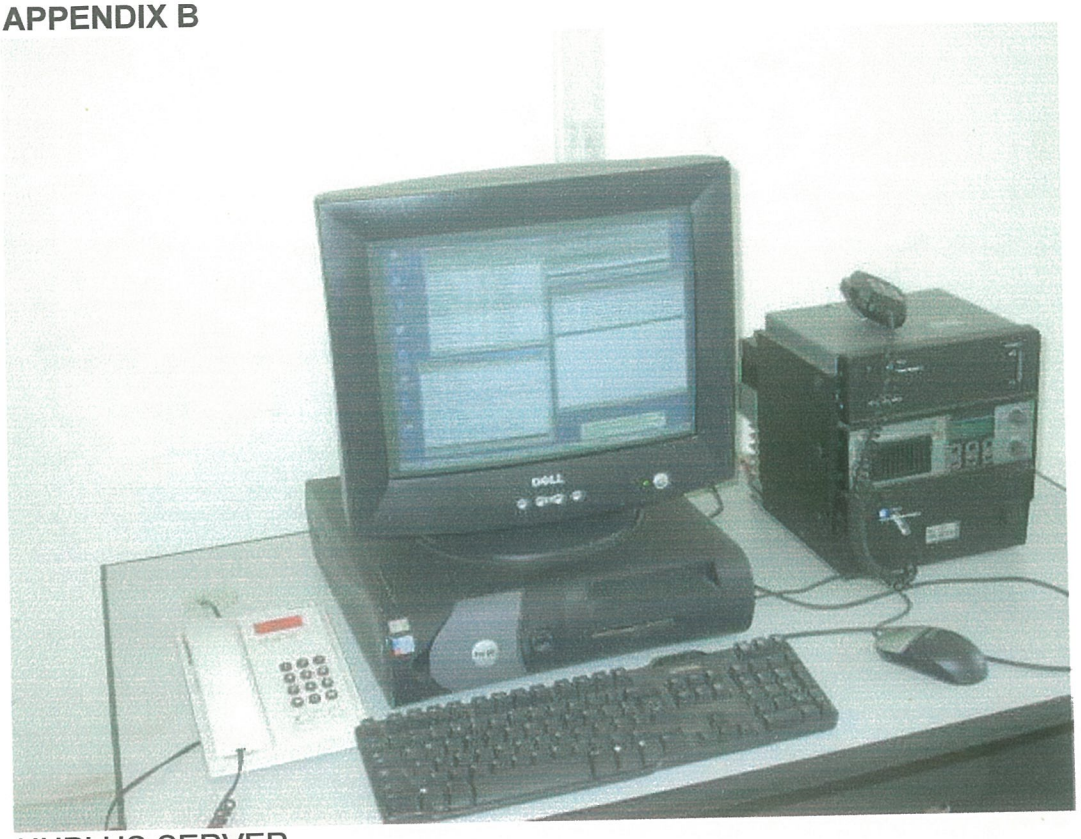
[61] http://simple.wikipedia.org/wiki/Computer_network

