FRAMEWORK FOR SECURING WIRELESS LOCAL AREA NETWORK

By

JOYCE M MWENJA

A DISSERTATION SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF MASTERS OF SCIENCE IN DATA COMMUNICATIONS IN THE FACULTY OF COMPUTING AND INFORMATION MANAGEMENT AT KCA UNIVERSITY

10th

SEPTEMBER 2013

DECLARATION

I declare that the work in this dissertation has not been previously published or submitted elsewhere for award of a degree. I also declare that this my own original work and contains no material written of published by other people except where due reference is made and author duly acknowledged.

Student Name: JOYCE MUGURE MWENJA   Reg.No: KCA/07/03788.

Sign: ______________________________ Date: ________________________

I do hereby confirm that I have examined the master's Research project of

JOYCE MUGURE MWENJA

And have certified that all revisions that the dissertation panel and examiners recommended have been adequately addressed.

Sign: ______________________________ Date: ________________________

PROF. WILLIAMS DDEMBE

FRAMEWORK FOR SECURING WIRELESS LOCAL AREA NETWORK

ABSTRACT

For several decades security and wireless communication will remain to be interesting research areas. Change in technology enables the need of ease of use and flexibility of communications in the computer world without manipulating the existing content. This study seeks to illustrate various concepts of critical to securing data over wireless networks, and overall security of the networks.

In order to demonstrate wireless security, it is important to highlight key specifications of the common security standards in existence such as 802.11 WEP, 802.11 WPA, and WPA2 (802.11i). In the same light, the study explores the concept of Wireless Metropolitan Access Network and its security specifications besides vulnerability to security breach. Finally, the study sums up with reflections and recommendations about wireless network security, along with ample proposals to enhance wireless security especially in a public setting.

There is much regulatory and standards work in the area of network security, especially in wireless network. The wireless LAN standard IEEE 802.11b provides a mechanism for authentication and encryption. This paper describes the security of Wireless Local Area Networks based on the IEEE 802.11 standard commonly referred to as Wi-Fi Networks or WLANs. Similarly, the study examined works by other researchers with regard to security in a wireless network, and addresses current wireless security measures. It was established that the measures indicated by these researchers were largely unsatisfactory, owing to advances in technology that serve to compromise measures employed. The researcher analyzed different tools that used, to attack a wireless network and successfully identified various types of attacks by highlighting some loopholes in WLAN. The study concluded that wireless networks cannot be made completely secure, and should only be used to serve the needs of the organizations, rather than one of convenience. As per this findings and conclusion, the study recommends the adoption of measures serve to improve the security at a wireless deployment site.

Keywords: Security. Wireless LAN. Infrastructure. Attacks. Vulnerability

ACKNOWLEDGEMENT

I wish to thank everyone who contributed in one way or the other towards the completion of my research. My sincere gratitude goes to my supervisor Professor Williams for taking me through the whole process.

I want to thank my family for their continued support throughout the period especially my big sister for her encouragements. I also want to express my gratitude to KCA University for their support. I sincerely thank all my friends for their moral support. Above all, I thank GOD for his grace and helping me go through the whole process to completion.

DEDICATION

I dedicate this project to my dear Son Brandon Mwenja and all the other members of my family for their Love and support.

`

Abbreviations and Acronyms

1 **PKI**- Public Key Infrastructure

2 **Dr-** Doctor of philosophy

3 **Reg-** registration number

4 **WLAN-** wireless local area network

5 **Pda-** wireless Digital Personal Digital Assistant

6 **PC-** Personal computer

7 **WEP-** wired equivalent protocol

8 **Wi-Fi**- wireless fidelity

9 **WPS-** Wi-Fi Protected Setup

10 **AP-** access point

11 **BBS-** Basic service set

12 **WNIC-** a wireless network interface card

13 **Mac**- medium access control

14 **SSID**- Service Set IDentifier

15 **WPA-** Wi-Fi Protected Access

16 **RSN-** Robust Security Network Association

17 **AES-** Advanced Encryption Standard

18 **CCMP-** Counter Mode CBC MAC Protocol

19 **CBC-** Cipher Block Chaining

20 **TKIP-** Temporal Key Integrity Protocol

21 **CRC-** Cyclic Redundancy Code

22 **VPN-** virtual private network

23 **DoS-** Denial of Service

24 **IPSec-**Internet Protocol security

25 **SSL** Secure Socket Layer.

26 **WNIC-** a wireless network interface card

27 **Mac**- medium access control

28 **SSID**- Service Set IDentifier

29 **WPA-** Wi-Fi Protected Access

30 **RC4-** Ron’s Code 4

31 **CBC-** Cipher Block Chaining

32 **TKIP-** Temporal Key Integrity Protocol

33 **CRC-** Cyclic Redundancy Code

34 **VPN-** virtual private network

35 **DoS-** Denial of Service

36 **IPSec-**Internet Protocol security

37 **SSL** Secure Socket Layer.

38 **WPS-** Wi-Fi Protected Setup

39 **AAA** Authenticating, Authorising and Accounting

List of Figures

List of Tables

Table of Contents

CHAPTER ONE

1.1 Introduction

According to Siemens Enterprise Communications, July 2008 white paper, a number of concerns related to insecurity risks with WLAN, such as loss of integrity, confidentiality, and network connectivity. Over the years, various flaws have been demonstrated in WEP while research attribute vulnerability of WLAN setups to installations that are inclined to with their default settings. Viehb, 2012 discovered vulnerability in the WPS technology for WLAN security owing to poor design that enabled efficient brute force attack, which led to immensely manipulating the security of all WPS-enabled Wi-Fi routers. Since recent models of routers are WPS enabled, millions of devices were affected globally leading growing concerns over network security.

Unethical hackers found WLAN very easy to break through, the wireless technology made it easy to break into wired networks. "War Driving is performed on wireless networks to verify the strength of the signal, encryption policy, wireless network name, and the used channel, thus can be used for either to monitor or hack as illustrated by Sangit 2007. It is important that enterprises identify major security weaknesses within their WLAN in order to define effective wireless security mechanisms policies that guard against unauthorized access to important data or information, which is a great resource to the organization.

Chandramouli, 2002 stated that the increasing demands for mobile and flexible mechanisms in our day to day life, contributed significantly to the evolution from wired LANs to wireless LANs (WLANs). A WLAN is based on a cellular architecture where the system is divided into subsystems, each controlled by a Base station, known as Access point or AP. Figure 1 shows a simple model for the wireless LAN

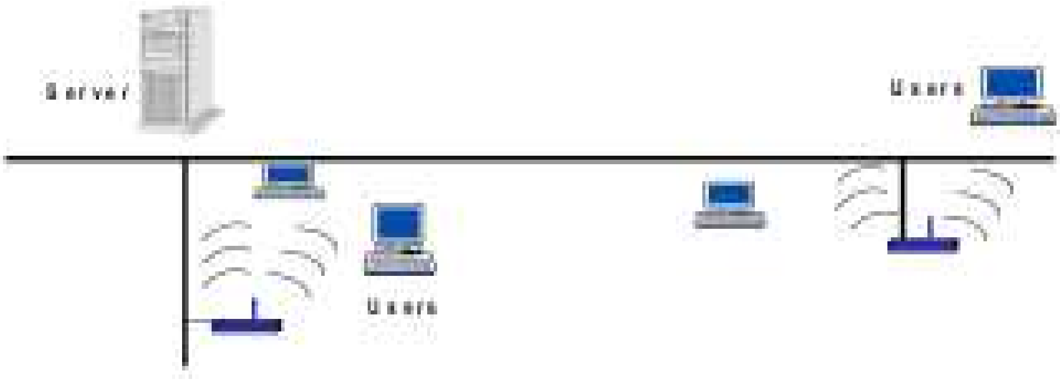
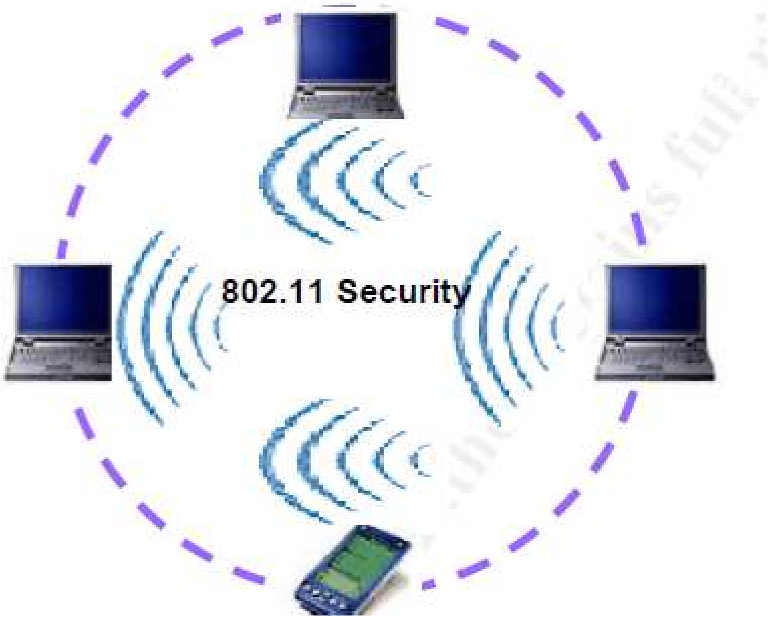


Figure 1: A Simple Model for WLAN

WLANs can be generally classified into two groups, that is, ad hoc wireless LANs as shown in figure 2 and wireless LANs with infrastructure mode as in figure 3. A number of wireless nodes link together to create a P2P communication channel in ad hoc networks where the connection allows Clients to communicate with each other on the network.



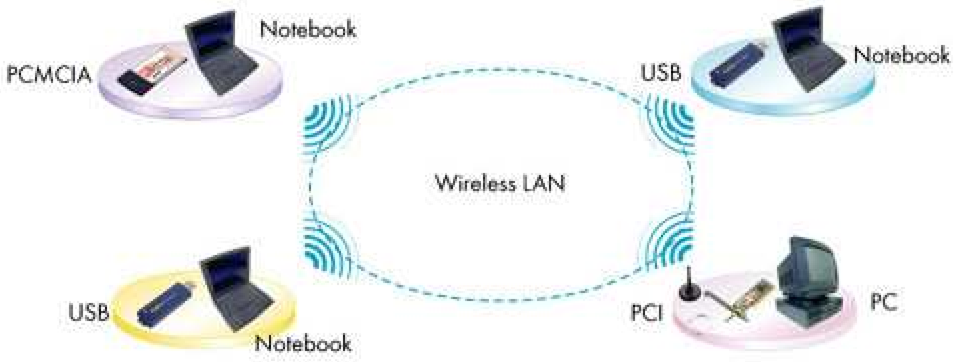


Figure 2: ad hoc wireless LAN mode. Source: EUSSO

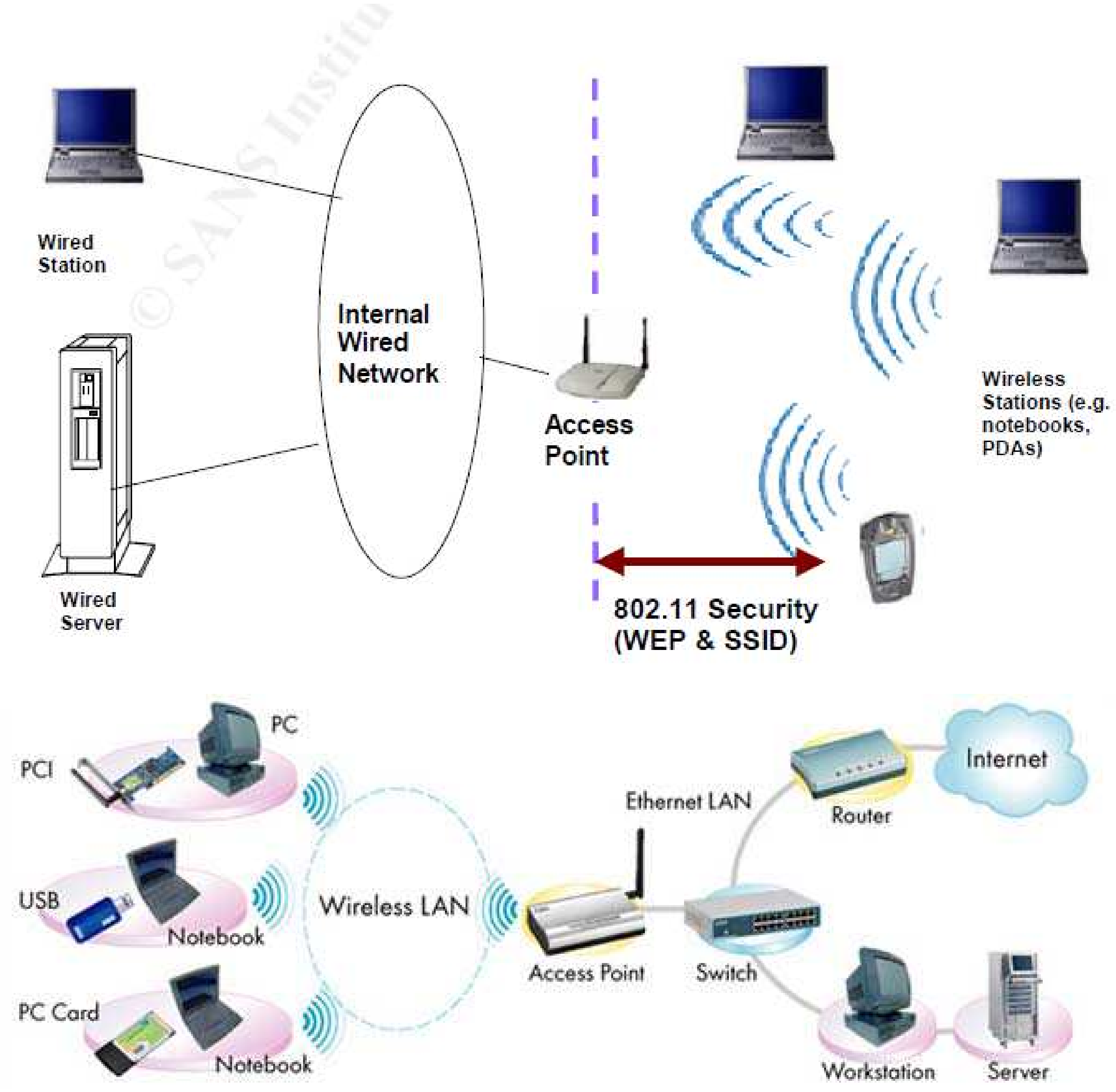


Figure 3: Wireless LANs with infrastructure mode. Source: EUSSO

Ad-hoc networks are planned in a way that only the nodes within transmission range and in the same cell can communicate with each other. Nodes with intentions to communicate outside the ad-hoc network require a member cell to operate as a gateway for routing purpose and thus, no administration is required.

