

**AN ASSESMENT OF THE SECURITY OF WIRELESS CAMPUS NETWORKS
IN SELECTED UNIVERSITIES IN KENYA**

BY

OTIENO, SAMSON OOKO

**A THESIS SUBMITTED IN PARTIAL FULFILMENT OF THE
REQUIREMENTS FOR THE AWARD OF THE DEGREE OF MASTER OF
SCIENCE IN INFORMATION TECHNOLOGY, DEPARTMENT OF
INFORMATION TECHNOLOGY, SCHOOL OF INFORMATION SCIENCES**

**MOI UNIVERSITY
ELDORET**

2022

DECLARATION

DECLARATION BY THE CANDIDATE:

This thesis is my original work and has not been presented for degree in any other University. No part of this thesis may be reproduced without prior permission of the author and/or Moi University.

Otieno Samson Ooko 

Date. 07/02/2022

IS/MPHIL/039/011


DECLARATION BY THE SUPERVISORS:

This thesis has been submitted for examination with our approval as university supervisors.

Mr. Shadrack Metto

Date.....

(Moi University, Eldoret, Kenya)\

Prof. Edwin O. Ataro 

Date. 18/02/2022

(Moi University, Eldoret, Kenya)

DEDICATION

To my only wife, Bedina, my son Dylan and my loving Parents, Mr. Robert Ooko & Mrs. Irene Ooko for their support and inspiration.

ABSTRACT

The use of wireless networks in institutions of higher learning is gaining popularity due to its flexibility. With wireless campus networks, students are able to use their mobile devices to access lecture materials, watch lecture videos, access online campus resources, attend online classes and do exams, assignments and quizzes irrespective of the time or location. The use of wireless campus networks also enhances collaboration and teamwork among students and faculty. However, due to its being uncontrolled medium, wireless networks are prone to more security risks as opposed to the traditional local area networks. Anyone who can access the signal can be able to apply different techniques to gain access to the network without permission. Cases of hacking into wireless networks have been reported across the globe, with universities and other learning institutions being the main targets. With the reviewed literature showing that security of wireless networks is usually an afterthought and no studies had been done to assess the security of wireless networks in Kenya. This study was therefore aimed at assessing the security of wireless networks in selected universities in Kenya and thereafter proposed an Online Wireless Network Security Assessment Tool (OWNSAT) and a model for securing such networks. The study was guided by the game theory. A qualitative research design was applied in the study. The data collection tool included; practical experiments, personal interviews, and covert observation. Data was collected from purposively selected 20 universities in Kenya. From an analysis of the collected data it was evident that there were major areas of concern that needed to be addressed by network administrators to improve on the security of their networks. Given that no single tool was found that could be used to assess security of wireless networks, the proposed OWNSAT is an invaluable contribution to this area of study. In addition, the recommended model can be used to ensure more secure wireless networks leading to many advantages for universities.

Key Words: *Wireless Campus Networks, Security of Wireless Networks, Wireless Network Security Assessment, Wireless Networks*

TABLE OF CONTENTS

| | |
|---|-----------|
| DECLARATION..... | ii |
| DEDICATION | iii |
| ABSTRACT | iv |
| TABLE OF CONTENTS..... | v |
| LIST OF TABLES | ix |
| LIST OF FIGURES | x |
| LIST OF ABBREVIATIONS | xii |
| ACKNOWLEDGEMENT | xiv |
| CHAPTER ONE | 1 |
| INTRODUCTION | 1 |
| 1.0 Overview | 1 |
| 1.1 Background to the Study..... | 1 |
| 1.1.1 The Need for Wireless Networks..... | 1 |
| 1.1.2 Security of Wireless Networks | 4 |
| 1.1.3 Wireless Network Security Assessment..... | 8 |
| 1.1.4 The Need for the Study | 9 |
| 1.3 Statement of the Problem..... | 9 |
| 1.4 Aim | 11 |
| 1.5 Specific Objectives | 12 |
| 1.6 Research Questions..... | 12 |
| 1.7 Scope of the Study | 12 |
| 1.8 Limitations of the Study..... | 13 |
| 1.9 Assumptions of the Study | 13 |
| 1.10 Significance of the Study | 13 |
| 1.11 Chapter Summary | 14 |
| CHAPTER TWO | 16 |
| LITERATURE REVIEW | 16 |
| 2.1 Introduction | 16 |
| 2.2 Theoretical Framework..... | 16 |

| | |
|---|-----------|
| 2.2.1 Game Theory | 17 |
| 2.2.2 Relevance of the Game Theory to the Study | 18 |
| 2.2.3 Systems Theory..... | 19 |
| 2.2.4 Relevance of the Systems Theory to the Study | 22 |
| 2.3 Wireless Networks..... | 22 |
| 2.4 Risks in Wireless Networks | 25 |
| 2.5 Wireless Network Threats..... | 27 |
| 2.6 Wireless Network Security Testing | 30 |
| 2.7 Study Gaps | 31 |
| 2.8 Summary | 32 |
| CHAPTER THREE..... | 34 |
| RESEARCH DESIGN AND METHODOLOGY | 34 |
| 3.1 Introduction | 34 |
| 3.2 Research Design | 34 |
| 3.2 Population and Sampling | 34 |
| 3.2.1 Target Population..... | 34 |
| 3.2.2 Sample Size | 35 |
| 3.2.3 Sampling..... | 36 |
| 3.3 Data Collection..... | 36 |
| 3.3.1 Data Collection Instruments | 36 |
| 3.4 Quality Control..... | 39 |
| 3.5 Data Collection Procedure | 40 |
| 3.6 Statistical Treatment of Data..... | 40 |
| 3.7 Ethical Considerations | 40 |
| CHAPTER FOUR | 42 |
| DATA PRESENTATION, ANALYSIS AND INTERPRETATION | 42 |
| 4.0 Introduction | 42 |
| 4.1 Description of Respondents | 42 |
| 4.2 Security Risks Associated Wireless Campus Networks | 43 |
| 4.3 Security Measures in Place for Wireless Campus Networks | 56 |

| | |
|---|-----|
| 4.4 Vulnerabilities of the Wireless Campus Networks..... | 66 |
| 4.5 Measures and Tools for Ensuring Improved Security of Wireless Networks..... | 69 |
| CHAPTER FIVE | 71 |
| SYSTEM DEVELOPMENT AND IMPLEMENTATION | 71 |
| 5.0 Introduction | 71 |
| 5.1 System Development Method | 71 |
| 5.2 System Requirements..... | 73 |
| 5.3 System Development | 75 |
| 5.2.1 System Design | 76 |
| 5.2.2 User Interface Design..... | 78 |
| 5.2.3 OWNSAT Database Management System (DBMS) | 80 |
| 5.2.4 The Main Application and Interface | 80 |
| 5.2.5 System Implementation..... | 88 |
| 5.2.6 System Validation and Verification..... | 88 |
| 5.2.7 Difference with other Tools..... | 89 |
| CHAPTER SIX | 90 |
| SUMMARY, CONCLUSION AND RECOMMENDATIONS | 90 |
| 6.0 Introduction | 90 |
| 6.1 Summary | 90 |
| 6.2 Findings and Discussion | 91 |
| 6.2.1 Findings on Research Question 1 | 92 |
| 6.2.2 Findings on Research Question 2 | 94 |
| 6.2.3 Findings on Research Question 3 | 96 |
| 6.2.4 Findings on Research Question 4 | 97 |
| 6.3 Conclusion..... | 97 |
| 6.4 Recommendations..... | 98 |
| 6.5 Suggestions for Future Research | 103 |
| REFERENCES | 104 |
| APPENDIX I: INTERVIEW SCHEDULE | 108 |
| APPENDIX II: OBSERVATION GUIDE | 110 |

APPENDIX III: NACOSTI CLEARANCE.....111
APPENDIX IV: SAMPLE STAKEHOLDER INPUT112

LIST OF TABLES

| | |
|---|----|
| Table 4.1: Transcription Summary of Responses from the Universalities | 43 |
|---|----|

LIST OF FIGURES

| | |
|--|----|
| Figure 1: Growth in Malware Infections (Firch, 2021) | 4 |
| Figure 2.0: Game Theory in Network Security (Liang & Xiao, 2013) | 19 |
| Figure 2.1: An Open System..... | 20 |
| Figure 2.3: Closed System | 21 |
| Figure 4.1: Frequency of Network Upgrades by the Network Administrators..... | 45 |
| Figure 4.2: Wireless Router Upgrade Status..... | 46 |
| Figure 4.3: Wireless Access Points Upgrade Status..... | 46 |
| Figure 4.4: Frequency of Conducting Security Assessments | 47 |
| Figure 4.5: Rogue Access Points..... | 49 |
| Figure 4.6: Disposal Methods | 49 |
| Figure 4.7: Wireless Router System Log..... | 51 |
| Figure 4.8: Automated System Logging..... | 52 |
| Figure 4.9: Network Configuration | 52 |
| Figure 4.10: Successful Guest Can Discoveries..... | 54 |
| Figure 4.11: Nmap Guest Scan Out Put..... | 55 |
| Figure 4.12: IP Addressing Technique used | 56 |
| Figure 4.13 Existence of Policy | 57 |
| Figure 4.14: User Awareness Training..... | 58 |
| Figure 4.15: Physical Security | 59 |
| Figure 4.16 Indoor AP Physical Locations | 60 |
| Figure 4.17 Outdoor AP Physical Locations | 60 |
| Figure 4.18 Router Traffic Statistics | 62 |
| Figure 4.19 Nmap Host Details..... | 64 |
| Figure 4.20: Intrusion Detection Logs..... | 66 |
| Figure 4.21 AP Broadcast beyond Boundary..... | 67 |
| Figure 4.22: Overlapping AP Channels | 68 |
| Figure 4.23: AP SSID Broadcast..... | 69 |
| Figure 5.1: Prototype Model | 73 |

| | |
|---|----|
| Figure 5.2: OWNSAT Use Case Diagrams | 77 |
| Figure 5.3 Registration Screen | 81 |
| Figure 5.4: Log in Page..... | 82 |
| Figure 5.5: Password Reset Link..... | 82 |
| Figure 5.6: Password Reset Screen | 83 |
| Figure 5.7: Users Main Page..... | 84 |
| Figure 5.8: Assessment Page | 85 |
| Figure 5.9: Recommendations Page | 87 |
| Figure 5.10: Responses Review Page..... | 88 |
| Figure 6.1 Wireless Network Security Model..... | 99 |

LIST OF ABBREVIATIONS

| | |
|---------------|---|
| AP | Access Point |
| ARP | Address Resolution Protocol |
| BYOD | Bring Your Own Device |
| DBMS | Database Management System |
| DHCP | Dynamic Host Control Protocol |
| DoS | Denial of Service |
| DS | Distribution System |
| DSL | Digital Subscriber Line |
| ICT | Information and Communication Technology |
| IDS | Intrusion Detection System |
| IEEE | Institute of Electrical and Electronics Engineers |
| IP | Internet Protocol |
| IT | Information Technology |
| LAN | Local Area Network |
| LIA | Letter of Interim Authority |
| MAC | Medium Access Control |
| NIST | National Institute of Standards and Technology |
| OS | Operating System |
| OWNSAT | Online Wireless Network Security Assessment Tool |
| PC | Personal Computer |
| PHP | Hypertext Preprocessor |
| SNMP | Simple Network Monitoring Protocol |

| | |
|--------------|---------------------------------|
| SSID | Service Set Identifier |
| STA | Session-Termination-Answer |
| TCP | Transmission Control Protocol |
| UDP | User Datagram Protocol |
| VLAN | Virtual Local Area Network |
| VPN | Virtual Private Network |
| WDS | Wireless Distribution System |
| WEP | Wired Equivalent Privacy |
| Wi-Fi | Wireless Fidelity |
| WLAN | Wireless Local Area Network |
| WNSM | Wireless Network Security Model |
| WPA2 | Wi-Fi Protected Access 2 |

ACKNOWLEDGEMENT

I am grateful to the almighty God for blessings upon my life and leading me this far. I thank Him for the good health and resources that made it possible for me to undertake this research.