APPENDIX A

Very Small Aperture Terminal (VSAT) OUTDOOR UNIT

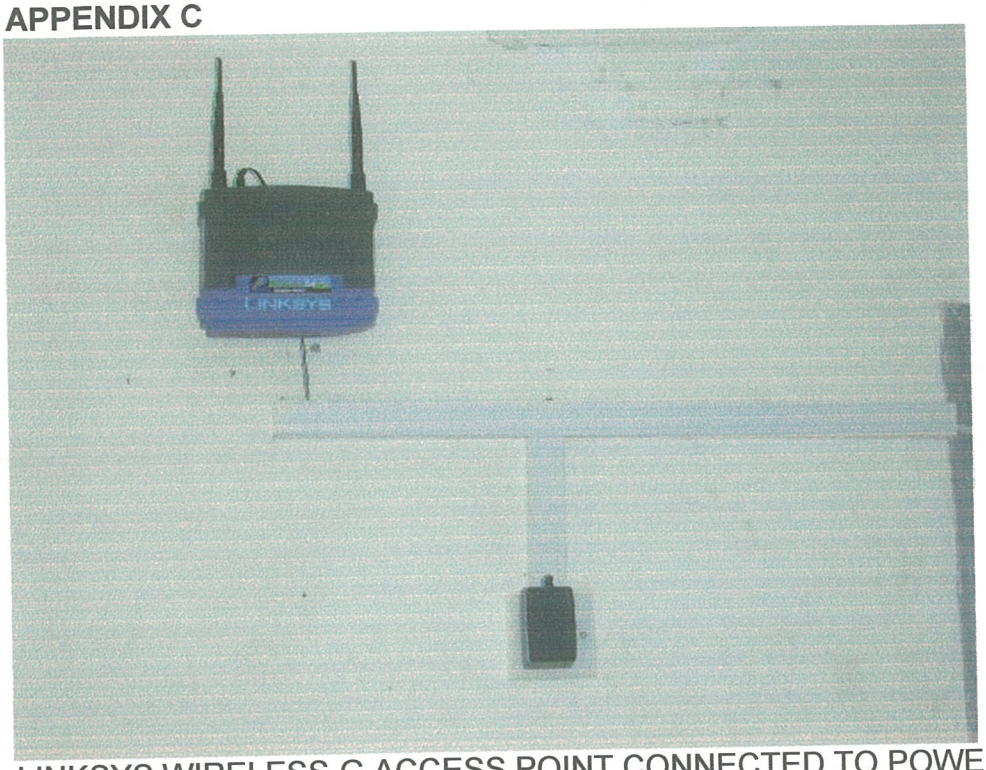
Very Small Aperture Terminal (VSAT) INDOOR UNIT