Networked nodes share their resources without a central server while wireless nodes access the wired backbone through access points. The access points allow the wireless terminals to share the available network resources efficiently. For better communication of data, wireless clients and access points must establish a relationship, or an interaction. The exchange of data between wireless stations commences only after a successful interaction among devices of interest.

Black hat hackers can inflict significant damage while comfortably camping outside the premises without WLAN but gaining access from a wireless-enabled device that is connected to a wired network. In essence, hackers gain access to wire networks using wireless-enabled laptops since most network access points cannot perceive intrusion from authorised connectivity without advanced security measures. Security is a top concern among those interested in deploying and adopting WLANs Vacca, 2006.

WLANs share similar risks and weaknesses with conventional wired networks; however, there exists specific threats to WLAN including passive and active attacks, as well as loss of confidentiality, integrity, and connectivity Choi, et al, 2006. Security Crow, et al, 1997 is a big concern in wireless networking, mostly in m-commerce and e-commerce applications though not limited to these applications.

Mobility of users as well as increase of mobile devices raises the security concerns in wireless network. Per Chandramouli, 2002 security among wireless networks is facilitated by authentication and data encryption techniques that rely on the air interface. The IEEE 802.11 standard describes wired equivalent privacy (WEP) that defines a method to authenticate users and encrypt data between the PC card and the wireless LAN access point. Data compromise, denial of Service, and unauthorized access are among the major concerns that threaten the use of WLAN Chandramouli, 2002.

1.2 Definition of theoretical terms

1.2.1 Framework

A framework represents a hypothetical description of a compound entity, process or model that creates a theoretical account into a concept. In essence, a framework describes the underlining structure that supports the existence of various platforms that offer valued services. Conceptual frameworks are useful in the definition of feasible sequence of action and/or illustrate a preferred approach to a proposition or scheme. Conceptual frameworks can act like maps that give coherence to empirical inquiry owing to their potential that is so close to experimental inquiry, and as such, they vary depending upon the research question or problem.

Per Miles and Huberman 1994, conceptual frameworks serve to explain either perceptibly or in narrative form, major aspects that require attention in a study such as key factors, constructs, or variables and the presumed relationships among them.

Smyth R 2004 and Professor Roger Vauger, 2008 conceptual framework; Provides the structure/content for the whole study based on literature and personal experience

Wireless: is a term used to describe telecommunications in which electromagnetic waves facilitate the transmission of signals as opposed to the use of wires along a communication path.

Wireless Local Area Network: is best described as a group of interlinked computers among other supporting devices that share an ordinary communications line or wireless link, NIST Special Publication, September 2011.

1.2.2 WLAN Security

WLAN Security means securing ICT by use of techniques to ensure that data or information stored in computers cannot be read, modified, or compromised by unauthorized users. Security is also perceived through protection of data against interference, which leads to negative consequences.

Henric Johnson et al, 2001, states that security can be categorised into three, that is, Physical security; how to prevent interference signals, Data Security; as in what encryption techniques are used to protect the network against intrusion, User authentication, which is how to protect the wireless network from unauthorized users and, lastly User anonymity that is to say what kind of protection is used against information gathering.

Wadlow, 2000 says that security is a process, which can be applied repeatedly to the network and the organization that maintains it. Having achieved this, the security of the network is bound to improve. Since, every time the process is applied, security gaps can be found, which means that countermeasures can be accomplished. If stop applying the process of security, the security becomes reduced, due to all threats and techniques that emerged from day to day.

Hence, WLAN security is a security system designed to protect networks from the security breaches to which wireless transmissions are vulnerable. This type of security is important because WLAN signals have no physical boundary controls, and are prone to unlawful access over network resources, resulting in the vulnerability of private and confidential data.

1.2.3 Background to the Problem.

Prior to the commercialization the internet, institutions as well as individuals remained connected without calls for concern with regard to the security of their system or network. With time, it was established that some form of security was essential in order to avert exploitation of the connected resources by malicious characters (Chandramouli, 2002).

The deployment of Wireless LAN to connect mobile devices with wired infrastructure for communication purposes elucidates technological advances made over the years in terms of computer networking. Security should also be taken as an important factor while considering this way of communication. In contrast to wired networks, wireless networks are relatively difficult to secure owing to the nature of transmission medium, which is open to anyone within the geographical range of a transmitter. Rysavy (2005) in his work stated this is a concern expressed by information and telecommunications managers he justifies this by saying that radio signals are inherently a subject to eavesdropping due to their extended propagation.

Data privacy is usually accomplished over a radio medium using encryption, but while encryption is achievable, it leads to increased cost and decreased performance.

This paper focuses on computer wireless local area network (WLAN) security by Identify security weaknesses or Vulnerabilities, and Threats within its environment. Establish the Wlan Frameworks flows in the market.

1.2.4 The problem statement

The evolution of new technologies, hackers have embraced numerous techniques and better skills. Efforts to have advanced wireless security standards are being formed and implemented so as to restrict access by the hackers. According to (Choi, et al, 2006) several protocols including the once glorious Wired Equivalent Privacy (WEP) protocol have been demonstrated as incompetent to preserve the integrity of WLANs sufficiently.

With wireless becoming such an enhanced technology, this phenomenon triggers a rise in interest regarding its application in a commercial setting. Nevertheless, not all wireless security measures, no matter how evolved are implemented to the letter by the same organisations. This follows the need to design wireless networks that favour the requirements of a given organizations while others with existing networks perform cost-benefit analysis to determine how best to upgrade to a substantially secure framework (Choi, et al, 2006).

It is evident that there is increased adoption of WLAN technologies broadly; however, there is lack of knowledge of the security weaknesses accompanying widespread deployment of these technologies. Furthermore, there is no clear framework on how to address these security weaknesses, which leads to the realisation by organizations that there really is a need for security awareness training. A study initiated by McAfee in 2005, revealed startling statistics that necessitates redress with a sense of urgency, Browdie, 2008. From the study, one in five workers (21%) let family and friends use company laptops and PCs to access the Internet; more than half (51%) connect their own devices or gadgets to the work PCs, a quarter of who do every day; two thirds (62%) admitted they have very limited knowledge of IT security; more than half (51%) have no idea how to update the anti-virus protection on their company laptop/PC; and five percent say they have accessed areas of IT systems that they should not.

There are technology solutions that are inadequate while others have low levels of security awareness in organizations among other deficiencies. Given these startling research findings, the issue of how best to protect organizational information resources, especially with widespread adoption of wireless local area networks, is even more critical and is the basis of this research.

1.3 Objectives

1.3.1 General objectives

- Develop a framework for securing wireless local area network environment.

1.3.2 Specific Objectives

(i) Investigate the existing wireless networks in order to identify weaknesses.

(ii) Design the framework.

(iii) Develop the framework that will enhance security within the WLAN Environment

(iv) Validate the WLAN security framework

1.4 Justification

Although numerous advantages have been credited to wireless networking, the existence of new security threats alters an organization’s overall security risk profile. While the implementation of technological solutions is the routine reaction to security vulnerabilities, wireless security is described as a management issue.

Effective administration of vulnerabilities linked to wireless networks require significant and purposeful evaluation of risks in an environment before developing a strategic scheme to alleviate demonstrated weaknesses. Choi, et al 2008, several works have affirmed the weakness of Wired Equivalent Privacy (WEP) Security algorithm in the original IEEE 802.11 standard and suggested how the security mechanism of WLAN can be enhanced.

In Isaac and Borisov et al, 2008 the weakness of WEP is largely demonstrated. Though there are external security apparatus that can be used to strengthen the WLAN inbuilt security mechanism as stated by Burell et al, 2008. The research findings can be used as guidelines to create a WLAN framework that is secure, flexible, and interoperable as future standards and technology evolve.

The framework should facilitate a WLAN setup that provides access control channels, which support the expedience among users, secure validation protocols, and infringement detection systems.

1.5 Scope

The framework illustrated in this study can be applied to any WLANs environments. The purpose and intent is to build common architectures and security solutions that will be secure, flexible, and interoperable as future standards and technologies emerge.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

This review of the literature will start by basic introduction of threats and attacks in wireless LAN by discussing their clarifications and categories. The review identifies and discusses various types of WLAN threats and attacks in great detail by considering a number of related work will be reviewed. Major Security Protocols for Various WLAN Standards including Virtual Private Network (VPN) have been examined. The review gives a summary of design flaws in Wlan and propose a deployable/conceptual model of framework for enhancing wireless local area network security.

2.2 Threats and attacks in WLAN

Wireless LANs and wired networks are prone to similar risks and weaknesses that necessitate appreciation of such threats and attacks in order to protect the network from hackers and crackers.

Figure 4 identifies common threats to any seemingly secure wireless framework as passive and active attacks, loss of confidentiality, integrity, as well as network connectivity. Similarly, threats to physical infrastructure of a WLAN are observed by Nasre, 2004, and untrained users on WLAN security by Rathnakar et al, 2009.

Passive attacks: As quoted by Heather et al, 2005, these occur when unauthorized persons gain access to the network, but do not modify the content as illustrated by eavesdropping and traffic analysis/monitoring.

The diagram below shows a general classification of WLAN security attacks.

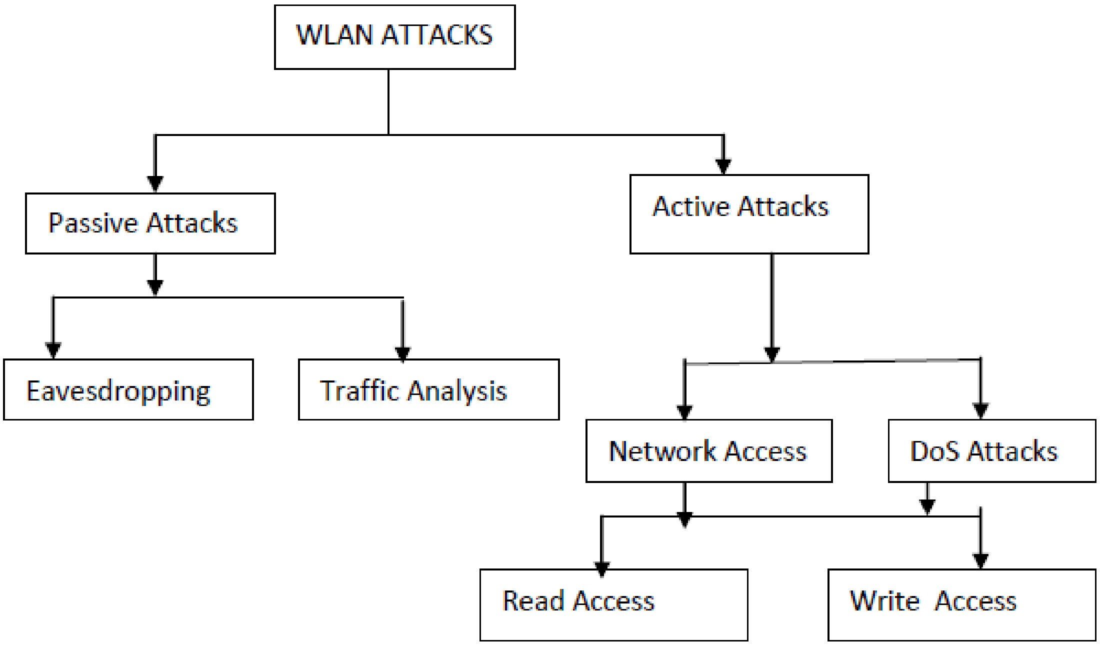


Figure: 4 Classification of WLAN Security Attack.

Per Jonathan, 2000 when an attacker listens and monitors transmission of message content more often than not from within the business premises where information is compromised and privacy is invaded, it is illustrative of eavesdropping.

The study of traffic analysis is a common undertaking by intruders who situate themselves outside the business premises with the aim of monitoring communication patterns through the transmissions waves. In essence, an intruder observes and generates analysis concerning the nature and volume of traffic as well as the transmission load, but does not make alterations to the accumulated information.

Active attacks: these occur when unauthorized persons go beyond their networking privileges and perform alterations to a message or file within the network. Four types of active attacks have been identified as replay, masquerading, message modification, and Denial-of-Service (DoS) all of which can be detected, but may not be prevented. Per Mitchell, 2005 masquerading occurs when an intruder mimics the identity of an authorized user to gain entry into a secure connection. As such, the identity and personal information of authorised personnel jeopardised allowing the intruder a free pass to exploit network resources.

These attacks can range from very simple to complex based on the security in effect. When an intruder monitors transactions before retransmitting the same information as the authorized user, replay is deemed to have occurred. The initial attack begins as a docile, but ultimately escalates to an active attack following an effective interception and reply to transmission by the intruder. As such, the attacker modifies attributes of the transmission through deletion or addition of content or a typical reorder of the message.

In contrast, a denial-of-Service (DoS) attack serves to incapacitate or disable the WLAN setup, which when successful the attacker disallows the use of the network by locking out other users. The purpose of intrusion is often to inhibit service delivery an aspect achieved by bringing the network to crawling speeds and subsequent failure to transmit owing to interference Choi et al, 2006.

There are multiple DoS attacks, one of which is the ‘brute force’ method. This can come in one of two forms, either a huge flood of packets that uses up all of the network's resources and forces it to shut down, or a very strong radio signal that totally dominates the airwaves and makes access points and radio cards useless.

Loss of confidentiality; Confidentiality is a major concern when dealing with any network. An organization does not want its company’s private information and investments open to competitors. With WLANs, network intruders need not to gain access to a network cable to establish themselves in the network; they often take advantage of radio and broadcast waves that render traditional security measures for LANs less effective.

Passive attacks are directed towards compromising the integrity and the confidential nature of wireless networks, which is achieved by simple interception of seemingly secure transmissions. Owing to varying ranges in connectivity, intruders often go unnoticed since transmissions can be accessed away from the premises and achieve the same damaging effect. The application of a hub by most users often increase the probability of network attacks since these provide communication to the integrated network and leaving transmission vulnerable.

Loss of integrity: In network connections characterised by loss of confidentiality, the integrity of such is largely compromised leading to loss of critical information such personal information. Notably, most companies lack sufficient protection with regard to networking, thus achieving integrity remains a fastidious task, which allows intruders to modify data. This can be devastating to an organization if important information is lost or modified.

Loss of network connectivity: this is known to occur along with severe DoS attacks, which often involve loss of network signal facilitated by tactics such as jamming. Jamming arises after an intruder successfully interferes with the wireless signals by blocking transmission across the network, which comprehensively incapacitates the ability to send and receive information across the platform. For instance, a user can deliberately initiate network jamming by prioritising the download of a significantly large file, hence placing other dependents on queue without reliable connectivity.