I would like to acknowledge the invaluable support offered by my supervisors Prof. Edwin Ataro, Dr. Harrison Bii and Mr. Shadrack Metto. I thank you for your dedicated support and guidance throughout the process. I do appreciate your encouragement and willingness to share your experiences. You have instilled in me a sense of self confidence and adequacy to conduct this and future research. I have learnt a lot from your supervision and I will be forever grateful.

My sincere appreciation goes to my loving family: to my dear wife Bedina, my son Dylan. my parents, my brothers and sisters for your prayers and encouragements during this research. I thank you for your patience, moral support and understanding.

In a special way I would like to thank the University of Eastern Africa, Baraton administration for giving me time off duty to enable me conduct this research. I would like to register my gratitude to Ms. Carolyn Hurst for her consideration and encouragements when needed. I thank all my work colleagues for helping when I was away.

I also appreciate the moral support of my colleagues in Moi University and friends, specifically Tony, Kirui and Rose, thank you for your encouragement, ideas and for being there. To all my lecturers that saw me through the course. I thank you.

CHAPTER ONE

INTRODUCTION

1.0 Overview

In this chapter the background to the motivation, statement of the problem, aims, specific objectives, research questions, scope of the study, limitations of the study, assumptions of the study, significance of the study and a summary of the chapter are presented.

1.1 Background to the Study

1.1.1 The Need for Wireless Networks

The success of any organization can be attributed to how best they manage information hosted both within the organization, information on transit, or information that is hosted externally (Artit, 2012). This means that communication of information is an integral part of the management process hence the need for well-designed and secure communication infrastructure within the organization.

The 2013 KENET e-readiness survey report concluded that universities in Kenya had enough measures in place and were ready to integrate the use of ICT in teaching, learning, research and management of the institution including computerization and automation of various operations. The report also notes that the use and availability of internet in different Kenyan universities had significantly improved over the past five years. The report further emphasized the need for a continued investment by the universities on an enhanced wireless campus network infrastructure so as to support the growing number of students and students who use laptops and other mobile devices to access services and other information resources (Kashorda & Waema, 2014).

The transmission modes during communication can be classified into two main categories namely; bound medium transmission or unbound medium transmission(Do & Van Nguyen, 2019). In bound medium combination, physical or tangible cables are used as the transmission medium while in unbound medium communication, transmission takes place through radio or microwave. Wireless communication can thus be classified as unbound due to the fact that communication takes place through an open medium by the use of radio waves (Bawiskar et al., 2013). This has made the use of wireless networks to gain popularity across the globe as most users would like to enjoy network connectivity without the limitation of their geographical locations. The popularity of wireless networks can also be attributed to the increasing use and reducing prices of mobile devices.

With the increased use of mobile devices on one hand, the use of traditional networks based on physical cables is proving inadequate due to the rising demand to move from one location to another while still enjoying the needed connectivity and interactions among users. Connection by physical cables would drastically reduce the movement of network user and also confine access to given geographical locations. There use of wireless networks is an ideal solution to such problems as it allows network users to move freely as there are no restrictions to physical location when accessing the network (Gast, 2010). This is supported by a survey by the Wi-Fi Alliance (2013), in which it was reported that 87% of U.S. youth aged between 18 and 29 years polled said they needed to have access to wireless networks in institutions(Alliance_WiFi, 2020).

The main advantage of wireless networks is mobility which can enable users to connect to existing networks while roaming freely. This allows users to access the network resources at locations of choice as long as they remain within the range of the wireless network (Gast, 2010). Wireless networks also offer a great deal of flexibility contributing to rapid network development. The infrastructure side of the wireless network remains the same whether connecting a single user or a number of users. All that is required to access after installation is authentication and authorization. This has made wireless networks a cheaper option than the traditional way of running cables, which is time consuming and expensive.

Universities in Kenya need networks to be able to access resources required for the day-to-day academic and administrative activities of the institutions. The main activity of these institutions is education and research. Due to wireless networks' advantages, it offers the best option for access to the internet and other institution-based resources and services like online applications, hostel services, fees information, learning platforms, etc. In many institutions, wireless networks have been implemented by using hotspots in different areas like libraries, hostels, student centers, and cafeteria.

However, the number of threats (when it comes to the security of computers a threat can be defined as a danger that results from attempts to exploit security weakness of a system resulting to a possible harm) and attacks on wireless networks have been increasing over the years. For example, according to statistics by Purplesec (2021), the number of devices infected by malware has grown from 12.4 million in 2009 to over 813 million in 2018 (Firch, 2021).

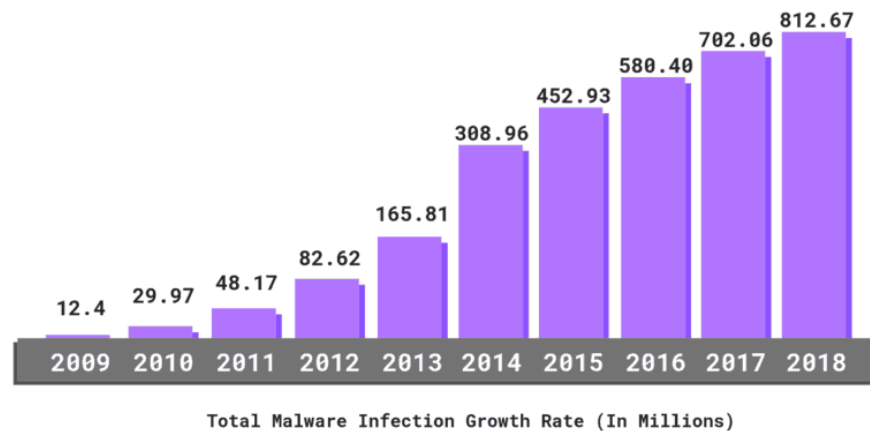


Figure 1: Growth in Malware Infections (Firch, 2021)

1.1.2 Security of Wireless Networks

Due to the use of unguided medium it is harder to control and secure wireless networks as compared to wired networks. However, it is important to ensure that the main security objective of confidentiality, integrity and availability are maintained when using the wireless networks. This calls for the implementation of tight security measures that will block any unauthorized attempts to gain access to data and network resources by malicious users and attackers. The existence of breaches to wireless networks and the increasing attacks and vulnerabilities have affected the rate of deployment of wireless networks in enterprises (Rawat et al., 2014). The security problem in wireless networks is further complicated by the use of wireless access points which were not used in the past for network deployment.

When compared to traditional networks the set of risks presented by wireless campus networks are very different. The main reason for this difference can be attributed to the

methods that are used in accessing wireless networks. The most widely used method for broadcasting wireless network signals is the use of radio units connected to wireless access points. The broadcasted signal often goes past the needed geographical boundaries given the fact that the radio waves can penetrate obstacles including walls and windows. Anyone close enough to the area is able to pick up the signals as there is very little network administrators can do to limit such boundaries (Zou et al., 2016a).

Wireless campus networks can be accessed by any students, workers or visitors who have access to the campus premises and can be compared to other public Wi-Fi networks that are accessed by a number of strangers. Students' major concern is having access to the internet and other network resources, but they are often unaware that some of the wireless campus networks they access may not be secure.

Cases of people gaining access to unauthorized resources through exploitation of loopholes in wireless sensor networks have been reported. An example of such cases was reported in the United States of America in 2011 when a famous motor vehicle company's wireless network was hacked by the use of network cracking tools and specialized antennae. The hackers were able to gain access to the company information systems as a result and stole financial data. They were able to direct payroll funds to accounts controlled by them by use of hijacked payroll information under their possession. In addition, they were also able to loot company funds through reloadable debit cards. The hackers also stole computer equipment that they later used to hack into the company's wireless network further leading to losses and interruption of services at the company premises. ((USAO), 2011). This

shows that strong security measures should be put in place to ensure that all the networks are well secured.

The focus of cybercriminals is not only the wireless campus networks but they also target to access to university systems and databases so as to gain information that can be used for identity theft. In 2012 it was reported that over 158 breaches were reported in different universities across the United States of America including; Purdue University, UC Berkeley and the University of Florida. As a result of the breaches over 2.3 million records were compromised (Legnitto, 2012). In March 2014, a Florida State University student in Panama City was reported to have hacked the wireless campus network of the university by exploiting loopholes in the wireless network security and redirected the network users to a porn site leading to interruption of services (Roberts, 2013). Because of the uncontrolled medium in wireless networks and an increase in hacking cases of campus wireless networks, an investigation of campus wireless security is a prerequisite for ensuring better network security. This will help identify vulnerabilities, risk and threats so that lasting solutions may be designed and built for secure organizational data and communication.

According to Kavianpour & Anderson, (2017) some of the reasons that lead to the insecurity of wireless networks include lack of adequate knowledge and tools for securing the networks, unawareness by some people of the security threats, vulnerabilities and countermeasures and also negligence and laziness in implementing well known precautions by those who install the networks (Kavianpour & Anderson, 2017). Leaving

wireless networks unsecured has often been compared to leaving a front door of a house open, meaning anyone can come in and go at any time and do what they want without knowing who came in and what they did. Anyone within the range of an insecure wireless network can be able to gain access to other peoples' files, read other people emails, sniff network packets and monitor the data being transmitted and even use someone's internet for free or perform actions that may make the wireless connection unavailable.

From personal experience and interaction with other network administrators, most of the time, network administrators think more about network security after the networks have been installed and running. Stein et al., (1998), notes that most of the time, the network administrators may not understand the magnitude of the risks they face as a result of setting up open or insecure wireless networks (Stein et al., 1998). According to the 2014 Kenya Cybersecurity Report, it was reported that there had been an increase in cybercriminal activities that were targeted at both public and private organization with universities being one of the major targeted areas (Kigen et al., 2014). The report further notes that in addition to targeting of information stored in computers and servers, the cybercriminals also targeted information on transit through different computer networks. The consequences to the organization, which include; interruption of normal business operation, denial of access to business operations, erosion of customer confidence on the organization, loss of confidential and important data or information and even loss of income and revenue, are usually the same irrespective of whether the attacker is from within the organization or is an external attacker or hacker (Kigen et al., 2014).

1.1.3 Wireless Network Security Assessment

Studies that have been conducted in an attempt to assess the security of wireless networks across the globe. To begin with, in a proposed study of a method for comparing and analyzing wireless security situations in two capital cities, Budapest and Belgrade, with a focus on access point configuration (Dobrilovic et al., 2016), it is noted that the increasing use of wireless networks has led a closer look at the security of wireless networks. It is further noted in the study that a majority of the population is not aware of the security risks posed by the wireless networks and there is a need for wireless security assessments from time to time so as to improve the security situation. This study shows the need for security assessment in all wireless networks, however, the method is not applicable to campus wireless networks as it only focuses on wireless access points, while wireless campus networks involve more.

In addition, in a study on automatic security assessment for next generation wireless mobile networks (Palmieri et al., 2011) it is noted that the use of mobile devices just like in universities in Kenya leads to more vulnerabilities. The use of third party authorization and authentications and a security assessment strategy are proposed in an attempt to solve the problem. The assessment involves analyzing of the user device by the infrastructure so as to determine if a device is secure or not and if not the device denied access to the network resources. Such a solution can help improve the security of networks but does not involve an assessment of the network infrastructure itself.

1.1.4 The Need for the Study

Even though studies have shown that there are increasing wireless security risks and that universities are one of the targeted areas not only in Kenya but also across the globe, some network administrators may not be aware of the risks they face. To the best of the researcher's knowledge and based on the reviewed literature, no studies had been done to assess the security of wireless networks in organizations in Kenya. In addition, existing related studies cannot be applied in assessing the security of campus wireless networks as the only focus on specific components of such networks. There was therefore a need for a study to assess the security of wireless campus networks in universities in Kenya and propose recommendations that can be put in place to make the networks even more secure.