APPENDIX B



UUPLUS SERVER

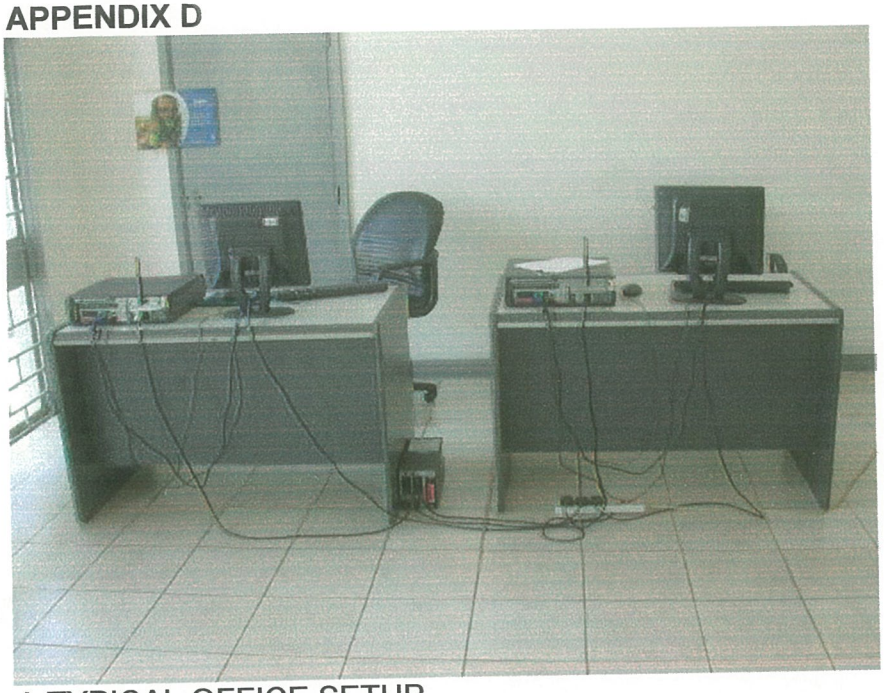
APPENDIX C



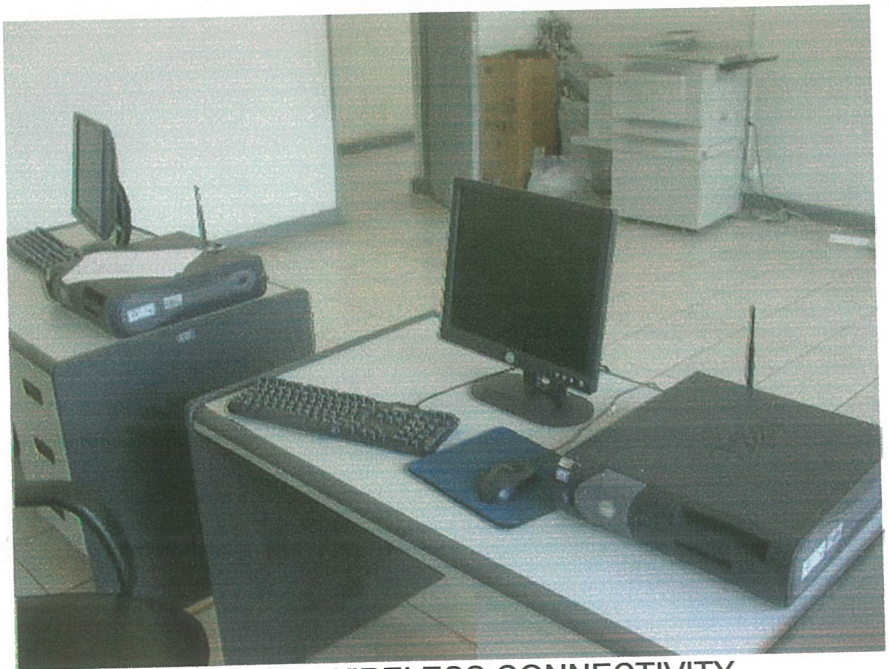
LINKSYS WIRELESS-G ACCESS POINT CONNECTED TO POWER

LINKSYS WIRELESS-G PCI ADAPTER ON A WORKSTATION

APPENDIX D



A TYPICAL OFFICE SETUP



OFFICE SETUP ON WIRELESS CONNECTIVITY

APPENDIX E

SAMPLE QUESTIONNAIRES – WLAN USERS

WIRELESS LOCAL AREA NETWORK SECURITY EVALUATION QUESTIONNAIRE

Survey by:

Kampala International University MSC Student – Tel: 0772-626620

Project Title: EVALUATING OPTIONS OF WIRELESS LOCAL AREA NETWORK (LAN) SECURITY SOLUTION – CASE STUDY OF THE WORLD FOOD PROGRAMME UGANDA.

Preamble: The purpose of this survey is to evaluate the wireless LAN security solutions being used by the organization in comparison to industry standards.

Complete this questionnaire to illuminate areas for improvement in the organization's WLAN security. Your response will be treated with confidentiality and will enable the selection of a suitable security solution that meets the organization's network and information security needs.

The completed questionnaire will be collected on the 27th march 2006, by the contact person mentioned above.

Instructions

1. Circle the appropriate option from the ones provided
2. Print your response in the space provides for open questions.

QUESTIONS

1. How would you grade your computer skills and knowledge?

a) Very Good b) Good c) Fair d) Low e) Very Low

2. Write any one of these terms/Abbreviations in full.....

a) LAN b) WAN c) WLAN

3. What is the use of a username and password on a computer network?

a) Security b) Privacy c) Confidentiality d) Identification e) All

4. What type of computer network does your organization use? (Choose all that apply)
   a) Local Area Network b) Wireless Local Area Network c) Wide Area Network
   d) None e) Don't know
5. How would you grade the security of the network incase you wanted to store you Personal information?
   a) Very Good b) Good c) Fair d) Poor e) Very poor
6. How often are you expected to change your password?
   a) Monthly b) Every 6 months c) Yearly d)Quarterly e) Never f)Don't know
7. How important is information security for achieving organizational goals and/or Objectives?
   a) Very important b) Somewhat important
   c) Unimportant d) Neither important nor Unimportant
8. How often is your top management (country directors), provided a status report on network and information security?
   a) Monthly b) Quarterly c) Semi Annually d) Annually e) Never
9. How often do information security personnel form ICT unit meet with other unit heads To understand their information security needs?
   a) Monthly b) Quarterly c) Semi Annually d) Annually e) Never
10. How would you rate the effectiveness of ICT unit in meeting the organization's needs With regard to security of information on the network?
   a) Very Effective b) Somewhat Effective c) Ineffective d) Don't know
11. How often are you trained on the use of the network and its resources irrespective of the changes in the system?
   a) Monthly b) Quarterly c) Semi Annually d) Annually e) Never