Nasre, 2004 indicates that the infrastructure of WLAN is prone to damage following successful malicious intrusions. As in the case of wired connections, operating WLAN in infrastructure mode depends on various components including APs, cables, antennas, wireless adapter, and software. Harm to any of these could significantly reduce the signal strength within limit coverage area, or reduce bandwidth.

Access points should be placed in secured locations, Prof Rathnakar et al, 2009 stated that easy access-to-access point is a security threat in that information available about a wireless network is also the information needed to launch an attack. With this in mind, access points should not be installed in areas with easy accessibility since this exposes the facilities to vulnerabilities such as being be removed or tampered with altered configurations.

Poor security configurations pose significant threat when the 802.11 security settings, useful in authentication and encryption, fail in their functionality, or the service set identifiers (SSIDs) are not configured accordingly. One of the weaknesses of WLAN is lack of physical boundaries set.

Wireless access points tend to lose signals depending on the deployment environment, which governs the signal strength varies based on the materials surrounding the platform such as walls, doors, floors, insulation, among others. In light of this, signals have demonstrated to availability to other user’s airspace and connect with their wireless local area network, as illustrated by accidental associations, which occur in densely populated areas where several people or businesses use wireless technology.

Untrained users: this group poses a serious threat to WLAN deployment experience since most of the users either lack the fundamentals that govern network security, or have a strong desire to utilise the network that overshadows efforts to secure the system. A good example a rogue access points (APs) brought in to the enterprise by employees, or poor access point setup by the untrained employee described above.

Such characters may utilise access points that do not favour network security, thus leaving the entire infrastructure open exploitation and loss in the network integrity. Other rogue actions include external malicious users such as black-hat hackers who thrive by exploiting wireless networks within their reach, which can be costly to any organization owing to compromised data.

In 2007, the Wi-Fi alliance developed a Wi-Fi Protected Setup (WPS) protocol, which is a simplified mode of establishing secure wireless connections. While this protocol addressed vulnerabilities found in WPA and WPA2 prior to December 2011, the setup was found to be Vulnerable to Brute Force Attack. Viehbook, December 27, 2011 established that many wireless access point (AP) models with the feature called WPS have vulnerability.

2.3 Related Work:

Choi et al, 2006, suggests key steps that are critical when implementing a robust WLAN security for organisations by use of enhanced security mechanism such as visual to reassure security of information. The authors, by use of actual scenarios on different organization employing variety of secure procedures and demonstrating fully executed channels of a secure framework, propose the advantage of repeated measurement of the Wireless Local Area Network; to facilitate durable, global and secure assurance by use of a company WLAN Security enhancement structure.

Vijay, 2002, has a general overview approach to WLANs, which fails to give an in-depth study of security issues in WLAN and the possible threats and vulnerabilities. The author identifies that wireless communication is a developing field that holds many future possibilities in this area. Such expectations indicate the importance developing ample security as technology advances to cater for communication devices that support communication with higher data rates.

Vijay agrees and further suggests that a dominant means of supporting such communication capabilities would be through the application of Wireless LANs; of which he focuses that as the deployment of Wireless LAN increases well around the globe, it is increasingly important to understand different technologies and select the most appropriate one. The author provides a detailed study of the available wireless LAN technologies and issues of security concern while evaluating and suggesting a feasible standard for future. However, the researcher neglects to explore vividly available frameworks, which addresses security flaws in WLANs.

Chen et al, 2005, reviews wireless LAN security by focussing on the new and evolving IEEE 802.11i standard where major security enhancements in encryption and authentication specific to this standard are illustrated. In addition, the newly introduced key management in 802.11i is captured by discussing the incorporation of IEEE 802.1X as an authentication security enhancement. Similarly, the researcher delves in to the specifics of both intra-subnet and inter-subnet roaming with regard to networking security. The paper thus does not address framework issues that are relevant in enhancing security with regard to WLAN.

Hamid, 2003, in his approach begins by introducing the concept of WLAN where in the introductory section he gives brief information on the WLAN components and its architecture. Seeking to understand security threats associated with WLAN, the study explores at Denial of Service, spoofing, and eavesdropping forms of network attacks. The author further explores into the functionality aspects of Wired Equivalent Privacy (WEP), which is a significant standard in IEEE 802.11b/WiFi encryption for wireless networking. The researcher examines weaknesses indicated for WEP to discover that the system is relatively weak in terms of security than anticipated and thus further study are required to develop practical solutions for more secured WLAN.

He also covers the new standards to improve the security of WLAN such as the IEEE 802.1x standard, which comprises of three separated sections: Point-to-Point Protocol (PPP), Extensible Authentication Protocol (EAP) and 802.1x itself. The author identifies that 802.1x is included in 802.11i, a newly proposed standard for key distribution and encryption that will play a big role in improving the overall security capabilities of current and future WLAN networks.

The 802.11i standard establishes a pair of significantly improved encryption algorithms that include Temporal Key Integrity Protocol and CBC-MAC Protocol to succeed WEP, and improve on network security. The study provides a comprehensive list of networking products that afford users protection to their wireless networks from attacks, thus maintaining the integrity. The paper therefore fails to address a framework for enhancement of WLAN security.

Park, et al, 2003, in their paper enumerates the various advantages of WLAN and the reasons for their implementation. The authors concur that although WLANs solve some problems that exist in traditional wired LANs, they also introduce new security issues. The study appreciates current and future security concerns with regard to networking and possible countermeasures, which include standards, technologies, management, policies, and service environments. They suggest that risks that WLAN services present can only be mitigated rather than completely eliminated, of which they suggest that although there is no single solution for perfect WLAN security, WLAN security can be enhanced to an acceptable level by a proper combination of countermeasures.

Singh, et al, 2010, illustrates security flaws of Wireless LAN facilitated by cracking the 64 bit WEP key on Wi-Fi access points using Backtrack, which is a Linux-based operating system popular among hackers. Backtrack users can attack an Wi-Fi access point by initiating the generation of packets in the cracking effort, which results in the successful generation of the WEP key. The authors give a detailed procedure of how to achieve the cracking process thus showing the vulnerability and weakness in WLAN.

The points out that owing to the broadcast nature of the wireless communication, it’s relatively easy for intruders to interject communication and disrupt normal operations of the network by diverting resources to serve their needs. They equally are of the opinion that security is of ultimate importance to the global communication and information networks and that that data, which are encrypted with WEP Key, are also insecure. They however have failed to address the solution to this flaw or weakness.

2.4 Major security protocols for wireless LANs

2.4.1 802.11b:

Over the years, WLAN setups have faced enormous security threats and attacks leading to compromised networks, however, emerging technologies facilitate security and protection from most attacks. Among the steps taken towards securing WLAN from vulnerability is the addition of the 802.11b standard that employs the Wired Equivalent Privacy (WEP) protocol, which was developed to ensure user-friendly encryption.

WEP functions by encrypting the network's packets with an encryption key, which is then sent to its destination for decryption of the packet in order to retrieve its contents. Theoretically, this is an efficient way to secure data using encryption codes whose key is known to the originating and the target addresses; yet, there exists intrinsic flaws that compromise this security to experienced hackers.

This flaws are highlighted within WEP protocol that generates a proportion of encryption key as plain text, which hackers, using reverse engineering software, extract the key to decrypt packet contents. A plausible countermeasure to ensure protection when using the WEP protocol is achieved by changing the encryption key frequently such that intruders do not accumulate enough data on packets to crack the key. Owing to the demonstrated vulnerabilities regarding WEP, a vast majority of organisations and firms opt for alternatives as they abandoned the implementation of 802.11b wireless LAN in their premises.

Moreover, it has been demonstrated that in 802.11b, the WEP protective functionality can be switched off, which justifies reluctance by most firms and companies who ensure that the function is running. However, most home users remain ignorant of the benefits of WEP and end up leaving it turned off, thus increasing the risk for security attacks.

Following lack of adequate knowledge on the benefits of the 802.11b standard and massive abandonment by commercial institutions, the security measure can be consider a failure.

Nonetheless, even as the 802.11b standard is illustrated as a failing measure, the demeaning aspects sparked off a campaign seeking to overhaul current wireless security and replace them advanced technology.

2.4.2 802.11i,

802.11i was developed as a result of 802.11b WEP security failure. 802.11i brings more protection by making use of secure keys and encryption. According to Dulaney et al, 2004, 802.11i security standard was permitted incorporation into WLAN setups by IEEE.

The 802.11i security standard was approved by the IEEE to be incorporated in securing WLANs networks Dulaney et al, 2004.

The 802.11i standard employs a dual layered security protocol namely the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP) and the Temporary Key Integrity Protocol (TKIP). CCMP is the primary method employed in the protection of wireless packets in the 802.11i standard, which confers significant benefits that address the shortcomings experienced while using WEP in the 802.11b standard. The CCMP protocol is designed to be always active, thus enabling security features even if the user does not know how to configure manually.

The CCMP adopted a differentiated version of the Advanced Encryption Standard (AES) encryption algorithm, which provides a robust security where the packets are encrypted using a 128-bit key to offer a nearly impenetrable system.

Despite encrypting the message data, the origin, target as well as other interactions remain encrypted. Another crucial feature of CCMP worth noting regards the encryption key, which does not need to be included in the packet thus eliminating risk of interception. Among the drawbacks of WEP lie with the inclusion of portions of the encryption key in the packets, which culminated in transmission of large volumes of packets increasing the chances of cracking the key.

With 802.11i standard, CCMP preserves the integrity of wireless networks by securing them against a majority of common networking threats, and thus ensure an efficient security mechanism. However, the sole indicated setback lies with infrastructure requirements where CCMP being new technology, demands high end hardware and software, which is a necessary step to ensure security protection in wireless networks. Another important encryption method within the 802.11i standard is TKIP, serves as a wrapper around the old WEP protocol to seal off previous limitations. Contrary to the infrastructural demands of CCMP protocol, TKIP is readily compatible with old hardware and software that satisfy WEP requirements, thus curtailing additional costs during implementation.

The TKIP and CCMP functions works in a similar manner only that TKIP makes use of a number of keys for purpose of encrypting the data packets. It also helps in and the addition of encryption keys in the packet. This mechanism makes use of 64 – bit encrypting key whereby each packet is encrypted prior to packet transmission. The encryption process involves encrypting the header and data for every packet, and due to change of keys with each packet, it’s important to have these keys to the packet. In addition to a 64 bit encryption key, a 128 bit encryption key is employed to enhance security and integrity of the whole packet.

2.4.3 WPA/WPA2; Wi-Fi Protected Access (WPA & WPA2)

While the 802.11i standard was conceived to resolve issues demonstrated in WEP and expedite the implementation adequate WLAN security scheme for the enterprise market, the process took time to approve. As such, the Wi-Fi Alliance established the WPA, which is based on a subset of the 802.11i draft in 2002, as a temporary remedy to ensure vendor interoperability. While still utilizing RC4 encryption, TKIP applies a temporal encryption key that is regularly renewed in order to discourage efforts made towards stealing the encryption key before deciphering a sizeable amount of information. Furthermore, the integrity of data is largely improved by the use of the more sturdy mechanism, the Michael Message Integrity Check (MMIC).

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.

Nevertheless, concern is expressed concerning the use of RC4 encryption algorithm in TKIP as opposed to the use of temporal keys, which are considered to offer relatively superior security solutions. For this reason, most institutions viewed WPA as a provisional measure purposed to reconcile the gap between WEP and the soon-to-be ratified 802.11i standard and thus opted to hold off on their deployments. The year 2004 ushered in WPA2 after the WiFi Alliance upgraded the WPA standard by replacing the RC4 encryption algorithm with AES (Advanced Encryption Standard).

2.4.5 VPN;

Tyson, 2001 defines a Virtual Private Network as an isolated network that utilises open networks to remotely connect users or sites together. VPNs have a wide array of security attributes that facilitate user connectivity to different networks while preserving the integrity.

According to Tyson, 2001 a VPN is made up of four parts that guard its security and they include firewall, encryptions, IPSec, and AAA Servers. A VPN’s firewall acts exactly like any other firewall that block and only allows certain ports whose packets have been filtered and deemed as malicious-free through a designed mechanism. A firewall is an important unit in the VPN as it ensures viruses and Trojans do not jeopardise the server. There exists no defined encryption mechanism in a VPN setup; nonetheless, three key approaches have been implemented.

First is the Symmetric Key Encryption whereby every connected device is allocated a unique key that affords each the capacity to decrypt packets as they are received. Notably, the symmetric keys used on each device are identical and thus require frequent reassessment to deter efforts made by intruders to compromise the network.

The second is the Public Key Encryption that operates by both communal and personal keys to enhance network security. The private key is applied by the sender to encrypt data packets (which they only know), while the public key is employed by the receiver to decipher the packets using the source's public key. Public key is identical to the symmetric key, with only difference being that two divergent keys are applied as opposed to one. For the purposes of a successful connection every user should obtain an access key, which guarantees controlled connectivity.

The third way of encryption is by use of Pretty Good Privacy (PGP) that relies on a generated session key to promote and secure protection. Sessional keys are generated per session for each user, and are renewed in every session or for each user seeking to connect. The PGP system then transforms into a public key system as it encrypts the packet and assigns sessional keys to available public keys. The newly encrypted packets and keys are then sent to the destination device where private keys are applied to decrypt information.

While these are the most common techniques, there are no limitations to govern the encryption systems within VPN, thus the lack of a defined encryption standard in the setup.

Internet Protocol Security Protocol (IPSec) provides alternative security to VPN setups by enhancing privacy protection through message encryption. Two methods are sought in IPSec where one (tunnel) involves the encryption the whole packet encompassing the header.

The second method is transport, whose only role is to encrypt the data section of the packets and not the header. These methods demand that the user and the access point have the same key in order to decrypt the message as it arrives.

Lastly, is the use of an Authenticating, Authorising, and Accounting (AAA) server in which connection requests are passed on to a proxy server where the user is determined and authenticated according to the scope of what he/she is allowed to do against what he/she is actually doing Tyson, 2001. This system has extra security because it monitors what the user is doing. Through monitoring efforts, the system establishes a pattern and defines the likelihood of a security breach based on user activities. Although the VPN setup does not compare competitively in terms of security with the 802.11i standard, it facilitates flexibility within an institution.

CHAPTER THREE: RESEARCH METHODOLOGY

3.0 Research Methodology

3.1 Introduction

General the section addresses the research approaches, the activities, method and procedures for the study are discussed. Specific issues to be discussed here include the research design, the data collection instrument, the population, the sample size, and methods of analysis. Moreover, the study relied on both primary and secondary sources of data to establish its findings.

3.2 Research Approaches

The key activities undertaken during the research project include collection of data both Secondary and primary, State of the Art Literature Review, Formulation of questionnaires and interview questions; generally, the techniques focused on interviews, depth interviews and projective techniques. Identification of data sources (key respondents/ informers; selection of sample sizes among others), Administration of questionnaires, interviews and field visits for data collection. Data collection and analysis of research findings was subjected to a web based application for designing surveys, collecting responses, analyzing data.