1.3 Statement of the Problem

Universities in Kenya have been increasingly adopting the use of information technology to improve efficiency and effectiveness. The institutions have thus set up databases in which confidential student and employee data are stored. So as to enhance access, the universities have installed wireless campus networks that the students use to access such resources at their convenience, using personal devices. Such networks are also used to access the internet for research and day-to-day use (Kashorda & Waema, 2014).

Given the fact that wireless network radio propagation is broadcast in nature, the signals can be accessed by both authorized and unauthorized users. This is unlike with the wired campus networks which require physical connection by cables to gain access to the network thus only network nodes with direct access can connect. With wired networks it is also easy to trace a user in case of any security problems. However, wireless networks

are more vulnerable to attacks such as eavesdropping, malicious attacks, jamming, data interception and man-in-the-middle attacks due to the use of open medium (Zou et al., 2016b).

There have been reported incidences of hacking into university wireless campus networks in Kenya and other countries across the globe with an aim of compromising student account details and also to gain access to databases where sensitive information is stored. In a study that done in the United States of America, it was found out that, cases of hacking into universities' wireless networks by those outside the organization was over 300 times than was expected (Aubuchon, 2014). If insiders would be included the numbers would even be higher than reported. Kenya, Egypt, Morocco and South Africa were ranked top among countries that lead in cyber attacks in Africa according to a report by cyberoam which is a company that supplies wireless security device in over 125 countries globally (*Cyberoam Security Assessment Report*, 2015). The reports further noted that the motives behind the hacking of university wireless networks and subsequently information systems were to gain unauthorized access to grading and financial systems.

In Addition, Universities in Kenya are supporting the concept of Bring Your Own Device (BYOD) which allows students and staff to bring their own devices to the institutions. The implementation of BYOD policies requires additional effort on the part of the Information Technology (IT) staff, and has resulted to daunting challenges in ensuring security of the wireless networks. It was noted in a security report that 59% of organization in Kenya

including universities that allow BYOD lacked policies and procedures to manage the same (*Kenya Cyber Security Report 2015, 2015*).

Given the above mentioned challenges security assessment of wireless networks is an important exercise that any organization need to take so as to ensure all the precautionary measures are put in place. Few studies have been conducted for the assessment of security of wireless networks, for example; a proposed study of a method for comparing and analyzing wireless security situations in two capital cities, Budapest and Belgrade with a focus on access point configuration (Dobrilovic et al., 2016), and a study on automatic security assessment for next generation wireless mobile networks (Palmieri et al., 2011). The studies support the need of continued assessment of wireless networks but are not applicable to the diverse setting of wireless campus networks. There was therefore a need for a study to investigate the security of wireless campus networks in universities in Kenya so as to identify vulnerabilities and recommend counter measures. The thesis research was thus focused on assessing the security of wireless campus networks in universities in Kenya and proposing a tool and a model that can be used in security assessment and improved security of such networks.

1.4 Aim

The study was aimed at assessing the security of wireless campus networks in selected universities in Kenya thereafter making recommendation for improving the security of such networks

1.5 Specific Objectives

The specific objectives of the study were:

- i. To investigate open source technologies and tools that can be used in assessing the security of wireless networks,
- ii. To investigate the vulnerabilities in wireless campus networks in Kenya,
- iii. To design and develop a tool for assessing security of wireless networks,
- iv. To propose a model for ensuring improved security of wireless campus networks in universities.

1.6 Research Questions

The research was guided by the following questions:

- i. What are the security risks associated with wireless campus networks in the selected universities in Kenya?
- ii. Which measures are in place to ensure security of wireless networks in the selected universities in Kenya?
- iii. How vulnerable are wireless campus networks in the selected universities in Kenya?
- iv. Which is the best model and tool to ensure security of wireless campus networks?

1.7 Scope of the Study

The study covered all the aspects of wireless campus network security in the selected universities in Kenya. The universities were selected from chartered public and private universities at the time of study and did not include any constituent colleges or universities with letters of interim authority due to the limited amount of time and resources.

1.8 Limitations of the Study

The limitation of this study was the selection of universities to be included in the population sample or not, given that many universities are investing in wireless networks all the universities are expected to face the challenges with wireless networks. This limitation was overcome by focusing on universities that had been chartered by the year 2014 when the study was proposed as per data from the Commission for University Education in Kenya.

1.9 Assumptions of the Study

The assumptions of the study were:

- ❖ Security issues that arise from wireless campus networks in Universities in Kenya are usually similar.
- ❖ All chartered public and private universities have invested in wireless campus networks.
- ❖ It is possible to use open source technologies to investigate the vulnerabilities of wireless campus networks.
- ❖ There are guidelines that can be followed in assessing the security of wireless campus networks.

1.10 Significance of the Study

As the use of mobile devices continue to become popular among university students and staff and with the continued automation of services in the universities. The findings of this study will be significant to different stakeholders as follows;

To the university management; The implementation of the recommendations of the study will ensure that confidential information cannot be accessed by unauthorized users, this will raise confidence in the university and attract more students. In addition, the university will experience little or no disturbance to online services and thus avoid financial losses that may result from disrupted service provision.

To the network administrators and ICT staff; The implementation of the recommendations will ensure the ICT staff and mainly those in charge of managing the wireless campus networks will have an easy way of finding out the vulnerabilities in their network and the needed measure that can be put in place to secure the networks. The work load of the staff will also reduce when there are reduced security breaches.

To students, workers and guests; The implementation of the recommendations of this study will ensure that the student, workers and even guest are more secured when using the wireless campus networks.

To other organization and stakeholders; other organization and stakeholders could also make use of the proposed model and tool to ensure improved network security in their organizations.

1.11 Chapter Summary

The rationale for conducting the study is provided in this chapter as reflected in the background to the study, statement of the problem, aim of the study, specific objectives for the study, study research questions, scope of the study, limitations of the study, assumptions of the study, and significance of the study.

From this chapter, it is evident that universities in Kenya are increasingly investing in wireless networks. Such networks bring with them increasing security challenges that have in some instance been exploited in universities across the globe. Most of the time network administrators are not aware of their network security challenges but focus on functionality. Periodic assessment of the security of wireless networks is recommended however studies that have attempted to assess security of wireless networks are not applicable to the university settings hence the need for the study. The implementation of the recommendations will benefit the universities, their stakeholders and other organizations.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

In this chapter, a review of literature that is related to the aim of the study is presented. Literature review helped to not only position the study in the context of previous research but also created a 'research space' for the study. The literature review was done based on the research objectives presented in the previous chapter. This section also presents a discussion of the theoretical framework on which the study was based. The conceptual frame work for the study is also presented. Available documents both published and unpublished that relate to each objective of the study and contain relevant information, data, evidence or ideas were selected.

The literature review covers a theoretical framework for the study based on the Game Theory. Also reviewed are studies and publications in the area of wireless network security in an endeavour to understand all the concepts necessary in investigating the security of wireless campus networks and to gain a greater understanding of to what extent the topic has been studied and at the end a rational for justification for concepts applied in the study is the developed.

2.2 Theoretical Framework

Different theories and models have been developed to guide security of wireless networks and the development of information systems. The two theories that guided the study were;

(i) The Game Theory (Tadelis, 2013)that was pioneered by John von Neumann, a

Princeton mathematician and (ii) The system theory (Ceric, 2015) which guided the development of the online wireless network security assessment tool.

2.2.1 Game Theory

Game theory is the science of strategy that attempts to determine mathematically and logically the actions that “players” should take to secure the best outcomes for themselves in a wide array of “games” (Barron, 2013). In the game theory a wide range of games are presented with interdependence being the common feature in the games. The strategies of all the participants of the game will determine the outcome of each participant. In scenario where the interests of the players vary and conflict totally the game is referred to as a zero sum game with one person’s loss being another person’s gain (Tadelis, 2013).

Multi person decision scenarios are described in the game theory as games which each player endeavours to choose actions that would best reward them but at the same time anticipate the actions of other players in the game. The basic entity in each game in the game theory is a player with the ability to perform actions and make decisions. Strategic interactions of the players including actions the players can take, the payoffs for each action to the players and the guiding constraints for each actions are described in the game but the actual actions taken by the player are not described (Tadelis, 2013).

The description of how a game can be played by the use of best strategies and the expected outcomes is referred to as the solution concept. A consequence function is used to associate each action of a decision maker to the consequence. Each player’s preference is modelled in relation to a set of consequences forming the preference relation. The

complete plan of action by a player for all the possible game situations forms the player's strategy. The strategy is considered pure if the action intended by the player is unique for the situation. On the other hand, the strategy is mixed if the strategy applies a probability distribution for the actions possible in a given situation. A steady game condition solution is referred to as the Nash equilibrium. In a Nash equilibrium if any of the players change their strategies the payoff would be lowered as the other players will be adhering to the set strategy (Barron, 2013).

2.2.2 Relevance of the Game Theory to the Study

In relation to the study, the nature of wireless network security conflict can be captured as a game with attackers and network managers being the players. The decision strategies of those who manage the networks in securing the network are closely related by the defender as a network attack will be based on a security vulnerability. The two intelligent agents in the wireless networks must therefore work towards maximizing the intended objective with a gain for network administrators being a loss to attackers and vice versa.

A tactical security threat, from either one attacker or an organized group of attackers', mitigation strategy can be performed by applying different techniques from the game theory. The game theory provides different scenarios that can be applied in a security system. In addition, people's actions along with the expected outcomes can be simulated and predicted so as to mitigate network security threats. With this, different what if scenarios that can be used to identify the level security during the network security assessment and thus propose recommendations to minimize the risks and achieve the

objectives of the study. The application of the game theory in Network security can be summarized as represented Figure 2.0:

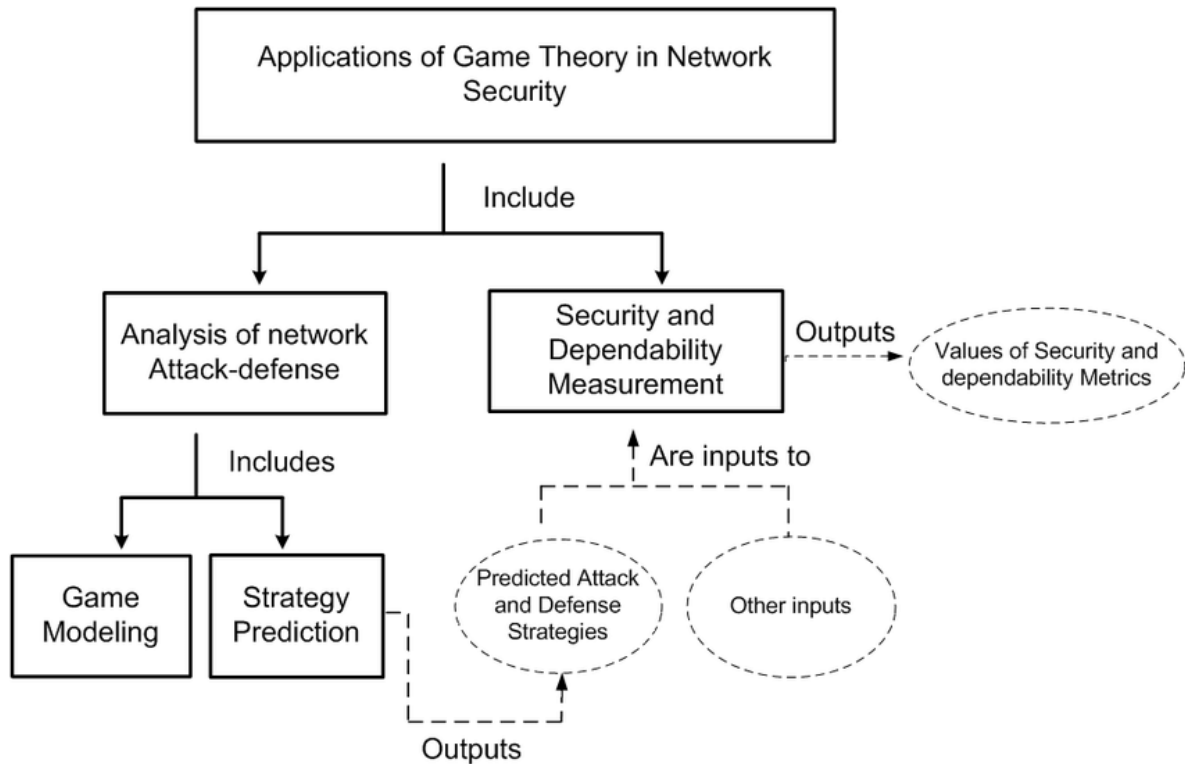


Figure 2.0: Game Theory in Network Security (Liang & Xiao, 2013)

2.2.3 Systems Theory

The systems theory was advanced in 1980. According to this theory, a system is defined

A set of parts that are interconnected to each other with a surrounding environment and work as a group towards the achievement of a common goal (Ceric, 2015). This is further summarized by (Burrowes, 2005) who views a System as a combination of parts to that together form a complex whole.