APPENDIX E

SAMPLE QUESTIONNAIRES – WLAN SYSTEM ADMINISTRATORS

WIRELESS LOCAL AREA NETWORK SECURITY EVALUATION QUESTIONNAIRE

Survey by:

Kampala International University MSC Student – Tel: 0772-626620

Project Title: EVALUATING OPTIONS OF WIRELESS LOCAL AREA NETWORK (LAN) SECURITY SOLUTION – CASE STUDY OF THE WORLD FOOD PROGRAMME UGANDA.

Preamble: The purpose of this survey is to evaluate the wireless LAN security solutions being used by the organization in comparison to industry standards.

Complete this questionnaire to illuminate areas for improvement in the organization's WLAN security. Your response will be treated with confidentiality and will enable the selection of a suitable security solution that meets the organization's network and information security needs.

The completed questionnaire will be collected on the 27th march 2006, by the contact person mentioned above.

Instructions

1. Circle the appropriate option from the ones provided
2. Print your response in the space provides for open questions.

QUESTIONS

1. How many existing users access the wireless LAN?.....
2. What applications are used over the wireless LAN?
   a) Data b) Voice c) Video and Voice d) Other
3. What type of wireless client devices are used on the LAN?

a) Laptops b) Desktops c) Handheld/PDA d) Printer e) Other

4. What type of network protocols and traffic types are in use over the WLAN?

a) IP b) IPX c) Internet traffic d) Other

5. How is the wireless network managed?

a) SNMP b) HTTP c) Telnet

6. By what means do the Access points obtain power?

a) AC power source b) Power over Ethernet

7. What brands of access points and wireless bridges are currently in place?

.....

8. How do you ensure system integrity?

a) HIDS b) Module checksum c) Virtualization

9. What are the currently problems faced with the existing wireless LAN?

a) Slow Throughput b) Frequent disconnects c) Difficulty roaming

c) Logon problems d) Other (Briefly explain)

10. What kind of wireless LAN security solution(s) are currently in place?

(Select all that apply)

a) WEP b) Kerberos c)EWG d) LEAP e) RADIUS f) EEG

g) LDAP h) Firewall i) EAP-TLS j) NDS k) PEAP l) Active Directory

m) VPN n) VLANs.

11. What WLAN security policies does the organization have in operation?

.....

.....

.....

.....

12. Incase a user(s) breach the security of the system, what is the procedure used in Handling this and ensuring that it doesn't happen again?