3.3 Methodology

The study's main aim is establish an effective framework that should enhance security of a wireless local area network environment. A step by step qualitative study by first identifying the security weaknesses or Vulnerabilities, and Threats prevalent in the WLAN Environment; discuss the effectiveness of the solutions in the market in addressing these security weaknesses, Vulnerabilities, and Threats; identify WLAN security frameworks available, their limitations and implementations.

A literature survey was carried out to help address the first objective and then a questionnaire was raised coupled with interviews to help clarify areas that are not clear from the questionnaires on selected institutions/organizations to help identify whether there are existing frameworks and if there are, their weakness.

As much as Security challenge is a global issue, the war drive was however done within Nairobi (Kenya) given the constraint of time and cost factors. A few education institutions and government institutions employing the use of WLAN were targeted for the survey.

3.4 Population and sampling

The respondents to questionnaires from the selected enterprises are people knowledgeable with the questions at hand and are the most senior persons of the firm, for example technical managers or Network administrators.

3.5 Data collection and analysis

Data was collected using a semi-structured questionnaire served to respondents. Snort, which is a compact utility application that operates in the background of computers, was used to assess the activity of wireless networks. For each wireless network connection established, the application displayed an in-depth analysis to reveal details on the SSID, signal's quality, Algorithms employed, MAC Addresses, Channel Frequencies, among others.

The system requirements for snort utility include a wireless network adapter with appropriate drivers that various operating systems such as Windows XP/Vista/7.

The questionnaires were administered through a web based application while the participants were called and some visited in order to explain the purpose of the study. This was then being followed with a telephone interviews and instant chats with the respondents to verify facts on the questionnaires. The methods were chosen because of effectiveness, time, and cost. The total numbers of participants (wireless network experts) that the questionnaire was send is thirty-eight (38) though only twenty-eight (28) responded representing a response of 74% with 26% abstaining.

To achieve a full interpretation, understanding and to extract useful information from the primary data, a formal statistical analysis methodology is vital. In this study, therefore, the researcher used the web application tool called survey “monkey”.

CHAPTER 4: CONCEPTUAL DESIGN AND FIELD STUDY

4.1 Research Design

Viehbook, December 27, 2011 discovered that Wi-Fi Protected Setup (WPS) was found to be Vulnerable to Brute Force Attack and this was brought by the design flow, which allowed an attacker to guess an access points, WPS Personal Identification Number (PIN) in a reasonable amount of time.

The sad thing is that Software, like Reaver Pro, that performs this attack is freely available over the internet. An attacker would need to be within range of your wireless network for several hours or more to conduct the attack.

With the WPS PIN, an intruder could gain access to your wireless network where it they may observe the network traffic before mounting further attacks and the only solution so far is to disable the WPS.

WEP employs the CRC-32 mechanism to perform integrity checks where the Cyclic Redundancy Code (CRC) is defined as a class of algorithms that operate by treating any message as a large binary number and then dividing it in binary without overflow by a fixed constant. In this light, the overflow that is referred to as the "checksum". As CRC is not cryptographically robust, it was not conceived for the purposes of message digest or hash functions since it fails to provide sufficient integrity protection.

Since CRC-32 is linear, it is feasible to calculate the bit variance between two CRCs by taking into account the bit differences in the messages and the manner of grouping. In essence, inverting the bits in the message results in a distinctive set of bits in the CRC that when examined generate the correct checksum on the modified message. The concept of flipping bits sails through an RC4 decryption, which allows attackers to flip bits randomly within an encrypted message before adjusting the checksum to reveal a seemingly valid message Owing to this characteristic, the CRC fails to provide the required integrity protection, and thus exposes the WLAN to vulnerabilities.

A media access control (MAC) address is a unique identifier assigned to a particular computer with the aim of authorising an access point to connect to a certain wireless network. Relying fully on this filtering can result in a security breach since an adversary can obtain valid MAC addresses easily by sniffing the traffic System Authentication thereby resulting in identity theft, as is the case with MAC spoofing attacks.

In Off-hours, traffic/war driving scenario an unethical hacker drives into parking lot with equipment loaded with software like NMAP, or using other detection devices in an attempt to gather data from enterprises with unprotected LANS. This is referred to as off-hours traffic and “some enterprises even take steps to turn off the access points during non-office hours” to frustrates they would be war driving unethical hacker.

4.2 Data Collection

This section presents the finding and analysis after the WLAN analysis using “Monkey survey”. Snort tool was used in war drive to assess the network's SSID, signal's quality, Algorithms employed, MAC Addresses, Channel Frequencies, among other networking variables.

The activities in WLAN survey was carried out from 21st June – 31st September 2012 in order to gain a better understanding of the use and deployment of WLAN in organisations. The questionnaire and subsequent results of the survey are indicated in a tabulated format.

A total of 76.8% WLAN professional from various organisations responded. Overall, 71.4% of the respondents have implemented or planning to deploy WLAN; 21.4 % Have plans to implement (including trial/pilot); 7.1% do not have plans to implement WLAN; the remaining are either in WLAN pilot trials or planning to implement WLAN in Year 2014.

When asked if there is a security policy in their organisation that addresses the use and security aspects of wireless technology, including WLAN; 76.8% of WLAN professional responded. 60.7% said yes and 35.7% while 3.6% said that the policy is not specific or it’s intertwined in the policy.

WLAN professional respondents majority agreed that there organizations are aware of the Wireless LAN Security Best Practices; 71.4% said yes while 28.6% said no. Despite the organisations being aware of the Wireless LAN Security Best Practices, when the WLAN professional were asked: Have your organization adopted the security best practices in your deployment? WLAN; 76.8% of WLAN professional responded, 53.6% said no while 46.4% said yes. Procurement and luck of management will to invest in security was pointed as one of the drawbacks.

The major security concerns in implementing WLAN in organizations were rated as 1 to 7 with 1 being the lowest and 7 being the highest as shown in table: 2 below;

	1	2	3	4	5	6	7	N/A	Rating Average	Response Count
a) How to secure Data on WLAN	**39.% (11)**	18.% (6)	4% (2)	3.6% (1)	5% (3)	14.% (4)	0.0% (0)	17.% (5)	2.482	28
b) Weak authentication implementation provided by IEEE802.11 WLAN standards.	25.% (7)	**35.% (10)**	7.% (2)	10% (3)	0.% (0)	7.1% (2)	3.% (1)	10.% (3)	2.56	28
c) Weak cryptographic implementation (i.e. WEP) provided by IEEE 802.11WLAN standards.	10.% (3)	10.% (3)	**35.% (10)**	7.1% (2)	7.1% (2)	7.1% (2)	0.0% (0)	21.% (6)	3.14	28
d) No effective solution in detecting unauthorized equipments	3.6% (1)	17.% (5)	17.% (5)	**32.% (9)**	10.% (3	0.0% (0)	3.6% (1)	14.% (4)	3.50	28
e) Degradation in network and system performance over WLAN.	10.7% (3)	3.6% (1)	14.3% (4)	7.1% (2)	**28.6 % (8)**	10.7 % (3)	7.1% (2)	17.9% (5)	4.22	28

f) No effective solution in preventing Denial-of-Service on WLAN.	3.6% (1)	10.% (3)	7.1% (2)	17.% (5)	**25% (7)**	17.% (5)	10.% (3	7.1% (2)	4.58	28
g) APs and WLAN being listed or published by entities conducting War Driving.	3.6% (1)	0.0% (0)	10.% (3)	10.% (3)	7.% (2)	17.% (5)	**39.% (11**)	10.% (3)	5.56	28

Table: 1 what do you think are the major security concerns in implementing WLAN in your organization?

APs and WLAN being listed or published by entities conducting War Driving was considered was the major security concerns in implementing WLAN in organizations as shown in table; 2 being rated at “7” with 39% out of 76.8%. Degradation in network and or system performance with VPN over WLAN was rated second with 28.6% out of 76.8% while; No effective solution in preventing Denial-of-Service (DoS) within WLAN was a third concerned by WLAN professionals who responded rating it at “6” with 25% out of 76.8%. Another issue of concern was, No effective solution in detecting unauthorized equipments (i.e. client devices and access points) deploy by malicious entities, WLAN Professionals who responded gave it a rate of “6” with 32% out of 76.8%.

It was observed that Some of the security measures that organizations have implemented or would consider implementing for WLAN according the WLAN Professionals respondents to this question 85.7% felt that User Authentication would be a priority, 75% Physical Security , Access Controls 71.4%, Logging & Audit Trail 60.7%, Confidentiality & Integrity 57.1%, APs Management 25.0% and the remaining percentage others .

The survey revealed that the primary use of WLAN in organisations was to provide; wireless access to Internet 92.9%, wireless access to corporate resources and information that are classified up to confidential 35.7%, wireless access to corporate resources and information that are unclassified 32.1%, Provide wireless access to corporate resources and information that are classified above confidential 17.9% and the remaining percentage use Wlan for other activities outside the organisation.

Majority of organisations according to the survey support the following security services ; WEP, WPA & WPA2, WPS 71.4%, Integrated Stateful Firewall in the AP 50.0%, Authentication: Open, MAC, 802.1x, Web Page Redirect 46.4%, switching performed at the Access Point 35.7%, Integrated IDS/IPS sensor 17.9%, Is encryption/decryption performed at the Access Point 17.9%,If encryption/decryption performed at controller 10.7%, Wireless Distribution Services (WDS) available in the AP 10.7%, QoS tagging applied at access point 7.1% and the remaining percentage of 7.1% was for other security measures supported which were not within the scope of the survey.

Snort (network sniffer) tool was used in war drive to capture the, SSID, Last Signal Quality, Average Signal Quality, Detection Counter, Authentication Algorithm, Cipher Algorithm, MAC Address, RSSI, Channel Frequency, Channel Number. According to Vollbrecht (2002), an attacker can gain the knowledge of basic information on WLAN security. The information can be used to launch an attack on the Wlan.

The Result from Snort can be used by hacker using another sniff software like Wireshark, The attacker can sniff IP address and MAC address of a valid Access Point and this will allow an attacker direct access to all devices on the network, else use the network to gain access to the wider Internet. When this happens it will be difficult to identify the attacker (or intruder or hacker) since the intruder appear to be valid user of the attacked network.

4.3 A Conceptual Model of Wlan framework

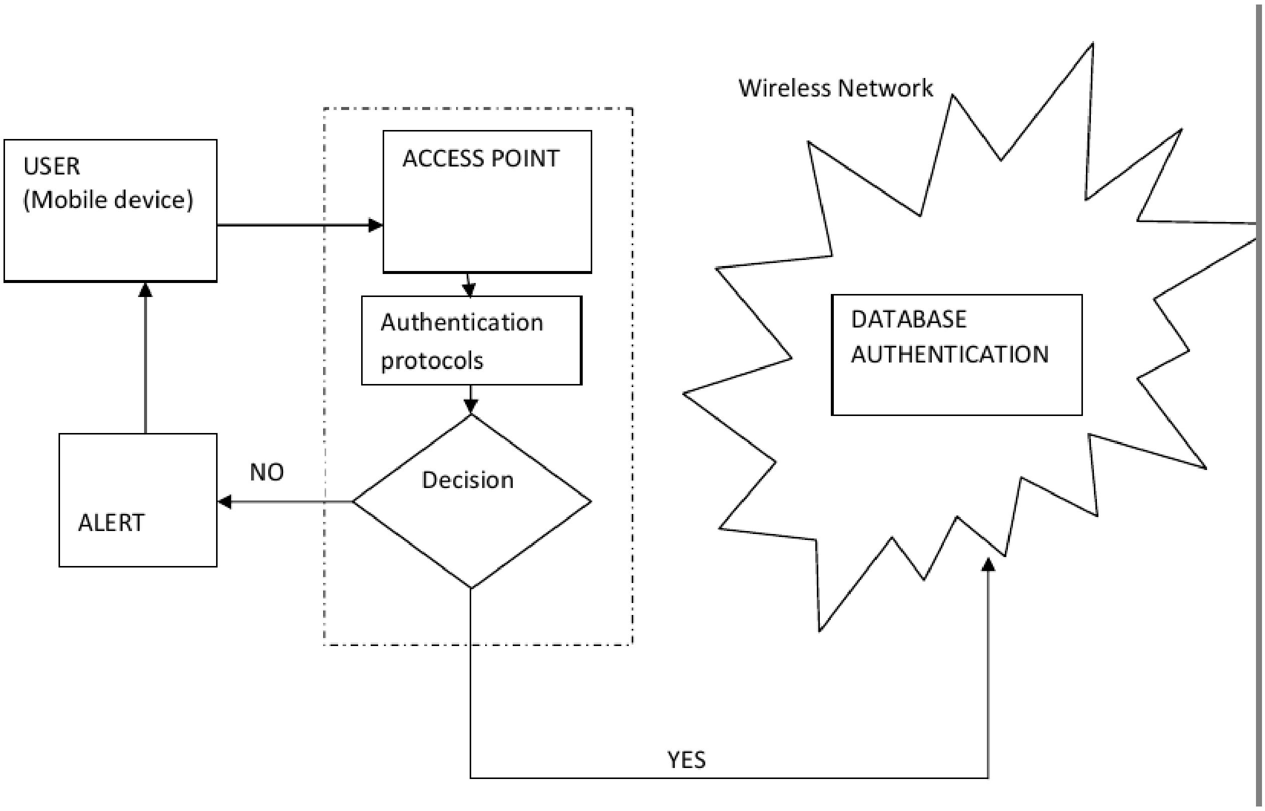


Figure: 5 Conceptual Model

The users are largely associated with the WLAN AP and the AP must have capability to connect with the network. For one to use the network one has to pass through the Authentication protocols and standards of a Wlan. The security mechanism should be efficiently proficient to identify the users and access points. The security method should be able to do Authentication, Authorization, and Accounting (AAA) through server. When a user requests a connection, the request is forwarded to a server that determines who the user is, as shown in figure 5. The authentication protocols determine whether a user is authenticated or not which determines whether a user is granted access to the network or not. The decision made is either Yes or No where an affirmative response means users are authorized to access the network with controlled access privileges, which is determined based on nature and level of tasks and activities to be performed by users. The system has additional security control since it controls all the operations of the user. By monitoring activities, the system has the ability to predict if an attack is about to happen based on certain user's habits.

Although no security system can ever be considered totally unbreakable, one Halil, 2006 stated that 802.11i RSN security seems to be a dependable. WLAN are known for the reducing costs in an organization network infrastructure because of the absence of wires and its mobility. Data is transmitted via radio frequency, which can be easily tapped using sniffer software’s.