In advancing the Systems theory, (Ceric, 2015)classified systems based on their nature of interactions with their environment. According to this classification, systems can be classified as follows;

A. Open system

A system is considered to be open if the system interacts with its external environment. The external environment in an open system can be influenced by or influence the system. In an open systems inputs can be taken from the external environment and the system outputs can influence the external environment. In the case of an online wireless network security assessment tool, the working of the system will be directly influenced by the action of system administrators.

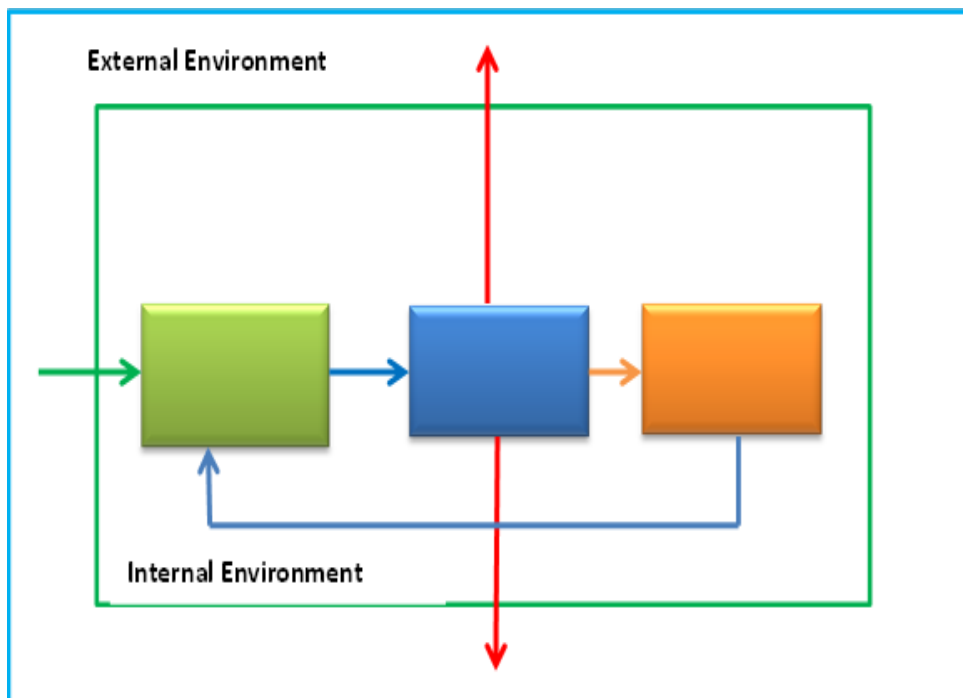


Figure 2.1: An Open System

B. Closed system

A system is considered to be closed if does not interact with its external environment, does not influence the external environment, and is not affected by what takes place in the external environment; consequently. In a closed system there are no inputs from the external environment and in turn no output to the external environment. The concepts of a closed system are not applicable to most systems and in some cases considered theoretical.

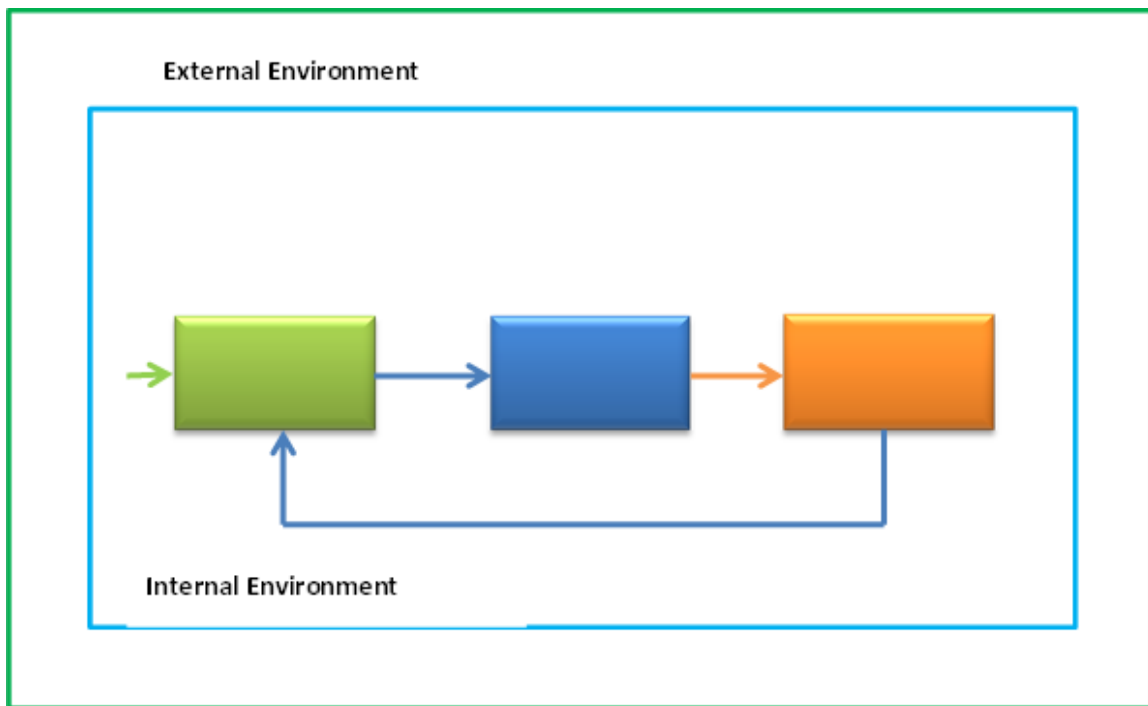


Figure 2.3: Closed System

C. Relatively closed system:

A relatively closed system uses specific methods and controls in the process of interacting with the external environment. The system inputs involve interaction of the system with the external environment with the results affecting the external environment and forming the main outputs. This view of a system best fits the interaction with the online wireless

network security assessment tool and for the purpose of this study, will be more applicable in the development of the tool.

2.2.4 Relevance of the Systems Theory to the Study

This theory has been purposefully selected because the realization an online wireless network security assessment tool involves different components that must work together for the system to meet the user needs. Ultimately, to achieve the overall mission of the network administrators, and all the different components will need to work well.

2.3 Wireless Networks

Computer networking has grown explosively over the recent past. (Comer, 2015) observes that before the 1970s computer communications was more of a research topic but that has since changed and it is now an part of the infrastructure. Networking is now an essential part of life and is applied in some of the following areas; advertising, business, shipping, accounting, production, planning, and billing.(Bargh et al., 2004)emphasize that most corporations have multiple networks. With this view it can be noted that learning institutions, the central and local government offices and non-governmental organizations use networks. In learning institutions computer networks are used to provide lecturers, staff and students with instantaneous access to online information and resources but also the central and local government offices use networks, as do non-governmental organizations. This is in itself in agreement with a statement by (Comer, 2015) that now computer networks are everywhere and are being used in every sector of any economy.

One of the most exciting and interesting phenomena in networking is the use and growth of internet globally (Bodhe et al., 2016). This view is supported by (Comer, 2015) who adds that in 1980, the internet was just but a research project in which only few sites were involved, as it stands today there has been a tremendous growth of the internet into a wide communication system that spans across the globe reaching all populations. The most common technologies used to access the internet include wireless technologies, DSL and cable modems (Bodhe et al., 2016). However, these are not the only means by which people are able to access the internet, broadband access technologies should be included in this list.

Computer networks can be created through different mediums, one of such mediums is through the use of radio waves in the name of wireless networks, which is the focus of the study. According to (Aspinwall, 2003) the term wireless is generic, and while it is typically synonymous with radio, it is not limited to radio. Wireless can also be defined as ultrasonic (sound) or infrared (light) wave communication between two devices. (Flickenger, 2002) notes that when wireless is used in the context of radio wave communications, regulatory and technical issues come into play, a view supported by (Aspinwall, 2003).

The use of mobile devices such as laptops, smart phones, tablets, PDAs among others have been increasingly becoming popular among network users across the globe. This has since made it almost impossible to continue depending on the traditional ways of networking as they have proven inadequate in meeting the challenges posed by the new ways of life. The use of physical cable to connect users drastically reduces their movement (Gast, 2010). This

is as opposed to the use of wireless communication technologies which come with many benefits for both the users and organizations as follows;

- ❖ Portability- The users of the networks can easily move with their devices while still enjoying the network connection unlike with wired networks where the people have to be at a given location to access network services
- ❖ Flexibility – The users are free to access the network from a preferred location
- ❖ Increased productivity – The users become more productive due to the ability to work from anywhere
- ❖ Lower installation costs – The installation and maintenance cost of networks is reduced when wireless networks are used

The capabilities of wireless networks are many and are oriented toward different organizational and user needs. To begin with, when users are connected through wireless local area networks they can easily move with their mobile devices from place to place without the need for connection with wires and without losing connectivity as they move (Karygiannis & Owens, 2002). The reduction of the need for wires when using wireless networks enhances flexibility and movement of users thereby increasing efficiency and productivity while reducing on costs. According to (Gast, 2010)the main advantage of using wireless networks is mobility of both users and device. This view is supported by (Flickenger, 2002)who states that that wireless networks enable the users to take advantage of the network and are able to move freely when connected to a network so long as they are within the range of the given networks for example in mobile communications where the users are able to even drive without losing connection so long as they are within the

range of a base station and when they leave that given range they are automatically handed over to the next base station. The users of such networks are able to enjoy connectivity and will not notice the effects of movements in such situations.

2.4 Risks in Wireless Networks

Even though users prefer to use wireless networks, they are however prone to more risks as compared to traditional networks. Some of the risks cut across both wireless and wired networks and others are specific to wireless networks. (Karygiannis & Owens, 2002) notes that the communication medium which is mainly through the use of radio waves is the most significant source of risk when using wireless technologies in networking. Radio waves are broadcast in air and are often compared to an open network port in a parking lot that is open to any intruder who can get access to the signal.

In the traditional wired local area networks information is transferred using network cables which are in themselves physically protected within the buildings where they are enclosed. This makes it difficult to compromise such networks as one is required to physically connect to the networks and must first break the physical security measures in place in addition to the set network perimeter security measures such as firewalls and intrusion detection systems. On the other hand, in addition to the risks and vulnerabilities of wired networks, wireless networks are exposed to additional risks that result from the medium used in transmission. The wireless radio signals broadcast beyond the perimeter boundaries as they can penetrate walls, windows, ceilings etc. Such signal can be accessed by any person within the broadcast range giving access to the network without the need to break any physical security measures in place (Ross, 2005).

Some of the most common risks associated with wireless networks include the threat of denial of service (DoS) attacks, the loss of integrity and the loss confidentiality. Unauthorized users may corrupt the organizations data, degrade network operations and performance, initiate attacks that interfere with access to the network by authorized users, gain access to the organizations systems and information, consume network bandwidth, and launch attack to other networks using the agency resources (Karygiannis & Owens, 2002).