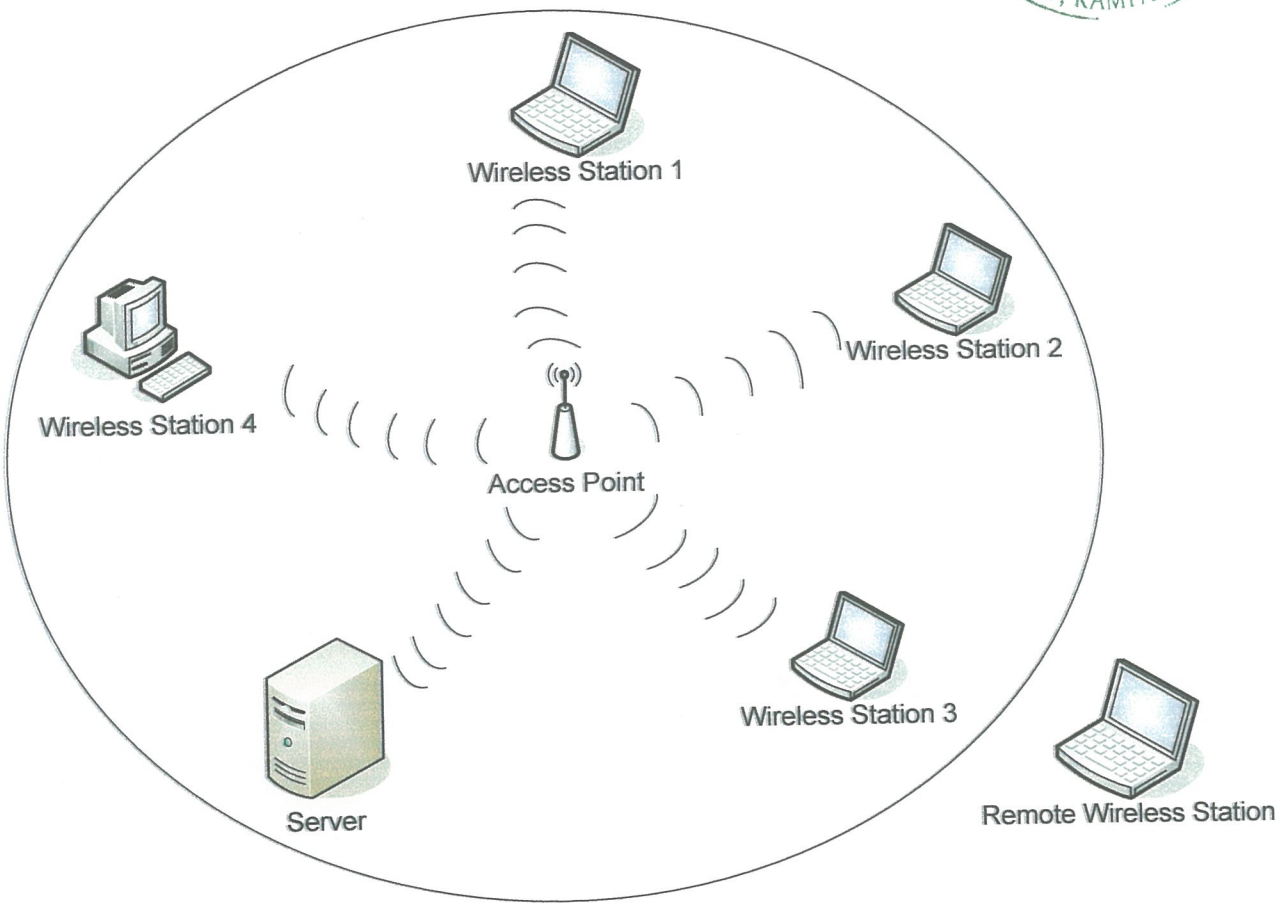
.....

.....

.....

APPENDIX F

WLAN TEST- BED SETUP



APPENDIX G

INTERVIEW GUIDE

The key respondents for this particular interview were the systems Administrators.

Areas of Interest included:

1. How often the WEP key and Service Set ID key are changed
2. How often the Administrator password is changed
3. The mechanism used to separate the wireless network from the wired network
4. How often a network scan is performed
5. The mechanism used to limit and monitor network access
6. How Wireless network traffic is secured during transmission
7. Wireless stations' operating system
8. Antenna types used in the base stations and wireless network cards
9. The level of antenna transmission power
10. How many bits the Access points support
11. Category of network users and their access levels
12. The power solution used to support and protect the system from irregular AC power supply.
13. Nature of physical security used.
14. The mechanism put in place to protect portable wireless stations from theft and if they are stolen, how the organization ensures that they do not become loopholes for attacks.
15. How safe the network configuration details are
16. Any history of information hijack, virus attacks and data interception incidents
17. Any record of prior assessment done before WLAN installation
18. Determine whether security management is centralized or distributed
19. How management WLAN security decisions are guided and made
20. WLAN use and monitoring procedures in place
21. Security policy infrastructure, enforcement and documentation mechanism.