4.4 Implementation Model

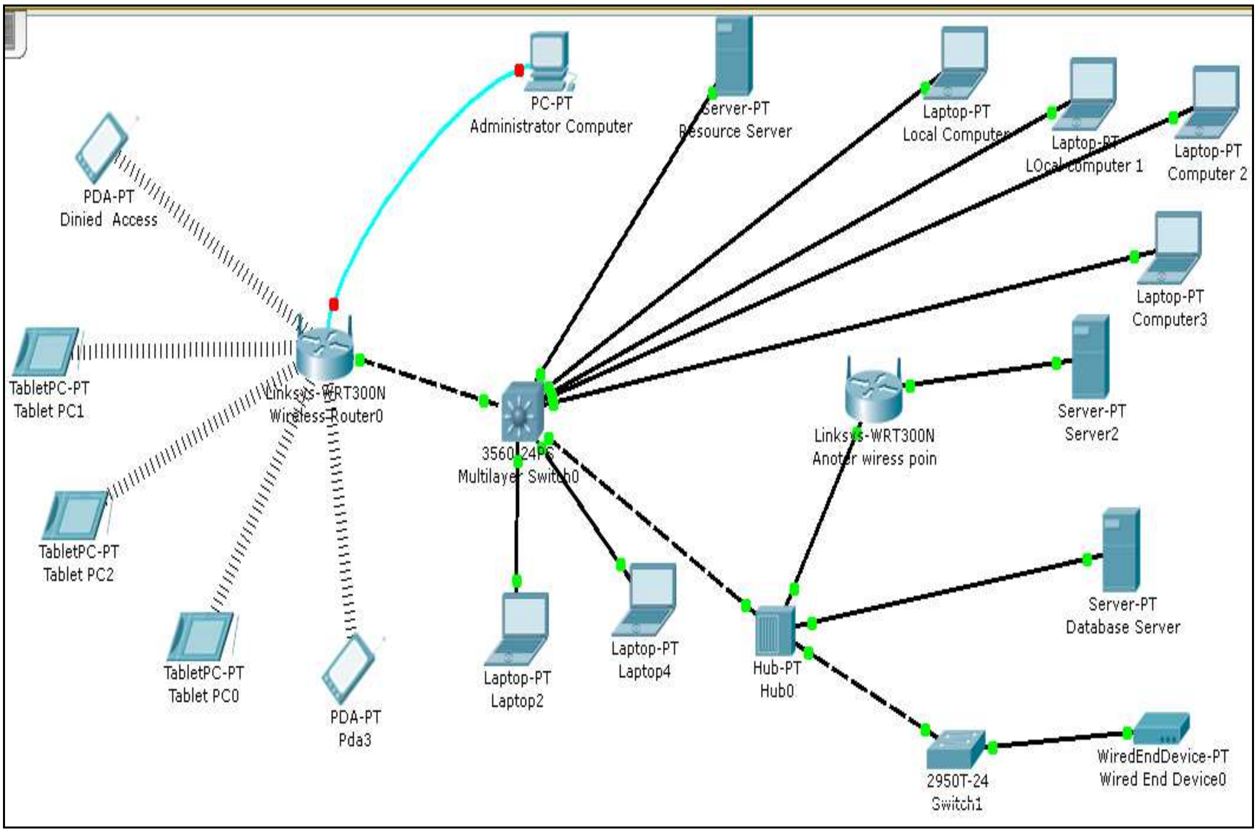


Figure: 6 Implantation model of Framework for enhancing wireless local area network security

The model enhances security by addressing the Wlan fundamentals by identifying users, the AP associated with them and the AP identities, Mac addresses, usernames, and ssid. Wlan standards 802.1i which is the Major secure security protocols for wireless LANs in figure 6 shows Authentications protocols for Wlan that is, CCMP, and RSNA, which validates and verifies credentials, secrets certificates of user who wants to use the network resources.

The Framework for enhancing wireless local area network security has method to detect wireless based sniffer software’s, by actively searching request frame on each channel where it is able to detect wireless activities.

The installation of a radio frequency monitoring mechanism such as RFMON, which offers detection wireless AP by specifically monitoring raw 802.11 frames to sense if there any broadcast frames, should be considered. A framework, which provides for authentication protocols and authorizes devices connecting to a network should also be considered, as this prevents a device from accessing the network until such device is cleared.

Authorisation and access control; allows access to networks and affects capabilities which has The security method for Authenticating, Authorising and Accounting (AAA) through server, that is, The security mechanism (AAA systems), that is, Closed Network with WPS, Firewall plus IEEE 802.1x and VPN. In this case, the VPN serves as a supplementary protection mechanism for the highly sensitive data including personal information.

While model 8 deals with message integrity and channel confidentiality. Wlan encryption and data integrity protocols, protocols for bootstraps, key exchanges, key refresh TKIP, CCMP are handled at this level.

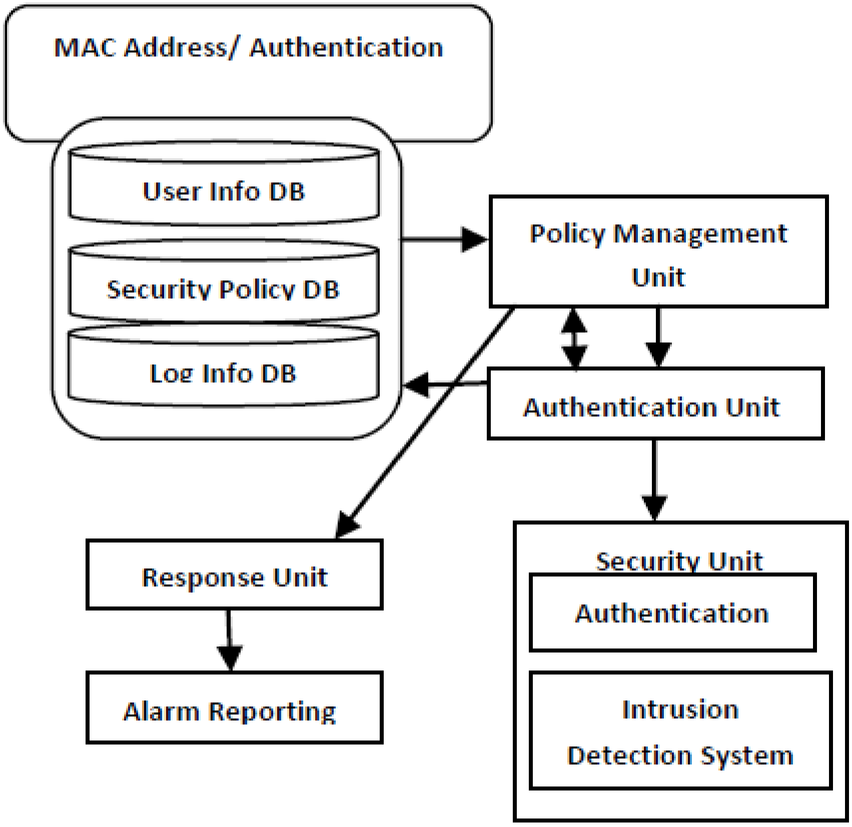


Figure: 7 Security Mechanisms

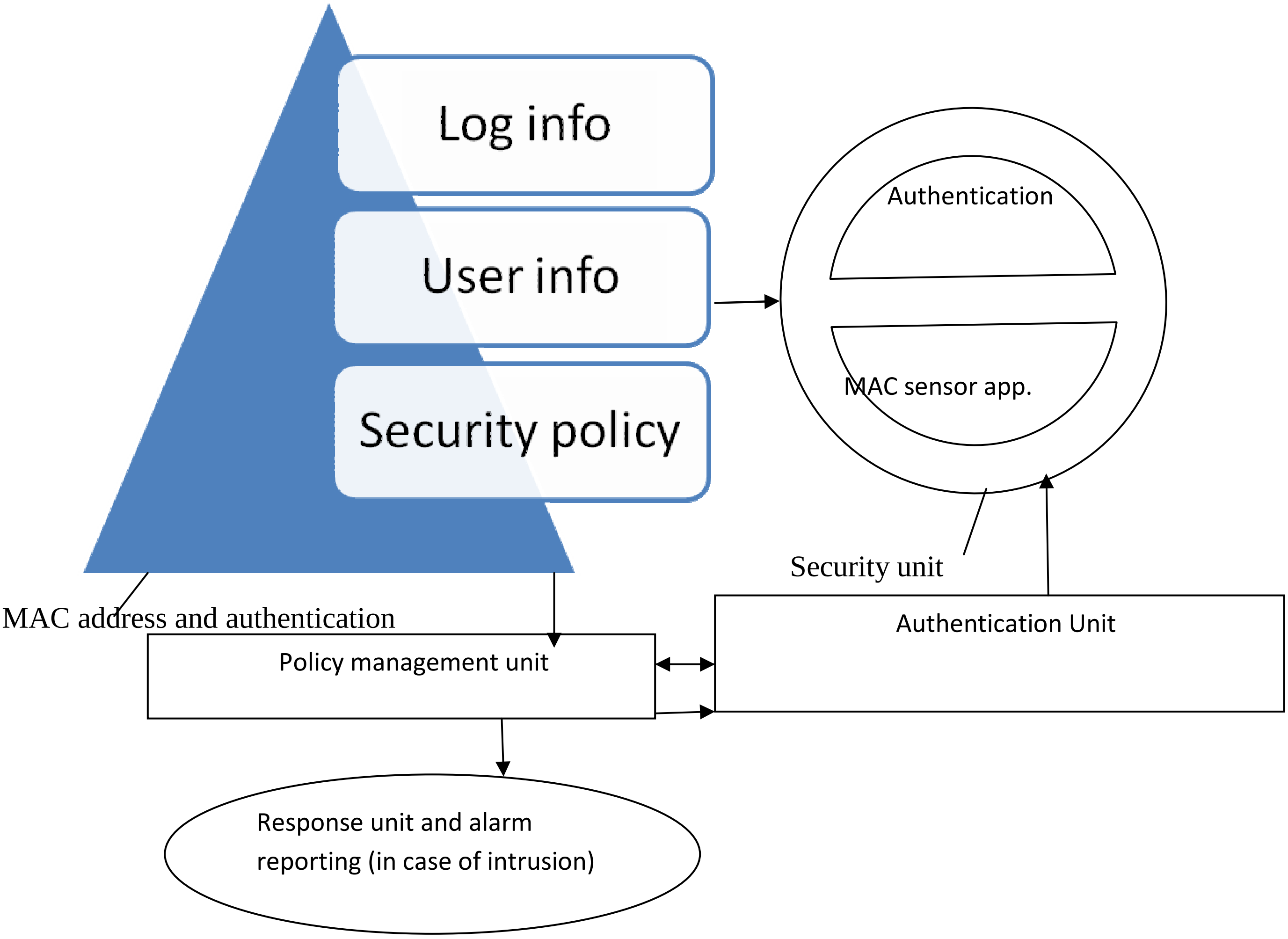
The Table below outlines a checklist for a secure deployable WLAN framework; this should be done after assessment;

S/No	Proposed Security Measure
1	Have WLAN Security Policy
2	WLAN To Be Broken Into SSIDS
3	Put Into Operation Access Controls
4	Utilize Virtual Private Network (VPN)
5	Application Of Encryption In Wireless Data
6	Solidify WLAN Infrastructure
7	Secure Wireless Clients/Implement MAC Address Filters
8	Scrutinize Wireless Traffic
10	Prevent Wireless Intrusions/ Activate Authentication Credentials
11	Enforce Network Security

Table 2: Framework for securing WLAN

CHAPTER 5: IMPLEMENTATION AND TESTING

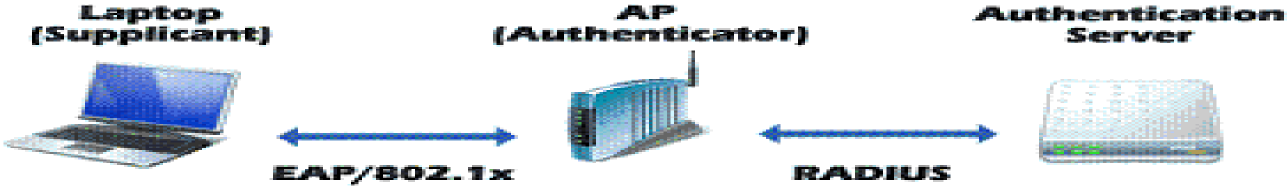
An expanded form of what goes on in Figure 7 is shown below:



The figure above is a clear explanation of what goes on inside the authentication management unit.

- In stage one, the user information is taken in
- In stage two, MAC filtering application comes in.
- The policy management unit ensures the WLAN protocols are followed
- The authentication unit provides basic authentication
- Response and alarm reporting unit notifies the administrator in case of any attacks or illegal access on the system.

Authentication



The security mechanism has a couple of features that enables it to ensure security over a wireless network as the thesis aims to illustrate. Among the key features, is a MAC/IP address filter, an application that runs through the database every 30 seconds to check for any unauthorized MAC addresses, there is also a feature that allocates keys to the users for access. This feature enables key distribution to users/clients in wireless networks. Bearing in mind that this has to be done in an unsecure environment elicits significant difficulty that necessitates establishment of a means to cater for those with and without deployment knowledge.

It is a security management approach to handle a key distribution by using the specific locations of data delivery using their MAC addresses, which ensures that data is not compromised during transit. In this case, the study implemented an application in a database that is in between the user and the main database where the data is stored in the network. In this first database, the information stored here is the user details, and in it lies the application for MAC filtering, intrusion detection application system and alarm unit. This database is our base station and has no other information that a hacker can benefit from if he accesses it. The 'external database' acts as a secure base station.

The use of a different key pool in storage of user login information details results in reduced connectivity over multiple deployments because nodes of different deployments do not share any keys and this enables easy auditing of security and helps in detection of intrusion. Communication with the main database once a user log in, is improved by using path key establishment, a secure direct link is created if there exists secure path between them, which is confirmed by connection history or user privileges.

In this cases, traditional schemes such as Kerberos that rely on trusted third party infrastructure, become less practical with regard to sensor networks, which function autonomously over a limited communication range. Similarly, lack of adequate resources render the implementation of Asymmetric Cryptosystems inconceivable owing the significant demand with regard to computation and memory, which makes algorithms such as Diffie-Hellman key agreement and RSA undesirable. Furthermore, symmetric key ciphers and hash functions have been indicated as relatively fast in contrast to digital signatures. Asymmetric cryptosystems cannot be used even to establish session keys because that would leave the nodes vulnerable to Denial of Service attacks A popular technique for key distribution for nodes with limited resources; little or no deployment knowledge is key redistribution.

This involves the loading of information required by the nodes for key establishment before their deployment. However, when a node is physically compromised, the keys present within the node are revealed to the attacker, which not only exposes the link of the captured node, but also the connections of the remaining nodes.