Once they have accessed systems, the privacy of legitimate users is violated by the intruders, viruses or malicious code may be inserted by the intruders, denial of service attacks may be launched, identities are stolen, and interfere with normal operations. In cases where strong encryption is not used to protect confidential or sensitive information, such information may be intercepted during transmission between different wireless devices. Despite the new security risk that have been brought about by the use of wireless networks, the use of wireless devices and wireless local area networks has continued to grow. Many mobile devices used by a majority of users today such as personal digital assistants, laptops and smart phones are now wireless enabled by default (Scarfone & Dicoi, 2007).

From this section it can be concluded that wireless communications enhance portability and flexibility in access to network resources, responding to changes and information delivery in information communication technology infrastructure and user needs. However, the use of wireless networks result to new security risks that every organization need to understand and factor in in their day to day business decisions so as to put in

lasting measures to mitigate such risks. Risk assessment is should therefore be done periodically given the fact that new risks continue to emerge with the advancement of technology.

2.5 Wireless Network Threats

According to (Xiao et al., 2009)and supported by (Newman, 2017)the most common security objectives that need to be supported by wireless networks are as follows:

- ❖ Confidentiality – This objective is aimed at ensuring only authorized parties are able to read any communication or data.
- ❖ Integrity – Ensures that there are no unintentional or intentional changes made on the data during transmission or storage.
- ❖ Availability – This objective ensures that persons and devices in a network do not get any interrupted access to networks and network resources when needed.
- ❖ Access Control – This objective ensures restricted access to a network and network resources based on the permission and privileges of an individual or device

The prevailing security threats faced by both wired and wireless networks are the same and thus the security objectives are also similar. However, given the maturity level of wired networks the objectives have been understood and addressed to a high degree as compared to wireless networks which is rapidly evolving and call for frequent updates to ensure such objectives are met. Moreover, given some cases where wireless networks are extensions of wired infrastructure, such networks expose additional security threat that can be used by attackers to bypass the security control mechanisms in place (Ross, 2005). Hence, there is

a need to secure wired networks for both the threats that result from within the wired connection and those that are brought about by extensions to wireless networks

The major threats faced by wireless networks result from the ability of attackers to gain access to the radio communication between wireless devices, such abilities determine the extent to which such networks can be compromised. The relative ease by which an attacker can intercept wireless communications as compared to interception of wired communications bring about a difference in protection strategies (Xiao et al., 2009).

The most common threat in wireless networks is eavesdropping given that all an attacker needs is to be within the range of the wireless communication unlike with wired networks where physical access is needed to attack or in some cases remote login may apply to gain access to the networks as well.

In addition to eavesdropping, the installation deployment of rogue access points by attackers is also a common threat experienced in wireless networks. Such rogue devices are usually configured to appear to be from the organization so as to confuse the users and other network devices into accessing the device. This form a backdoor entry point into the network by passing the set security mechanisms like use of firewalls. The attacker can also be able to capture and view the information transmitted by clients who unknowingly connect through such devices.

The attaches on wireless networks mainly target to compromise the three security objective of confidentiality, integrity and availability. Such attacks can either be active attacks or

passive attacks. In active attacks the attacker does not only gain access to unauthorized information but also modify the information unlike in passive attacks where the attacker only gain access to a network asset of information but does not make any modifications to the setting or information.

Some common passive network attacks include eavesdropping where an attacker can tap into a communication channel and listen to information being transmitted without making any changes and traffic analysis in which an attacker monitors the transmission patterns of information being communicated over period of time with the aim of gaining sensitive information such as user log in credentials.

Active attacks may be in form of the following; Masquerading where the attacker pretends to be an authorized user so as to gain access to unauthorized resources or information, replay in which a passive attacker can retransmit messages as if they were the authentic users, Modification in which the attacker alters the original messages either by adding or deleting wrong information for malicious gains or denial of service in which the attacker ensures that normal users are not able to use a services or access networks as required.

The insecurities and vulnerabilities inherent in wireless networks is also confirmed by (Và, 2018)who notes that with appropriate tools an attacker can be as far as 20 miles but still be able to gain unauthorized access to a wireless network. He further notes that the most vulnerable networks are networks with poor configurations and those that do not utilize any encryption techniques. In spite of such challenges and many others that result from vulnerabilities in a range of wireless network standards and protocols, there also exist

solutions that can be used in securing the networks. Such solution requires a careful plan, design and engineering when deploying wireless networks (Và, 2018)

2.6 Wireless Network Security Testing

Security testing varies depending on the user's choice, tools and methods used. The test can be manual where individual have to plan and conduct the test or can be automated thus requiring less human involvement (John Wack, Miles Tracy, 2003). Some of the commonly used security testing include:

- ❖ Network Scanning: In network scanning a port scanner is used in identifying the host that have been connected to a local area network. This can also identify the services running on the hosts and applications that are related to the identified services.
- ❖ Vulnerability Scanning: This is used to identify the hosts connected to a network and open ports in the hosts. In additional, a vulnerability scanner has the capability of providing additional information on the associated risks.
- ❖ Password Cracking: Password cracking automatically test and identifies weak password used for authenticating users in accessing devices
- ❖ Log Review: Logs are reviewed with the aim of identifying any deviations from the set organizational security policy. Some of the logs that can be reviewed include; IDS logs, server logs, firewall logs and also other logs that are used to collect system and network audit data.
- ❖ War Driving: This involves the exploitation of flaws on some security mechanisms for example the flaws in implementation of WEP in 802.11b networks

- ❖ **Penetration Testing:** The evaluators in penetration testing have an understanding of the way the systems have been designed and implemented. They use this knowledge to try and go round the well know security feature to see to what extent such features can be broken.

So as to get a more comprehensive results of security testing and determine the network security posture several of the techniques are combined together. None of the tests can single handily provide a comprehensive result. An example would be before undertaking a penetration test one has to carry out a network scan and vulnerability scan with the aim of identify ports and services that can be exploited in the test. There are also vulnerability scanners that have incorporated password crackers.

2.7 Study Gaps

Wireless network security is an ongoing process and network administrators need to continually be on alert since unauthorized people, including cybercriminals, can gain access to their networks without being detected and cause them much harm by hijacking and altering communications, stealing their data, sabotaging their network, among others. Thus, it is very important to always know what is happening and keep WLANs. So as to ensure this regular network assessment is required to help identify the vulnerabilities and develop counter measures thus reduce on the effect of such attacks.

However, limited studies have been done to assess the security of wireless networks across the globe. As study was done on wireless network risk assessment method which is only a component of wireless network assessment (Dongmei et al., 2007). In another related study

on cyber security assessment for wireless network at nuclear facilities (Kim et al., 2018) the focus is on wireless sensor networks which are prone to different risks as compared the traditional wireless networks. A study on assessment of security and vulnerability of home wireless networks (Stimpson et al., 2012) focused on a home network which is meant for fewer users and the challenges experienced may not be the same to those experienced in wireless campus networks. In addition, apart from available commercial solutions such as the one offered by seven layer7 (*Wireless Security Assessment*, 2021) and guard point security (*Wireless Security Assessment | GuidePoint Security*, 2021) that are expensive, the existing tools used for such assessments target only specific areas and for one to do a comprehensive assessment, they will need to use many of such tools leading to longer times and requirement of skills to perform such test.

2.8 Summary

The underlying communication infrastructure determines access to information which is key to success of every organization. In the recent a tremendous growth of the internet has been witnessed and is compared to the internet phenomena from the 1990s. The media through which data is transmitted in wireless local area networks is through the air by use of radio waves at different frequencies. For any wireless device or client to be able to access the network they must be within the broadcast range. Given the nature of radio waves, they do not have a well-defined boundary and can travel through floors, ceilings, and walls, making it possible for such signals to be accessed by unintended users who may be sometimes out of the building. Often wireless networks are compared to Ethernet ports that

have been put everywhere leading to both privacy and security concerns as it impossible to direct the signals to the intended recipient

The use of Wireless Local Area Network (WLAN) technologies has been on the rise in organization of all sizes including learning institutions and so an increasing concern of security. From the review different authors have covered many aspects that must be put into consideration with wireless networks. Security comes out as a major challenge and it is so in learning institutions also. However, the existing commercial solution for security assessment are expensive and there have been no studies to assess the security of wireless networks on a campus environment. There was therefore a need for a study into the security of wireless network in universities in Kenya that will help in ensuring all information resources and communication are secure.

CHAPTER THREE

RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

This chapter describes the research design and methodology that was used in the study, population and sampling, data collection instruments and procedures, quality control measures, statistical treatment of data and analysis techniques, and ethical considerations.

3.2 Research Design

This study was conducted using qualitative research design. In a qualitative research the experiences, accounts or perceptions of the participants are elicited. This method was chosen so as to gain a better understanding of the security of wireless campus networks in the selected universities given the fact that little information to this effect was readily available. By the use of this design the researcher was able to get in-depth information with descriptive data being generated for further classification and analysis by the researcher.

3.2 Population and Sampling

3.2.1 Target Population

The total group of subject meeting a criteria defined in a research problem make the population. According to (Graneheim & Lundman, 2004)all cases from which generalization can be made by a researcher forms the target population out of this the cases that are accessible to the researcher form the accessible population. In this study the target population was made of chartered public and private universities in Kenya. By the time the study began in the year 2014, there were 30 chartered public universities and 17 chartered

private universities in Kenya. From the universities the network administrators or their representatives were the main respondents as they are directly involved in the day-to-day management and securing of wireless campus networks.

3.2.2 Sample Size

Given limited time and resources, a section of the population that represents the entire population was selected. The selection of a sample is supported by (Graneheim & Lundman, 2004) who note that for exploratory studies small samples that are representative of the desired population should be chosen in a deliberate process by the researcher. Different authors have suggested different formulas in selecting a sample, for this study the Slovin's formula (1946) was used in coming up with the sample size as follows:

$$n = N / (1 + Ne^2).$$

$$n = \text{no. of samples}$$

$$N = \text{total population}$$

$$e = \text{error margin / margin of error}$$

The total population for the public universities was 30, and that of private universities was 17. When the above formulae were applied the samples generated were as follows.

$$n = 30 / (1 + 30(0.21)^2) \quad \text{and} \quad n = 17 / (1 + 17(0.25)^2)$$

For the calculation the sample size was made of 13 public universities and 8 private universities in Kenya.

3.2.3 Sampling

Individuals selected for participation in a qualitative research based on their experiences with the area of study. This is unlike with a quantitative research in which the individuals are randomly selected and the intention of the study is not to generalize findings.

For selection of the privates and public universities, purposive sampling techniques was used. This involved a conscious selection of the universities that participated in the study. For the purpose of this study the universities were selected based on statistics and guidance from the Kenya Education Network who have helped many universities to set wireless campus networks as part of its objectives. For each university the respondents were the network administrators or their representatives who had firsthand information on the management and configuration of the wireless campus networks.

3.3 Data Collection

3.3.1 Data Collection Instruments

The main tools for collecting data used in the study were observation, personal Interviews, document analysis, and practical experiments. More than one tool was used due to nature of the study where there was need for verification of collected information by the application of a different method to get more and detailed information about the area of focus. The selection of these tools was guided by the objectives of the study, the nature of the data to be collected and the time available. In this study, the researcher was interested in assessing the security of wireless networks and there needed to collect data on the security measures in place, vulnerabilities and identify possible threats faced by the universities in which such networks are used.

Interviews:

The researcher conducted personal interviews by himself. Those interviewed were network administrators from the selected universities. The researcher booked an appointment with the interviewee and the conducted interviews took different amounts of time ranging from 1hour to 5 hours, this was affected by the nature of the university and the involvement of the network administrators in the practical sessions. The researcher developed and used an interview schedule to gather more information from selected respondents, in the selected universities. The interview schedule helped the researcher collect data that cannot be obtained through the use of a questionnaire. The interview schedule was based on the wireless LAN security checklist as recommended by The National Institute of Standards and Technology (NIST).