The nature of sensor networks is such that it is almost impossible to know which nodes would be within communication range of each other after deployment. There are instances when some nodes are more likely to be neighbours than others are and as such, the keys in each node can be decided by priority for security purposes. The precision involved when deploying a large number of nodes remains impracticable even as the exact position of the nodes is known. The approach illustrated in this study works for cases with and without deployment knowledge.

Our application enhances security by addressing the Wlan fundamentals by identifying users, AP identities associated with them, Mac addresses, usernames and passwords and SSid. Wlan standards 802.1i, which is the Major secure security protocols for wireless LANs, is also used in the part with the authentication protocols. Confirmation of details put in during login is done at this stage.

Authentications protocols for Wlan, that is, CCMP, RSNA validates and verifies credentials, secrets certificates of user who wants to use the network resources, at this stage, the user if confirmed is able to access the network if not, the user is taken back to the login page to star again with new login details.

Our framework for enhancing wireless local area network security has a method to detect wireless based sniffer software’s, by actively searching request frame on each channel where it is able to detect wireless activities. On identifying sniffer software or an unrecognized/unaccounted for user, it triggers the alarm system, notifies the administrator immediately, and terminates the connection immediately.

In this study, the adoption of RFMON, a radio frequency monitoring mechanism, is highly recommend. It can detect a wireless AP by specifically monitoring raw 802.11 frames to sense if there any broadcast frames. This mechanism provides for authentication, before authorizing devices to connect to a network, which prevents device from accessing the network until adequate vetting is done.

Authorization and access control facilitates access to the network and affects capabilities of various users in terms of their access levels and privileges. The security measure involving Authenticating, Authorizing, and Accounting (AAA) through server is often used. The AAA systems closed Network with WPS, a firewall, plus IEEE 802.1x and VPN where the VPN provides a supplementary protection mechanism for the sensitive data on the database such as user information, as earlier mentioned, hidden from the hacker in the secure base station pool.

The encryption level deals with message integrity and channel confidentiality. Wlan encryption and data integrity protocols, protocols for bootstraps, key exchanges, key refresh TKIP, CCMP are handled at this level. Similarly, it is at this level where our encryption mechanism enables us to encrypt our packets with the individuals MAC addresses for safe delivery to the user who sent the requests. This ensures that if a hacker tries to intercept the packets, they cannot decrypt them, since the messages use the MAC addresses for decryption.

CHAPTER 6: DISCUSSION OF RESULTS

6.1 Discussion of Results

This study hoped to develop an efficient framework that enhances data security in a wireless local area network especially within institutions. The study was to identify security weaknesses, vulnerabilities, and threats prevalent in the WLAN Environment that limit enterprise deployment of a WLAN, and evaluate the effectiveness of the WLAN security frameworks in addressing the Vulnerabilities identified, and then come up with a deployable WLAN security framework that will enhance security within the WLAN Environment.

In the past recent times, wireless networks have been widely spread and their use has become rampant in homes and corporate settings. This is due to the ease and convenience they come with, that well relates to the increasing innovation of portable devices that use wireless technology. The most outstanding problem with current WLANs is the security vulnerabilities that come with it. Presently, the IEEE 802.11b standard that employs the WEP algorithm to encrypt data, remains a popular wireless pre-set in various institutions. However, flaws with regard to the execution of the RC4 algorithm within WEP have led to compromised network systems that employ the IEEE 802.11b standard. As such, it is critical that the transmission of confidential data via WLANs under IEEE 802.11b standard be curtailed to a minimal.

Due to their unsecure nature, many algorithms have been created and improvements done to see to it that security is prioritized. In the wake of technological advances, it is prudent that wireless networks will grow more secure and wade off malicious attacks.

In the meantime, regular security risk assessments are necessary in order to generate a comprehensive list of vulnerabilities in a network and appreciate the severity each. This creates the need of coming up with a good security policy which is made to defend the network in all possible ways.

Our method of implementing the explained configuration and setup of a wireless architecture and embedding the application in the data bases as shown in the implementation model have proved to raise security levels of the wireless WLANs networks considerably. It does not entirely stop hackers/intruders from attacking the wireless network. However, the framework does the most important thing in the network protecting data. This ensures that even if the attacker gains access into the network he does not benefit much since he does not get access to the secured data, which is our main objective in trying to secure the network. Nevertheless, it is important to appreciate that security threats will always be there owing to the ever-evolving technology, which facilitates development in hardware and software with subsequent new threats.

6.2 Conclusions

Based on the finding of this study, the following conclusions were drawn:

1. The structure of WLAN technology has natural security issues, which expose the signals to attackers because the nodes and the end clients require to announce their presence through beacon frames.
2. Attacks are always inactive to active-on wireless LANs, and are aimed at compromising the network credibility through violation of confidentiality, integrity of information and network availability. Some of the attacks are less likely to inflict more damage than others are while their frequency varies significantly.
3. The flaws detected in Wi-Fi Protected Setup (WPS) Vie book, 2011 have not been fixed, however, a combination of security measures is required to increase further the security offered by WLAN technologies as shown in the implementation model.
4. Protection of networks against any attacks has proved impossible leaving prevention as the only option to minimize and bring down the risks to tolerable state. IEEE 802.11 standard provide initial security however, it is not fully recommended for high-level protection required for corporate network structures. This brings the need of creating a complex security structure to enhance security at different levels.
5. Risks evaluation procedures should be used to establish the mechanisms that should be deployed in for purpose of mitigating the risks connected with deployment of wireless technologies.

Wireless technology enjoys a growing popularity testament to the bundled convenience, cost sufficiency, and easy compatibility with other network setups and components. Wireless networks characterized by successful transmission of information over an electromagnetic wave system, such as radio waves to initiate communication as in the cases of Wireless PAN (Personal Area Networks) and Wireless LAN (Local Area Networks).

The WLANs are often identified by their standard, which is the 802.x with variations that include 802.11, 802.11a, 802.11b, and 802.11g. While the advantages of using wireless networks relate to mobility, and convenience, security concerns remain the greatest disadvantage of the platform.

6.3 Future Research

The security of wireless networks faces new threats each day due to the way it is rapidly evolving with cropping up of new technology. The researcher hopes updated with regard to issues surrounding networking and work to establish new solutions with every arising challenge in the field. However, the following issues need to be looked into further in the future research;

To study the cycle of the WLAN intruder, the research tries to help the network administrator think like a hacker, and this enables them to come up with counter attack measures. Due to the rapid changes growing with technology, continuous research of the same is recommended.

The databases have several limitations that require advanced improvements in future. This includes enhancing it in a way that not all the outcomes may materialise.The database should be converted into an executable file that can e used on any system, precluding that the MS Access application has to be installed on that particular system.

Coming up with a WLAN security policy would be useless if people do not take heed of it. Is therefore very important to create a user awareness model to create awareness to the users and equip them with necessary skills.

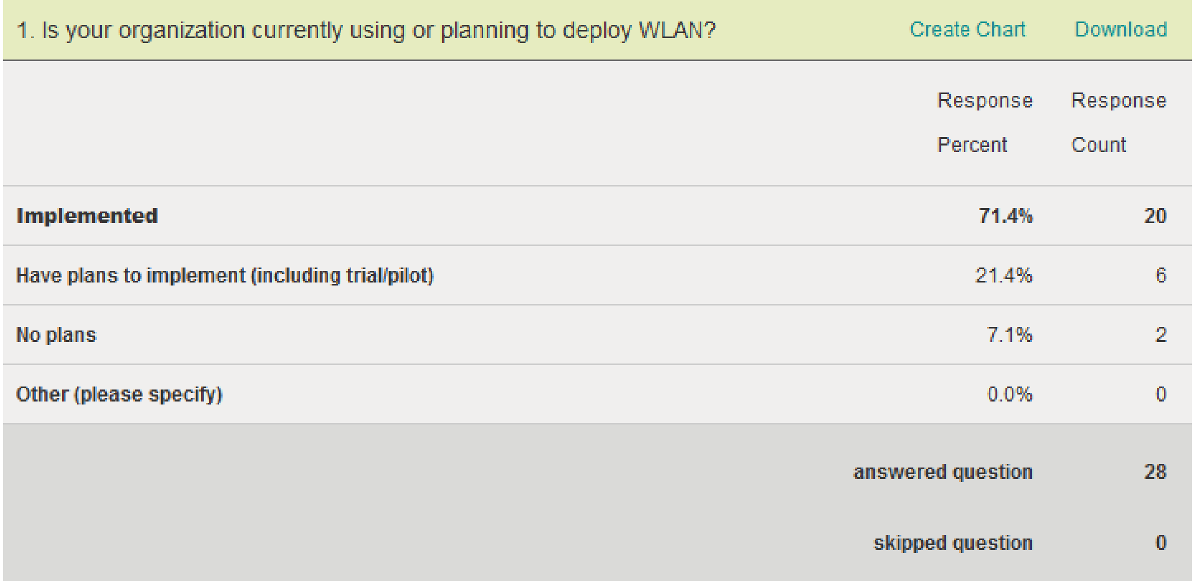
The researcher's interests include security and oS in wireless sensor networks, ad hoc networks, and cellular networks.

6.4 Summary

In this research, the study reviewed how security in wireless data networks has evolved over the last years. Moreover, the study highlights the role of divergence within the data transfer media, namely wired and wireless networks, in exposing the system to possible attacks. These are just but a few of the security issues experienced in WLAN wireless networks. Security hazards will always be around; they can only be avoided if the correct policies and standards are put in place. The 802.11i protocol promises to sort out most of the security issues found in its predecessor WEP, but since the standard is relatively new and many more protocols are coming up each day, only the future can tell us if the current standards are secure as they promise. Moreover, the study reveals some of the ways that can be utilized to improve the security of the wireless networks broadly, including those that have been tested in the past. However, the researcher strived to come up with a way of enhancing the security of data on a wireless network by implementing the security management unit in in the framework. Network security will continue elicits heated debate given that the integrity of networking remains at risk with numerous means to threaten data security. Both security and wireless communication will remain an interesting subject for decades. They reassure the need of ease of use and flexibility of communications in the computer world without jeopardizing the communicated content.

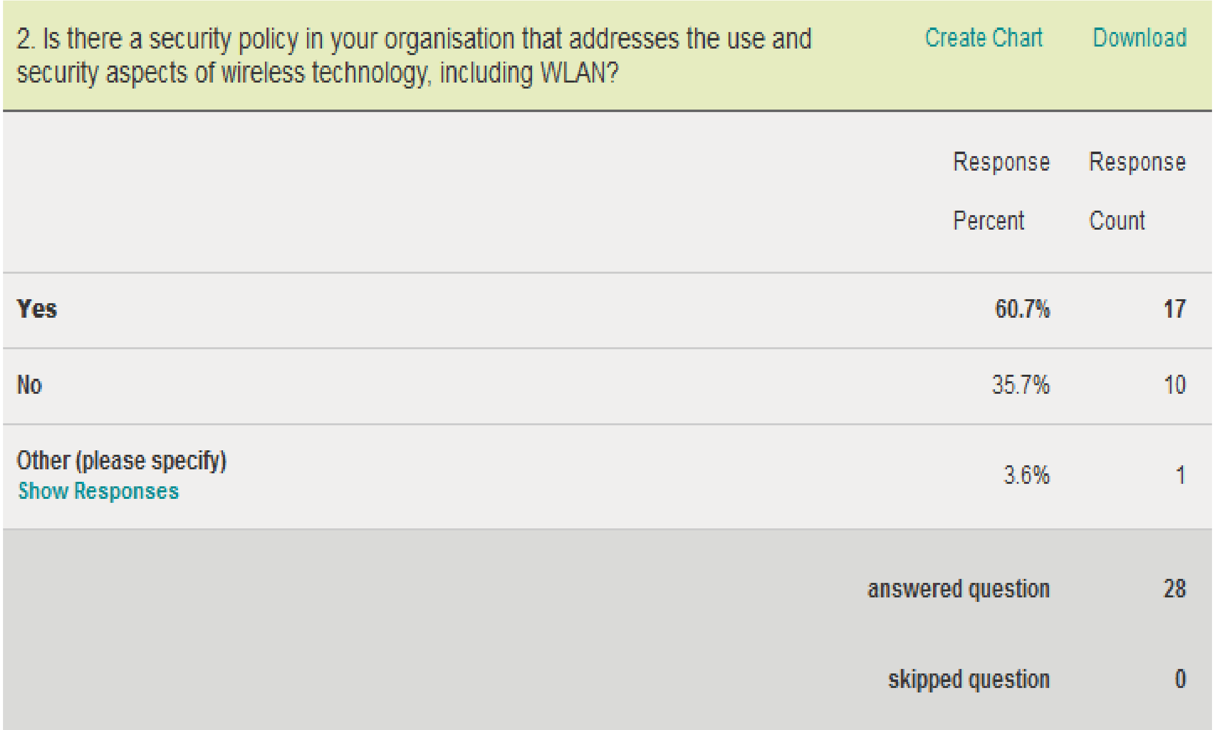
Appendix

A total of 25 Wireless local area network specialists from various agencies responded out of 35 surveyed. Certain questions have been sanitized as they contain sensitive information.


Create Chart
Download

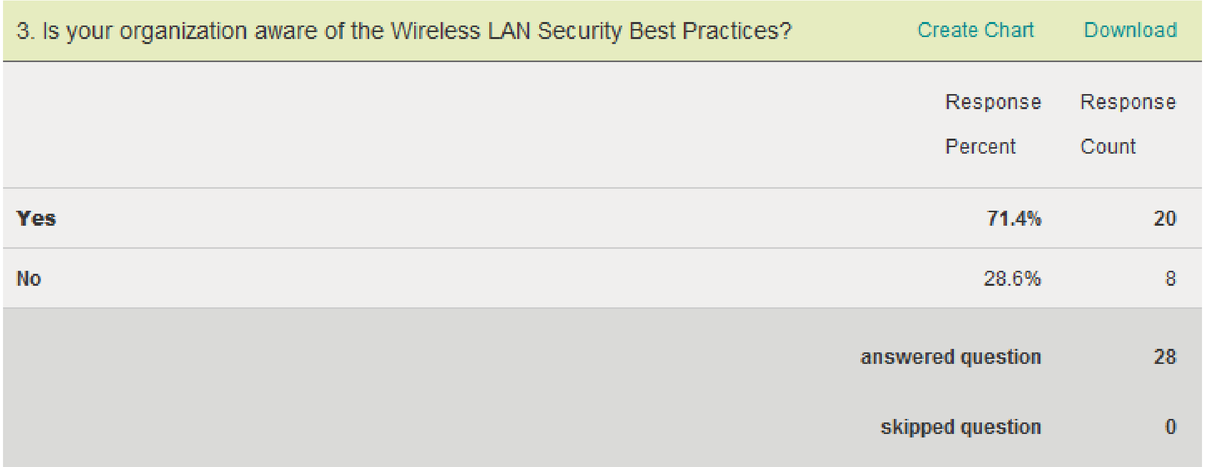
1. Is your organization currently using or planning to deploy WLAN?