Experiments:

In the practical experiment the researcher applied 'tests' to wireless networks in the target university so as to determine if the security measures were effective. Due to budget constraints and the researchers experience, open source tools were used as described below:

1. Nmap

Nmap ("Network Mapper") is security auditing tool that is available freely. The researcher downloaded and installed this tool and with the permission of the network administrators used the tool to scan the wireless networks in different universities. The tool was able to show available on the network, what services (ports) they were offering, what operating system (and version) they were running, what type of packet filters/firewalls were in use,

and other characteristics. This data was important in identify some of the threats and vulnerabilities that the institutions faced.

2. LANguard Network Scanner

LANguard Network Scanner is a freeware security and port scanner. This tool was used together with the nmap so as to gain more in-depth information about devices in the network. It provided NetBIOS information for each computer such as hostname, shares, logged on user name and also didpassword strength testing, OS detection, and detected registry issues.

3. Netstumbler/Acrylic

Netstumbler was used to listen for available networks and recorded data about that access point. This was necessary to help identify the broadcast ranges of different access points and also get more information relating to the SSID, broadcast channels, type of devices, enable security measures and locations.

4. Aircrack

Aircrack is a combination of tools that can be used to crack week WiFi passwords. Ater gathering adequate encrypted packets, it applies best cracking algorithms so as to crack keys used in wireless networks. This tool was used to attempt to crack the passwords set by network administrator so as to find out if they had used strong authentication mechanisms that could prevent such attacks

5. Wireshark

Wireshark (open source multi-platform network protocol analyzer. This tool was installed by the researcher and used to examine data from a live network with the permission of the network administrators. From the capture data the researcher was able to analyze the network traffic with the aim of finding security flows in the transmitted data just like a man in the middle attacker would do to compromise the network.

Observation:

Observation was used to gather data by noting the physical characteristics of the installed network devices. Covert observation was used and the observer was concealed with those involved not knowing there was observation going on. Some of the data collected through observation included location of access points and other network devices, the physical security measures around the devices, the extent of broadcasts and SSIDs used.

3.4 Quality Control

For quality control, the research instruments were piloted in one institution and modified to improve their validity and reliability. The interview guide was shared with Kenya education Network staff who are specialists in wireless networks so as to improve on the same before using it for a pilot interview in one institution and improving on the same. To ensure reliability and validity of the tools used. The researcher installed all the tools and used them in the pilot institution so as to test their functionality and capabilities to provide the intended data that was to be collected. Input was also sought from other network professionals so as to ensure best tools were used.

3.5 Data Collection Procedure

The researcher got permission from the university and the national science and technology council in Kenya. The researcher then sent written request for appointment to conduct research to the selected institutions and also to Kenya Education Network which helped set up wireless networks in most of the universities. Follow up telephone calls were made before visits.

In-depth interviews were used to collect data from the ICT staff in charge of networks in some participation institutions and at Kenya Education Network. An interview guide with open ended questions was used. This offered the researcher a chance to follow-up on questions and to explore the security of wireless networks in the institutions. The researcher also visited different locations in some of the institutions and observed how the wireless devices were installed with the help of an observation guide. Experiments were also conducted in 16 institutions that accepted to ascertain the security measures in place with the guidance of the network administrations in the institutions.

3.6 Statistical Treatment of Data

The qualitative data generated from the interviews and observation was transcribed and grouped. It was then analyzed based on the research questions and developed themes. Content and thematic analysis was used to analyze the data and make inferences by objectively and systematically identifying characteristics of responses.

3.7 Ethical Considerations

The major ethical problem in this study was the privacy, unauthorized access and confidentiality of the data transmitted across the wireless networks. To properly investigate

the security of the networks it entailed gaining access to some networks which led to infringement on the privacy and confidentiality of the users. However full consent of the respondents was sought prior to collecting and using their data and all data was treated in a way that protected the confidentiality of the respondents involved in the study.

Another consideration was to ensure that the knowledge gained about the organization was not used in anyway against them.

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS AND INTERPRETATION

4.0 Introduction

This study was aimed at finding out the security of wireless campus networks in selected public and private universities in Kenya. In this chapter the results of the data analysis and interpretation are presented. The findings are presented in the order of the research questions as posed in the first chapter as outlined below:

- i. What are the security risks associated with wireless campus networks in the selected universities in Kenya?
- ii. Which measures are in place to ensure security of wireless networks in the selected universities in Kenya?
- iii. How vulnerable are wireless campus networks in the selected universities in Kenya?
- iv. Which is the best model and tool to ensure security of wireless campus networks?

4.1 Description of Respondents

The tools specified in the previous chapters were used to collect data from the selected thirteen public universities and of the eight selected private universities. The researcher was however not able to collect data from one private university due to reluctance by the ICT management in revealing the network security status. It was also noted that even though the remaining seven private universities network administrators allowed the researcher to collect data, the network administrators were also reluctant in sharing information on their wireless network security. In collecting the data, the researcher made

observations, carried out practical tests and interviewed network administrators in the universities.

4.2 Security Risks Associated Wireless Campus Networks

i. Risk Assessment

Out of the 20 interviewed network administrators, only 4 indicated they had conducted a risk assessment for their wireless campus networks. Table 4.1 shows the transcription summary of responses from the universalities. So as to avoid exposure, the universities were given unique codes from U1-U20 as the transcription summary was being prepared.

Table 4.1: Transcription Summary of Responses from the Universalities

| University Codes | Response Summary |
|------------------|-----------------------------|
| U1 | Yes |
| U2 | No: Use known standards |
| U3 | No |
| U4 | No |
| U5 | No: Apply standard practice |
| U6 | No: Use known standards |
| U7 | Yes |
| U8 | |
| U9 | No |
| U10 | No |
| U11 | Yes |

| | |
|-----|-------------------------|
| U12 | No |
| U13 | No: Use known stds |
| U14 | No |
| U15 | Yes |
| U16 | No |
| U17 | No |
| U18 | No |
| U19 | No: Use known standards |
| U20 | Yes |

From an analysis of the data above it was noted that 80% of the network administrators had not performed any risk assessments. Half of them did not think about it while the other half relied on the published risks associated with wireless networks in coming up with countermeasures to secure their networks. This shows that many institutions are not aware of the specific risks that they face during the day-to-day operation of the networks.

ii. Patches and Upgrades

Figure 4.1 presents a summary of the interview transcription results of the question that sought to find out if the network administrators had performed firmware upgrades on network devices

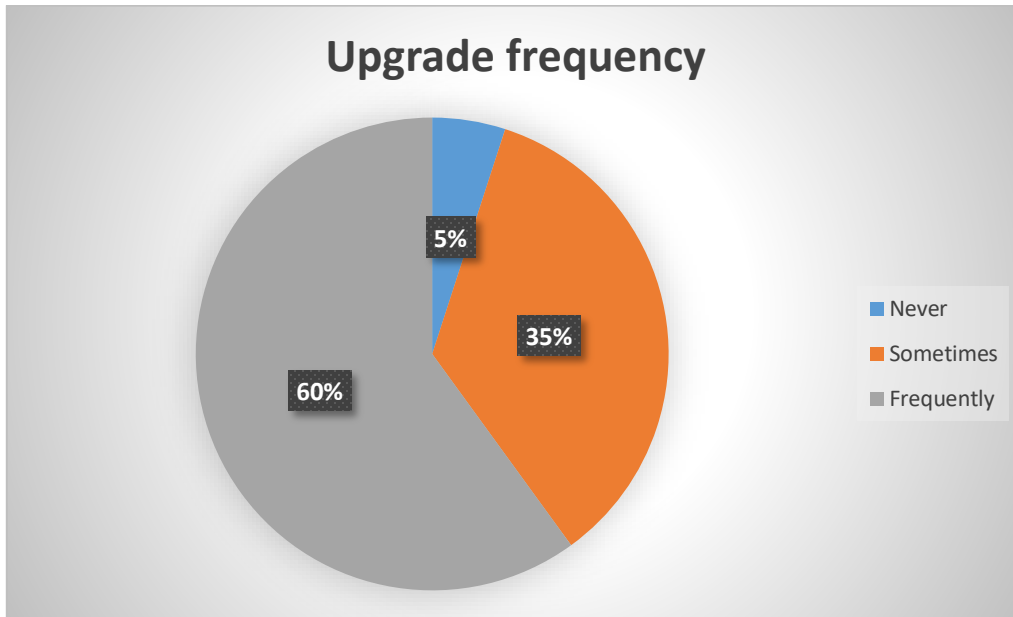


Figure 4.1: Frequency of Network Upgrades by the Network Administrators

From the data 60% of the respondents indicated they had conducted frequent upgrades. So as to ascertain this information, the researcher in collaboration with the network administrators went ahead to observe the upgrade status of sampled devices in 5 of the universities that reported to be doing frequent upgrades. It was however found out that in 2 out of the five universities where the observations were made, some devices had not been upgraded as indicated in the interview. Figure 4.2 and 4.3 give the upgrade status of core wireless campus controller and router from the universities.

The screenshot shows the Mikrotik WinBox interface. On the left is the 'Package List' window with a table of installed packages. On the right is the 'Check For Updates' dialog box.

| Name | Version | Build Time | Scheduled |
|---------------|---------|----------------------|-----------|
| routeros-tile | 6.39.2 | Jun/06/2017 08:01:04 | |
| advancedt... | 6.39.2 | Jun/06/2017 08:01:04 | |
| dhcp | 6.39.2 | Jun/06/2017 08:01:04 | |
| hotspot | 6.39.2 | Jun/06/2017 08:01:04 | |
| ipv6 | 6.39.2 | Jun/06/2017 08:01:04 | |
| mpls | 6.39.2 | Jun/06/2017 08:01:04 | |
| ppp | 6.39.2 | Jun/06/2017 08:01:04 | |
| routing | 6.39.2 | Jun/06/2017 08:01:04 | |
| security | 6.39.2 | Jun/06/2017 08:01:04 | |
| system | 6.39.2 | Jun/06/2017 08:01:04 | |
| wireless | 6.39.2 | Jun/06/2017 08:01:04 | |

The 'Check For Updates' dialog shows:

- Channel: current
- Installed Version: 6.39.2
- Latest Version: 6.40.4

What's new in 6.40.4 (2017-Oct-02 08:38):

- *) address - show warning on IPv6 address when acquire from pool has failed;
- *) arp - properly update dynamic ARP entries after interface related changes;
- *) crs1xx/2xx - fixed 1 Gbps forced mode for several SFP modules;
- *) crs317 - added L2MTU support;
- *) crs3xx - improved packet processing in slowpath;
- *) defconf - fixed RouterOS default configuration (introduced in v6.40.3);
- *) dhcp - fixed downgrade from RouterOS v6.41 or higher;
- *) dhcpv6-client - added IAID check in reply;
- *) dhcpv6-client - fixed IA check on solicit when "rapid-commit" is enabled;
- *) dhcpv6-client - ignore unknown IA;
- *) dhcpv6-client - require pool name to be unique;
- *) e-mail - auto complete file name on "file" parameter (introduced in v6.40);

Figure 4.2: Wireless Router Upgrade Status

From Figure 4.2 the current version of software installed in the device was version 6.39.2 while the version available for upgrading was version 6.40.4. This therefore meant that the updates of software in the device had not been upgraded frequently as stated in the interview.

| | | | |
|-----------|-------------------|-------------|----------------|
| CONNECTED | UniFi AP-Outdoor+ | 3.9.3.7537 | 4h 52m 51s |
| CONNECTED | UniFi AP-Outdoor+ | 3.7.49.6201 | 6d 23h 48m 45s |
| CONNECTED | UniFi AP-Outdoor+ | 3.9.3.7537 | 4d 17h 49m 12s |
| CONNECTED | UniFi AP-Outdoor+ | 3.7.49.6201 | 6d 23h 48m 50s |
| CONNECTED | UniFi AP-Outdoor+ | 3.7.49.6201 | 20h 52m 7s |
| CONNECTED | UniFi AP-Outdoor+ | 3.7.49.6201 | 7h 41m 35s |
| CONNECTED | UniFi AP | 3.9.3.7537 | 4d 18h 57m 25s |
| CONNECTED | UniFi AP-Outdoor+ | 3.7.5.4969 | 5d 2h 25m 14s |
| CONNECTED | UniFi AP-Outdoor+ | 3.9.3.7537 | 4d 17h 50m 4s |
| CONNECTED | UniFi AP-Outdoor+ | 3.9.3.7537 | 4d 1h 22m 20s |
| CONNECTED | UniFi AP-Outdoor+ | 3.9.3.7537 | 4d 1h 23m 15s |
| CONNECTED | UniFi AP | 3.9.3.7537 | 4d 17h 47m 47s |

Figure 4.3: Wireless Access Points Upgrade Status

From the screenshot of a wireless controller in Figure 4.3, out of the 12 access points listed, 5 were running version 3.7 as opposed to the latest version which was version 3.9.3.7537 showing that not all devices in the university had been frequently upgraded.