	Response Percent	Response Count
Implemented	**71.4%**	**20**
Have plans to implement (including trial/pilot)	21.4%	6
No plans	7.1%	2
Other (please specify)	0.0%	0
	answered question	28
	skipped question	0


Create Chart
Download
Show Responses

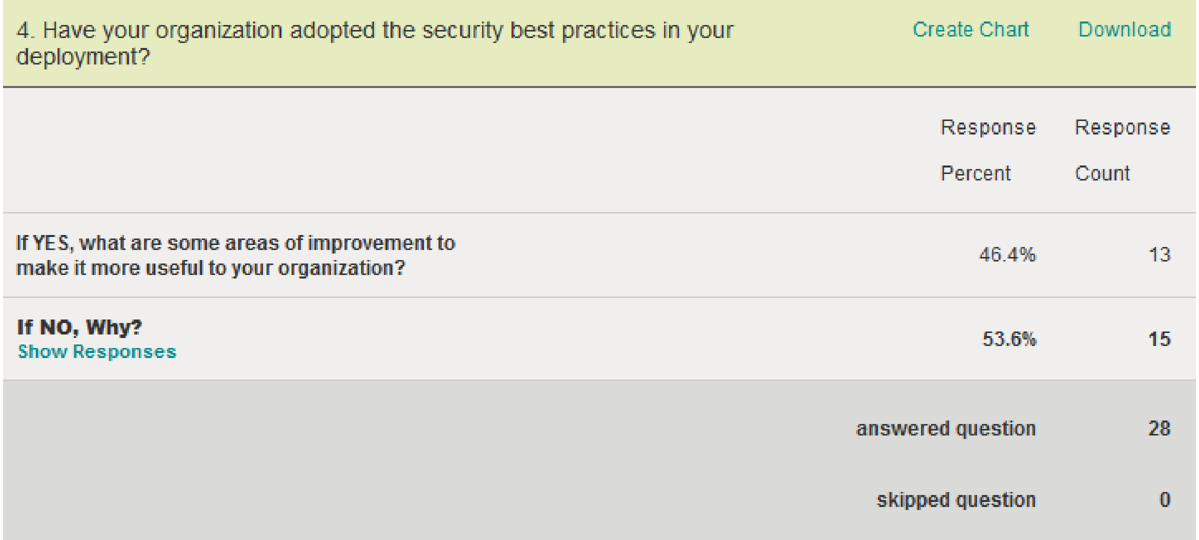
2. Is there a security policy in your organisation that addresses the use and security aspects of wireless technology, including WLAN?

	Response Percent	Response Count
Yes	**60.7%**	**17**
No	35.7%	10
Other (please specify)	3.6%	1
	answered question	28
	skipped question	0



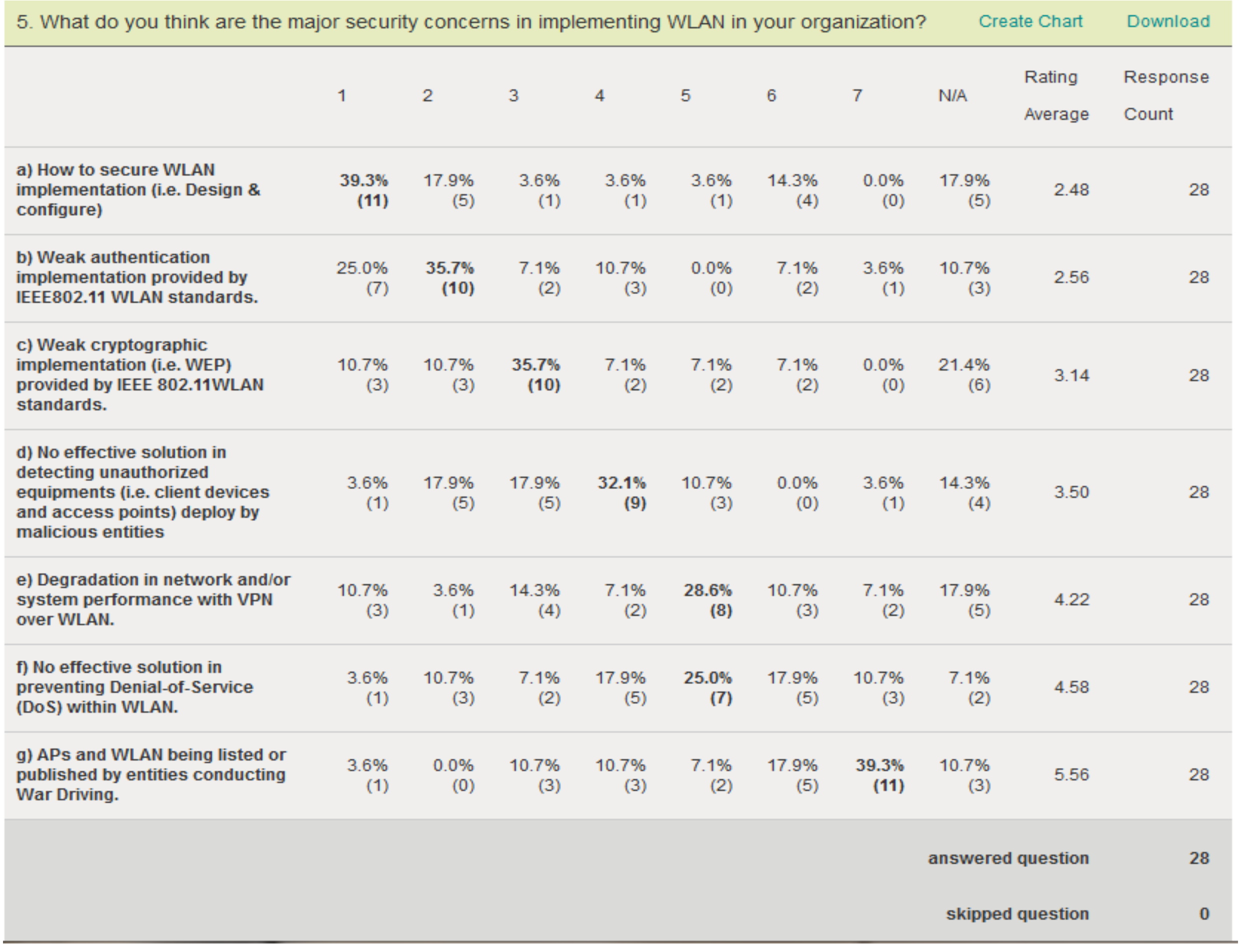
3. Is your organization aware of the Wireless LAN Security Best Practices?

	Response Percent	Response Count
Yes	**71.4%**	**20**
No	28.6%	8
	answered question	**28**
	skipped question	**0**



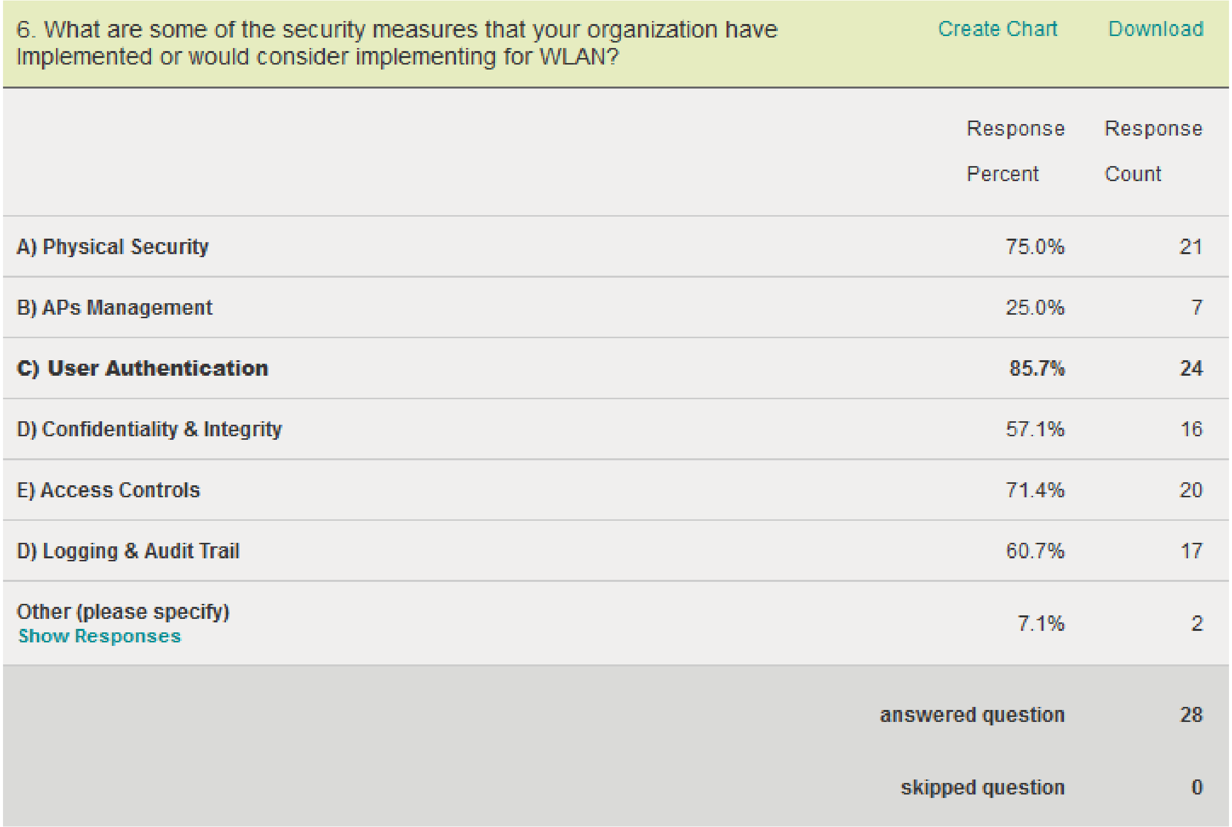
4. Have your organization adopted the security best practices in your deployment?

	Response Percent	Response Count
If YES, what are some areas of improvement to make it more useful to your organization?	46.4%	13
If NO, Why?	**53.6%**	**15**
	answered question	**28**
	skipped question	**0**



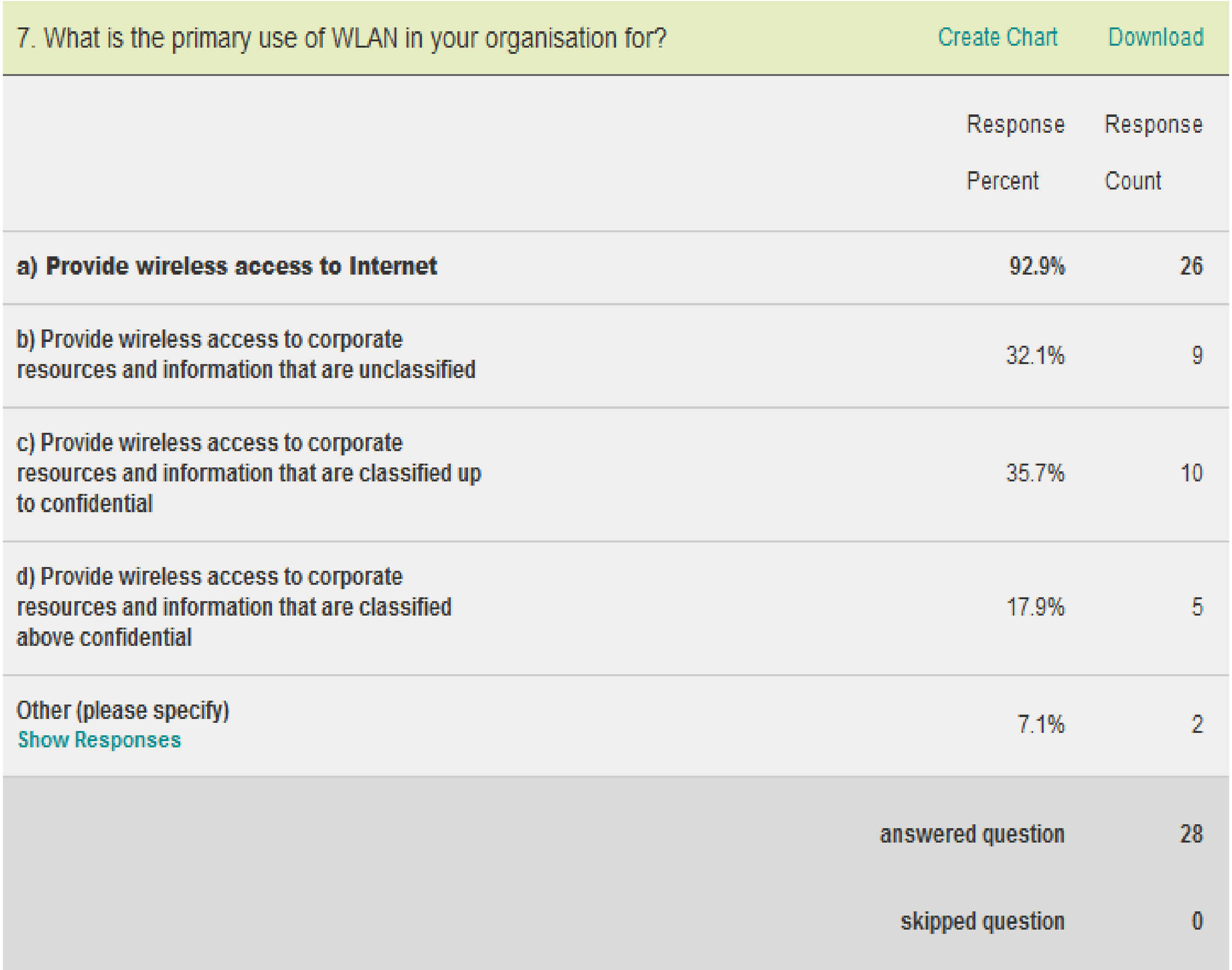
5. What do you think are the major security concerns in implementing WLAN in your organization?