Newly discovered security vulnerabilities of vendor products should be patched to prevent inadvertent and malicious exploits. From the data collected it can be concluded that most of the universities have attempted to upgrade and install the patches for the wireless campus network devices. It was however noted that the upgrades were conducted most of the time without testing, this can lead to security problems in case the patches have bugs.

iii. Security assessment

Figure 4.4 gives a summary of responses to a question that was aimed at finding out how often the network administrators conducted security assessments in their networks

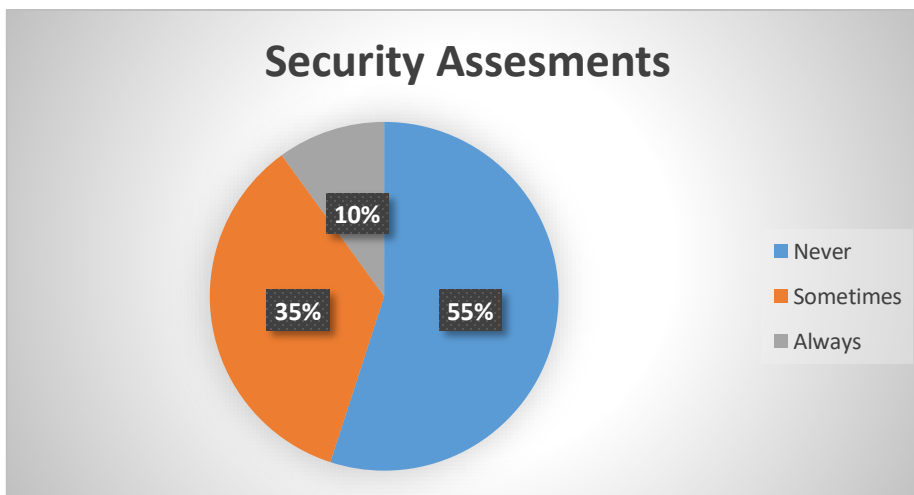


Figure 4.4: Frequency of Conducting Security Assessments

55% of the network administrators who responded to the interview questions had not conducted any security assessments for the wireless networks. Security assessments, or

audits, are an essential tool for checking the security posture of a WLAN and identifying corrective actions necessary to maintain acceptable levels of security. On a follow up interview question with the network administrators, this was attributed to lack of a specific tool to carry out a comprehensive assessment making the process to be complicated and even for those who found some tools they only targeted specific areas.

Many institutions are therefore not able to identify the corrective actions on time and thus are not able to maintain an acceptable level of security. This therefore supports the need for a tool that such network administrators can use to carry out such assessments from time to time.

iv. Inventory

A complete inventory of an organization's authorized APs is the basis for identifying rogue APs during security audits and can be helpful for a variety of support tasks. The researcher used Acrylic WiFi Home scan different networks with consent from the network administrators so as to find out the existing wireless access points with the SSID, MAC addresses, RSSI Channels, Vender, Security and speed. This practical test was conducted in 16 universities out from which 15 had rogue Aps being identified. Figure 4.5 gives a screen shot of the output from the software from on university, in the figure the AP with SSID Josephine was a rogue AP installed by a student in the halls of residence.

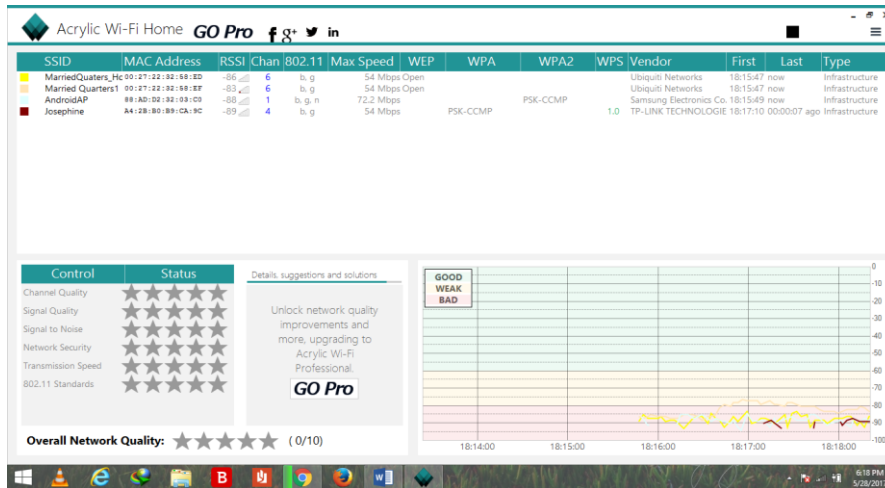


Figure 4.5: Rogue Access Points

Rogue access points can be used by hackers to gain valuable information from the network users and in some cases may lead to denial of service.

v. Disposal

On disposal of devices no longer in use the responses were as summarized in Figure 4.6:

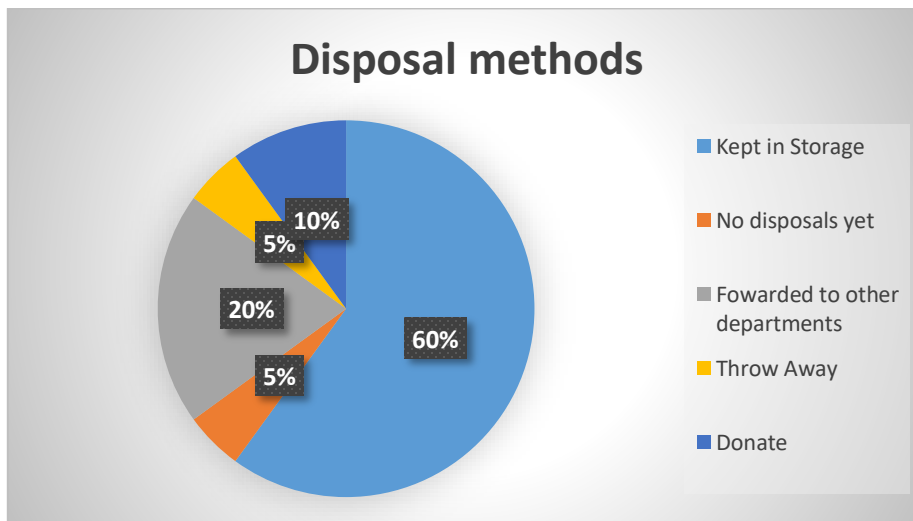


Figure 4.6: Disposal Methods

Only 2 out of the 21 network administrators indicated before their used devices left the organization or department they saved and reset the configurations on the devices. This shows that all the rest exposed the existing configuration to a possible review by authorized personnel. The methods of disposals pose a security risk for the universities thus they should identify the legal requirements to retain records that apply to their operations and copy the same before they are transferred to other departments. When donating they should ensure all the devices are reset so as to conceal organizational settings, something 19 institutions indicated they do not do.

vi. System logs

The researcher was able to observe system logs in 16 universities under the guidance of the network administrators in the institutions. 18 out of the 21 network administrators indicated that they reviewed their security logs, enabling the security and support staff to identify potential security issues and respond accordingly. Figure 4.7 shows a sample log from a mickrotik router in one of the universities. The researcher requested a filter to be done to show if there were any attempts to log in to the system by external users. The figure shows there were indeed several attempts to log on to the system

The screenshot shows a network management interface with a 'Log' window. The interface includes a top bar with 'Safe Mode' and 'Session: 41.89.162.2'. A left sidebar lists various system components like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Mesh, IP, MPLS, Routing, System, Queues, and Files. The main log window displays a list of system events, all of which are login failures for different users from the IP address 193.201.224.214 via ssh. The log entries are as follows:

| Timestamp | Device | Severity | Message |
|----------------------|--------|-------------------------|---|
| Mar/05/2017 08:35:37 | disk | system, error, critical | login failure for user hydrasna from 193.201.224.214 via ssh |
| Mar/05/2017 08:35:37 | disk | system, error, critical | login failure for user inads from 193.201.224.214 via ssh |
| Mar/05/2017 08:35:39 | disk | system, error, critical | login failure for user inads from 193.201.224.214 via ssh |
| Mar/05/2017 08:35:40 | disk | system, error, critical | login failure for user init from 193.201.224.214 via ssh |
| Mar/05/2017 08:36:03 | disk | system, error, critical | login failure for user install from 193.201.224.214 via ssh |
| Mar/05/2017 08:36:04 | disk | system, error, critical | login failure for user install from 193.201.224.214 via ssh |
| Mar/05/2017 08:36:07 | disk | system, error, critical | login failure for user installer from 193.201.224.214 via ssh |
| Mar/05/2017 08:36:12 | disk | system, error, critical | login failure for user intel from 193.201.224.214 via ssh |
| Mar/05/2017 08:36:12 | disk | system, error, critical | login failure for user intermec from 193.201.224.214 via ssh |
| Mar/05/2017 08:36:15 | disk | system, error, critical | login failure for user IntraStack from 193.201.224.214 via ssh |
| Mar/05/2017 08:36:31 | disk | system, error, critical | login failure for user IntraSwitch from 193.201.224.214 via ssh |
| Mar/05/2017 08:36:36 | disk | system, error, critical | login failure for user jagadmin from 193.201.224.214 via ssh |
| Mar/05/2017 08:36:36 | disk | system, error, critical | login failure for user JDE from 193.201.224.214 via ssh |
| Mar/05/2017 08:36:36 | disk | system, error, critical | login failure for user kemit from 193.201.224.214 via ssh |
| Mar/05/2017 08:36:38 | disk | system, error, critical | login failure for user l2 from 193.201.224.214 via ssh |
| Mar/05/2017 08:36:40 | disk | system, error, critical | login failure for user l3 from 193.201.224.214 via ssh |

Figure 4.7: Wireless Router System Log

Frequent reviews of audit logs allowed security and support personnel to identify security issues and take corrective or preventative measures quickly.

It was also noted that in seven of the universities, automated logging tools were used to assist with log review and send real-time alerts in response to critical events. Events tracked included failed authentication attempts and MIC failures. Figure 4.8 shows a screen shot from such an automated logging tool. From the figure events that were considered a threat were automatically flagged such as a rogue access point that was flagged red and interference on channel 1 that was flagged a trigger for further check.