	1	2	3	4	5	6	7	N/A	Rating Average	Response Count
a) How to secure WLAN implementation (i.e. Design & configure)	**39.3% (11)**	17.9% (5)	3.6% (1)	3.6% (1)	3.6% (1)	14.3% (4)	0.0% (0)	17.9% (5)	2.48	28
b) Weak authentication implementation provided by IEEE802.11 WLAN standards.	25.0% (7)	**35.7% (10)**	7.1% (2)	10.7% (3)	0.0% (0)	7.1% (2)	3.6% (1)	10.7% (3)	2.56	28
c) Weak cryptographic implementation (i.e. WEP) provided by IEEE 802.11WLAN standards.	10.7% (3)	10.7% (3)	**35.7% (10)**	7.1% (2)	7.1% (2)	7.1% (2)	0.0% (0)	21.4% (6)	3.14	28
d) No effective solution in detecting unauthorized equipments (i.e. client devices and access points) deploy by malicious entities	3.6% (1)	17.9% (5)	17.9% (5)	**32.1% (9)**	10.7% (3)	0.0% (0)	3.6% (1)	14.3% (4)	3.50	28
e) Degradation in network and/or system performance with VPN over WLAN.	10.7% (3)	3.6% (1)	14.3% (4)	7.1% (2)	**28.6% (8)**	10.7% (3)	7.1% (2)	17.9% (5)	4.22	28
f) No effective solution in preventing Denial-of-Service (DoS) within WLAN.	3.6% (1)	10.7% (3)	7.1% (2)	17.9% (5)	**25.0% (7)**	17.9% (5)	10.7% (3)	7.1% (2)	4.58	28
g) APs and WLAN being listed or published by entities conducting War Driving.	3.6% (1)	0.0% (0)	10.7% (3)	10.7% (3)	7.1% (2)	17.9% (5)	**39.3% (11)**	10.7% (3)	5.56	28
									answered question	**28**
									skipped question	**0**



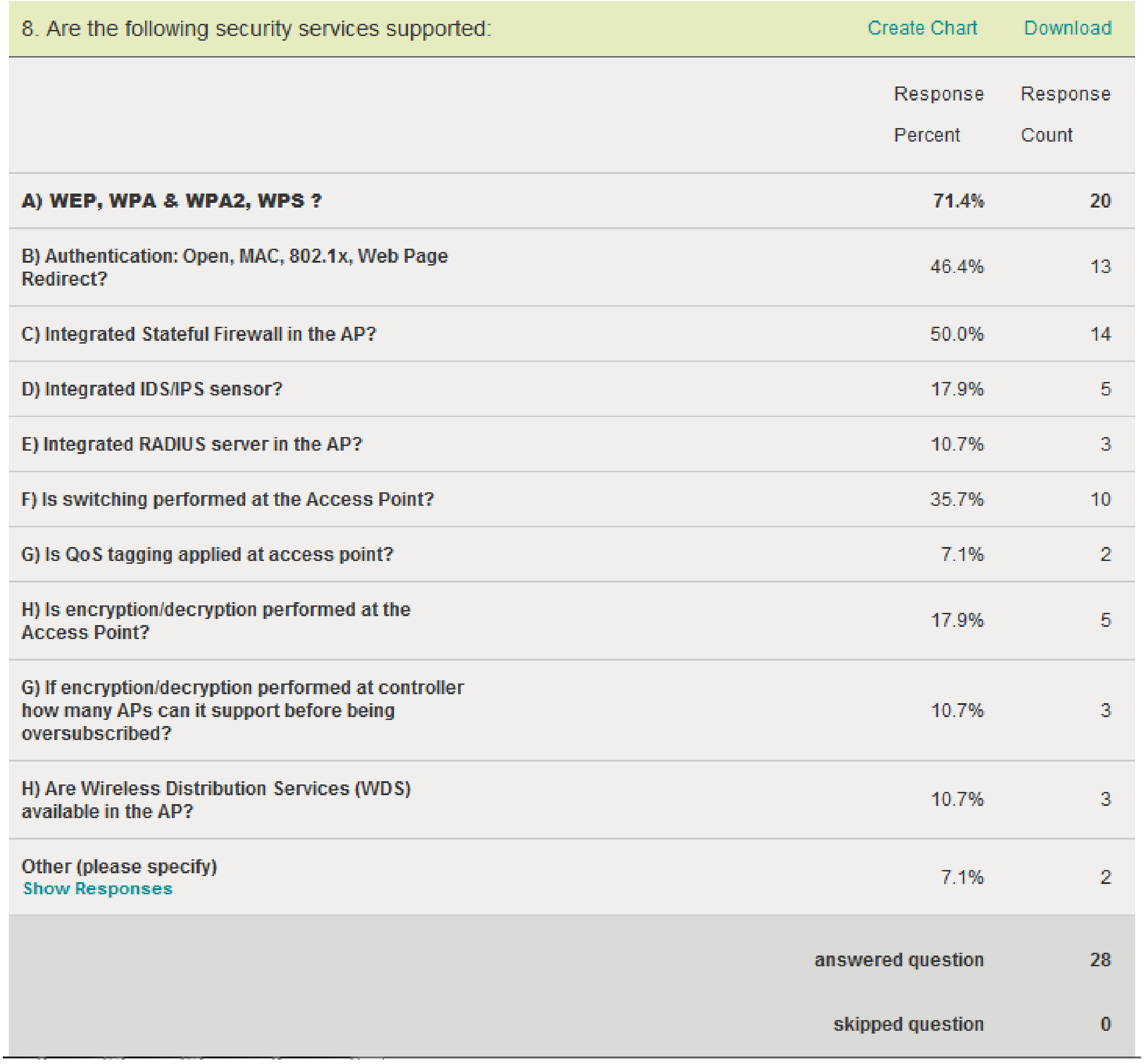
6. What are some of the security measures that your organization have Implemented or would consider implementing for WLAN?

	Response Percent	Response Count
A) Physical Security	75.0%	21
B) APs Management	25.0%	7
C) User Authentication	**85.7%**	**24**
D) Confidentiality & Integrity	57.1%	16
E) Access Controls	71.4%	20
D) Logging & Audit Trail	60.7%	17
Other (please specify) Show Responses	7.1%	2
	answered question	28
	skipped question	0



7. What is the primary use of WLAN in your organisation for?

	Response Percent	Response Count
a) Provide wireless access to Internet	92.9%	26
b) Provide wireless access to corporate resources and information that are unclassified	32.1%	9
c) Provide wireless access to corporate resources and information that are classified up to confidential	35.7%	10
d) Provide wireless access to corporate resources and information that are classified above confidential	17.9%	5
Other (please specify) Show Responses	7.1%	2
	answered question	28
	skipped question	0



8. Are the following security services supported:

	Response Percent	Response Count
A) WEP, WPA & WPA2, WPS ?	**71.4%**	**20**
B) Authentication: Open, MAC, 802.1x, Web Page Redirect?	46.4%	13
C) Integrated Stateful Firewall in the AP?	50.0%	14
D) Integrated IDS/IPS sensor?	17.9%	5
E) Integrated RADIUS server in the AP?	10.7%	3
F) Is switching performed at the Access Point?	35.7%	10
G) Is QoS tagging applied at access point?	7.1%	2
H) Is encryption/decryption performed at the Access Point?	17.9%	5
G) If encryption/decryption performed at controller how many APs can it support before being oversubscribed?	10.7%	3
H) Are Wireless Distribution Services (WDS) available in the AP?	10.7%	3
Other (please specify) Show Responses	7.1%	2
	answered question	28
	skipped question	0

Reference

1. Brian P. Crow, Indra Widjaja, Jeong Geun Kim, P. T. Sakai, .IEEE 802.11 Wireless Local Area Networks., IEEE Communications Magazine , Sept. 1997

2. Choi, Y.B., Muller, J., Kopek, C.V. and Makarsky, J.M. (2006) 'Corporate wireless LAN security: threats and an effective security assessment framework for wireless information assurance', Int. J. Mobile Communications, Vol. 4, No. 3, pp.266–290.

3. GAO, United States Government Accountability Office Report to Congressional Committees INFORMATION SECURITY

4. Federal Agencies Have Taken Steps to Secure Wireless Networks, but Further Actions Can Mitigate Risk ,November 2010

5. Henric Johnson, Arne A. Nilsson, Markus Fiedler, Wireless Network Security, conference paper , 2001

6. Wadlow Thomas ; The process of network security; designing and managing a safe network, 2000 ISBN 0-201-43317-6 NIST Special Publication 800-153, GUIDELINES FOR SECURING WIRELESS LOCAL AREA NETWORKS, Guidelines for Securing Wireless Local Area Networks (WLANs),Murugiah Souppaya and Karen Scarfone, September 2011

7. ©Siemens Enterpris Communications (July 2008): WLAN Security Today: Wireless more Secure than Wired. Siemens Enterprise Communications, p. 1.

8. US-CERT Technical Alerts(2012) Vulnerability note VU#723755: Wi-Fi Protected Setup pin brute force vulnerability

9. SANGIT, Z. B. M.,(2007). WIRELESS SECURITY ASSESSMENT, ON THE FTMSK2 BUILDING. thesis ,university of technology Mara

10. Vacca, J., 2006. Giude to Wireless Network Security. Springer, Volume XXIV, p. 58.

11. Min-kyu Choi, Rosslin John Robles, Chang-hwa Hong, and Tai-hoon Kim, (2008) Wireless Network Security: Vulnerabilities, Threats and Countermeasures. International Journal of Multimedia and Ubiquitous Engineering Vol. 3, No3(3), pp. 77.

12. N. Borisov, I. G. &. D. W., 2008. isaac. [Online] Available at: <http://www.isaac.cs.berkeley.edu/isaac/wepfaq. [Accessed 26 april 2012].

13. Baird., M. L. a. R., July, 2002.. Advanced 802.11 attack. Black Hat. Las Vegas,, s.n.

14. Braunton, G., 2004. A security Assessment Methodology. GSEC Practical Assignment, 29 January, 1.4b(option 1), p. 4.

15. Burell, J., 2008. Wireless Local Area Networking: Security Assessment and Countermeasures IEEE 802.11 Wireless Networks. telecom.gmu.edu/publications/Jim-Burrell-December-2002.pdf.

16. Halil Ibrahim BULBUL, I. B. O., 2006. Comparison of WEP (WiredEquivalent Privacy) Mechanism, WPA (Wi-Fi ProtectedAccess) and RSN (Robust Security Network) SecurityProtocols.,Gazi University. Wireless Network Security, pp. 1-7.

17. Lane, H. D., 2005. Security Vulnerabilities and. GIAC Security Essentials Certification (GSEC), Volume 1.4c, pp. 4-7.

18. Mitchell, C. H. a. J. C., 2005. Security Analysis and Improvements for IEEE 802.11i. Electrical Engineering and Computer Science Departments, Stanford University, Stanford CA 94305, pp. 1-19.

19. Stephen Northcutt, J. N., 2002. Network Intrusion Detection. 3rd ed. s.l.:Team Lib.

20. Viehbook, S., December 27, 2011. Wi-Fi Protected Setup PIN brute force vulnerability, usa: USA-CERT/CC.

21. Nasre, S., 2004. Wireless Lan Security. Information Security, Issue IT 6823 Information Security.

22. Maharaj, N. S. a. M., 2011. Alternation 18,1 (2011) 318 - 335 ISSN 1023-1757. Wireless Network Security, 18 january , 2011 p. 324.

23. PROF. RATHNAKAR, D. V. D. P. R., 2009. Wireless LAN Security – Challenges and Solutions. International Journal of Computer and Electrical Engineering,, No. 3, August 2009, 1(1793-8163), p. 256.

24. Sprint Proprietary, 2004. KCCMG Impact Conference, s.l.: Sprint.

25. Gayal S and S. A. Vetha Manickam, (2002). Wireless LAN Security Today and Tomorrow. Pune, India: Center for Information and Network Security, Pune University, URL: http://www.itsec.gov.cn/docs/20090507163620550203.pdf

26. A Detailed Study on Wireless LAN Technologies Vijay Chandramouli Department of Computer Science and Engineering The University of Texas at Arlington vmouli@uta.edu

27. Young B. Choi* Department of Computer Information Systems and Management Science James Madison University 800 South Main Street Harrisonburg, VA 22807-0001, USA E-mail: choiyb@jmu.edu *Corresponding author, Jeffrey Muller Integrated Science and Technology and School of Media Arts and Design James Madison University 800 South Main Street Harrisonburg, VA 22807-0001, USA E-mail: mullerjx@jmu.edu Christopher V. Kopek and Jennifer M. Makarsky James Madison University 800 South Main Street Harrisonburg, VA 22807-0001, USA E-mail: kopekcv@jmu.edu E-mail: makarsjm@jmu.edu

28. 0163-6804/97/$10.00 © 1997 IEEE IEEE Communications Magazine • September 1997, IEEE 802.11 Wireless Local Area Networks Brian P. Crow, The MITRE Corporation Indra Widjaja, Fujitsu Network Communications Jeong Geun Kim, University of Arizona Prescott T. Sakai, Cypress Semiconductor

29. SECURE WIRELESS NETWORKING USING SSL VPNS; Rysavy Research White Paper; Page 3, Prepared by Peter Rysavy, 2005 http://www.rysavy.com 1-541-386-7475

30. Security Vulnerabilities and Wireless LAN Technology Heather D. Lane, Location:Virginia, February 6, 2005

31. Smyth R. (2004): “Exploring the Usefulness of a Conceptual Framework as a Research Tool: A Researcher's Reflections.” Issues In Educational Research, Volume 14

32. Professor Roger Vauger,2008 Bournemouth university. Presentation

33. Jonathan wiessWIRELESS NETWORKS: Security Problems and SolutionsSANS Institute 2002

34. AF19 FA27 2F94 998D FDB5 DE3D F8B5 06E4 A169 4E46

35. The Importance of Security Awareness Training, Cindy Brodie , GIAC Gold Certification, 2009 June 30th 2008

36. EUSSO, 54Mbps Wireless-G Cardbus Adapter: Linking your Computer with Wireless G network, retrieved 16 April 2008, <http://www.eusso.com/Models/Wireless/UGL2454-01R/UGL2454- 01R.htm#Diagram

37. Vollbrecht, John, David Rago, and Robert Moskowitz (2002). “Wireless LAN Access Control and Authentication”, a white paper from Interlink Networks Resource Library, http://www.interlinknetworks.com/images/resource/WLAN_Access_Control.p

38. Wright J. (2003). “Detecting wireless LAN MAC address spoofing,” URL: www.uninett.no/wlan/download/wlan-mac-spoof.pdf

39. Woodward A, "Recommendations for wireless network security policy: an analysis and classification of current and emerging threats and solutions for different organisations", in Proc. 3rd Australian Information Security Management Conference, Perth, Western Australia, 2005, pp. 133-140.

40. Jihwang Yeo, Moustafa Youssef, and Ashok Agrawala. 2004. A framework for wireless LAN monitoring and its applications. In Proceedings of the 3rd ACM workshop on Wireless security (WiSe '04). ACM, New York, NY, USA

41. Vollbrecht, John, David Rago, and Robert Moskowitz (2002). “Wireless LAN Access Control and Authentication”, a white paper from Interlink Networks Resource Library, http://www.interlinknetworks.com/images/resource/WLAN_Access_Control.p

42. Jihwang Yeo, Moustafa Youssef, and Ashok Agrawala. 2004. A framework for wireless LAN monitoring and its applications. In Proceedings of the 3rd ACM workshop on Wireless security (WiSe '04). ACM, New York, NY, USA