System log review and more so automated log reviews are important as they ensure that the network administrators are informed early enough in case of any security breaches so that corrective action can be taken.

| EVENTS | | | |
|--|-------|---------|---|
| SHOW: LAST HOUR ▾ | | | |
| ALL (200) ADMIN (0) LAN (0) WLAN (200) | | | |
| Search | | | 🔍 |
| EVENT | TIME | | |
| 🚫 Rogue Access Point Classof2015 [04:18:d6:8f:6c:2d] was detected | Today | 5:20 pm | |
| 🚫 Rogue Access Point Classof2015 [04:18:d6:8f:6c:18] was detected | Today | 5:20 pm | |
| 🚫 Rogue Access Point Classof2015 [04:18:d6:8f:6c:18] was detected | Today | 5:20 pm | |
| 🔄 android-13ea4f22714d776a roams from Science to Humanities_ChurchSide from channel 6 to channel 1 on ssid "Classof2015" | Today | 5:20 pm | |
| 🚫 Rogue Access Point Classof2015 [04:18:d6:8f:6c:18] was detected | Today | 5:20 pm | |
| 🔄 android_e4324fd7c94b927 has connected to Annex-3 with ssid "Classof2015" on channel 11 | Today | 5:20 pm | |
| 🔄 android-3da26bc6db960140 has connected to Humanities_ChurchSide with ssid "Classof2015" on channel 1 | Today | 5:20 pm | |
| 🔄 HUAWEI_GR5_mini roams from Admin_Registrar's_Side to Humanities_ChurchSide from channel 1 to channel 1 on ssid "Classof2015" | Today | 5:20 pm | |
| 📶 Box-Middle was encountering some interference on channel 1 | Today | 5:19 pm | |
| 🔄 Windows-Phone has connected to Box-Middle with ssid "Classof2015" on channel 1 | Today | 5:19 pm | |

Showing 1-100 of 200 records. Items per page: 100 ▾ Page(s): < Prev 1 2 Next >

The number of results is limited to 200 of 1217. [Fetch more](#)

Figure 4.8: Automated System Logging

vii. Network separation

Figure 4.9 shows the response on the question as to whether the network administrators had separated the networks

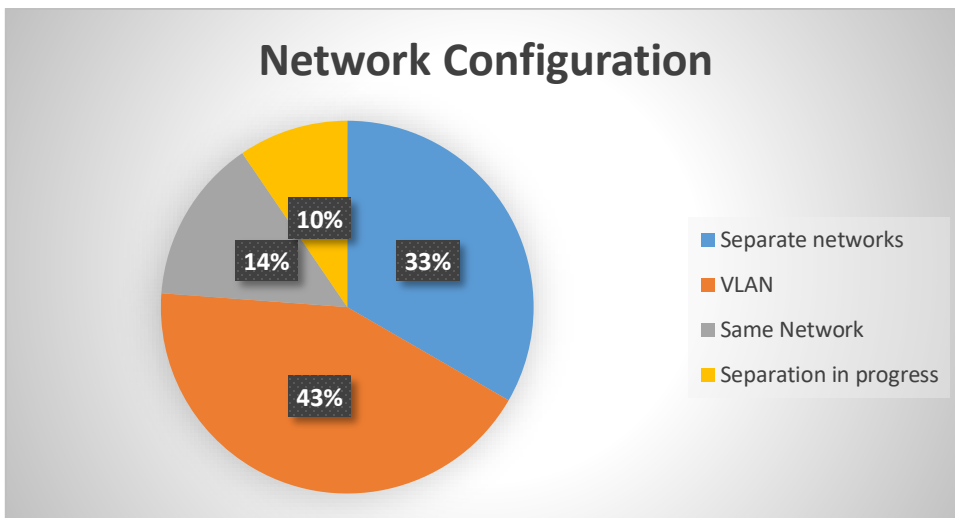


Figure 4.9: Network Configuration

43% of the universities had separated their networks and 33% using dedicated VLANs which facilitated the use of network access control lists, which identified the protocols and services that were allowed to pass from WLANs to the DS. Different VLANs were defined within the wireless connections to further separate varying security policies. Those that did not use the VLANs and did also not have separated networks, found it difficult to implement required security policies.

viii. Guest access

There was high volume of guest demands which required the universities to do more than just rely on their wireless infrastructure to set up guest wireless access. You need a good solution or network access control solution that adjusts depending on what device is being used, where it's being used and who is using it while at the same time deploying reliable policy management that can automatically enforce those rules.

In an attempt to find out how well the guests accounts were managed in the universities, the researcher working together with network administrators in 15 of the selected universities used nmap to scan the network traffic obtaining the results as given in Figure 4.10.

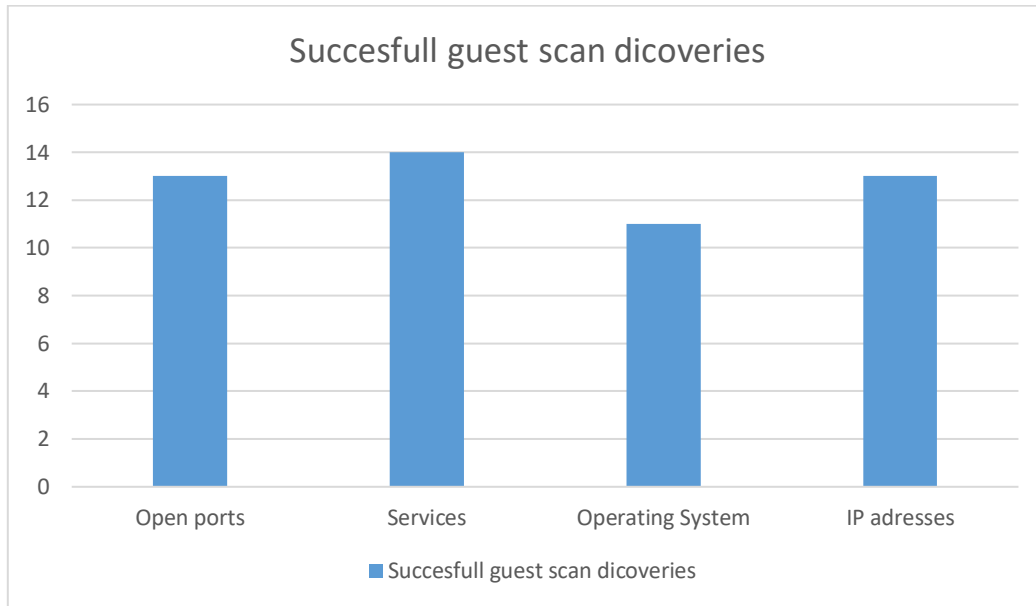


Figure 4.10: Successful Guest Can Discoveries

From the results presented in Figure 4.10 most universities did not have the best solutions thus may be faced with challenges of hacking from guest accounts. Figure 4.11 gives a detailed view of one of the scan outputs. In this scan the researcher through the provided guest credentials was able to identify 21 open ports, services running on different devices in the network, the IP addresses and the operating system. This is information that can further be analyzed by hackers to be able to compromise a wireless campus network.

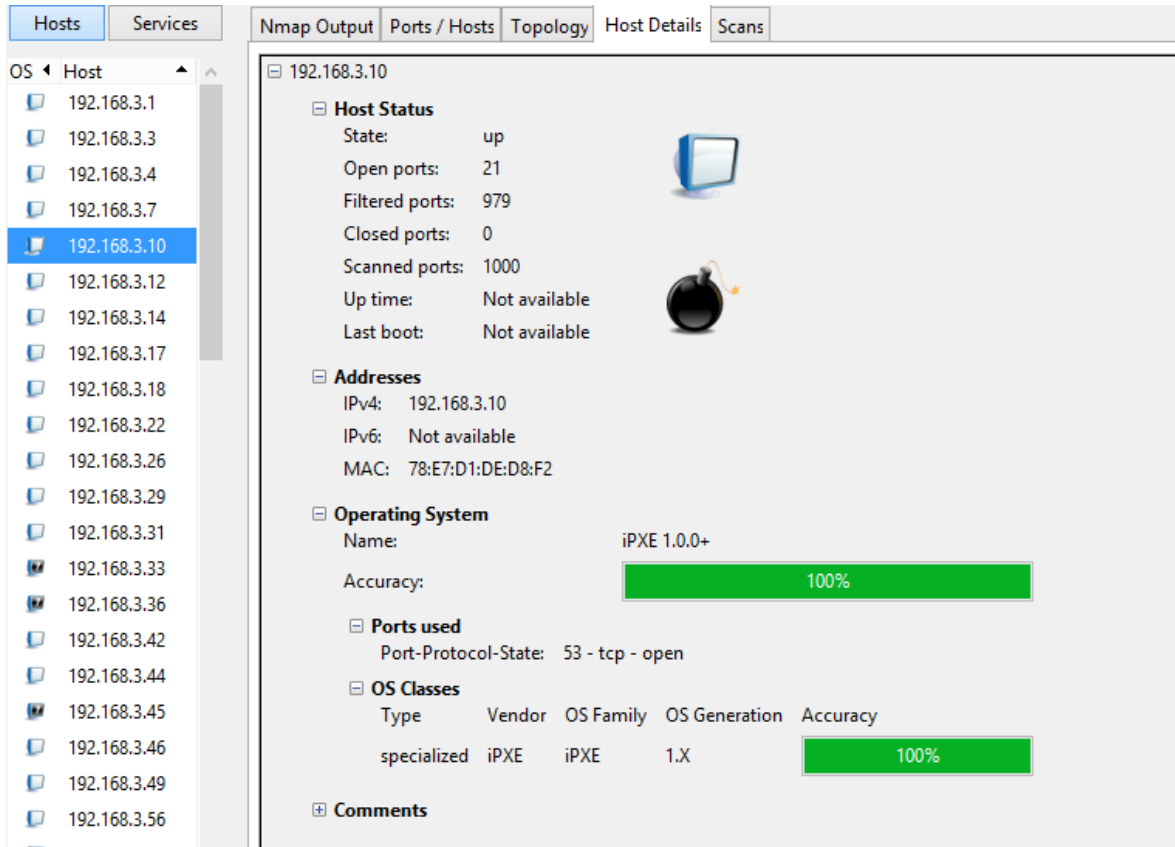


Figure 4.11: Nmap Guest Scan Out Put

ix. IP Addressing

In an answer to the question as to whether the universities used either dynamic or static addressing for the wireless campus network devices the results were as presented in Figure

4.12

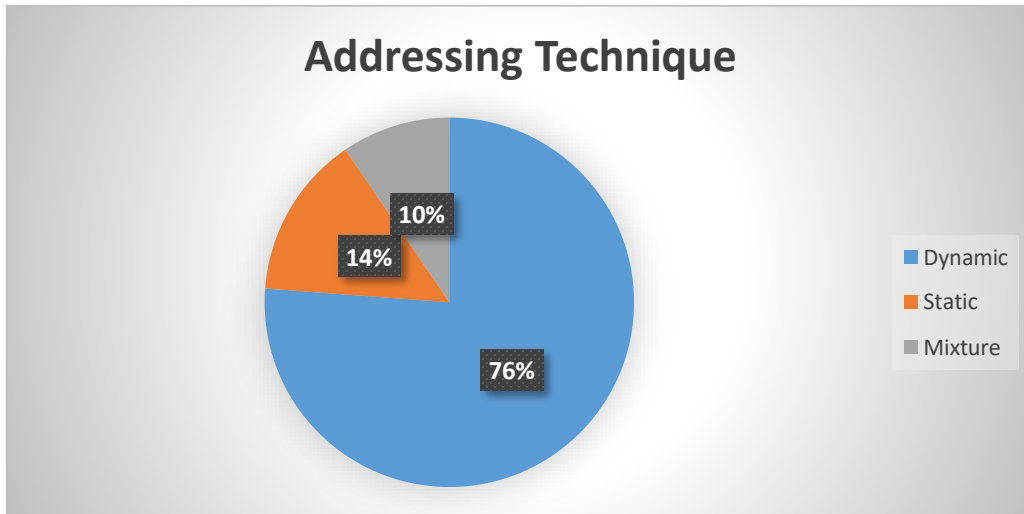


Figure 4.12: IP Addressing Technique used

76% of the universities used dynamic addressing with dynamic addresses assigned to users while the network devices had static addresses. Even though many universities prefer to use dynamic addressing due to convenience, this method makes it difficult to track and control access based on IP addresses creating a security management challenge to the administrators.

4.3 Security Measures in Place for Wireless Campus Networks

i. Policy

Figure 4.12 present the results based on the responses of the network administrators on the existence of acceptable use policies for the wireless campus networks.

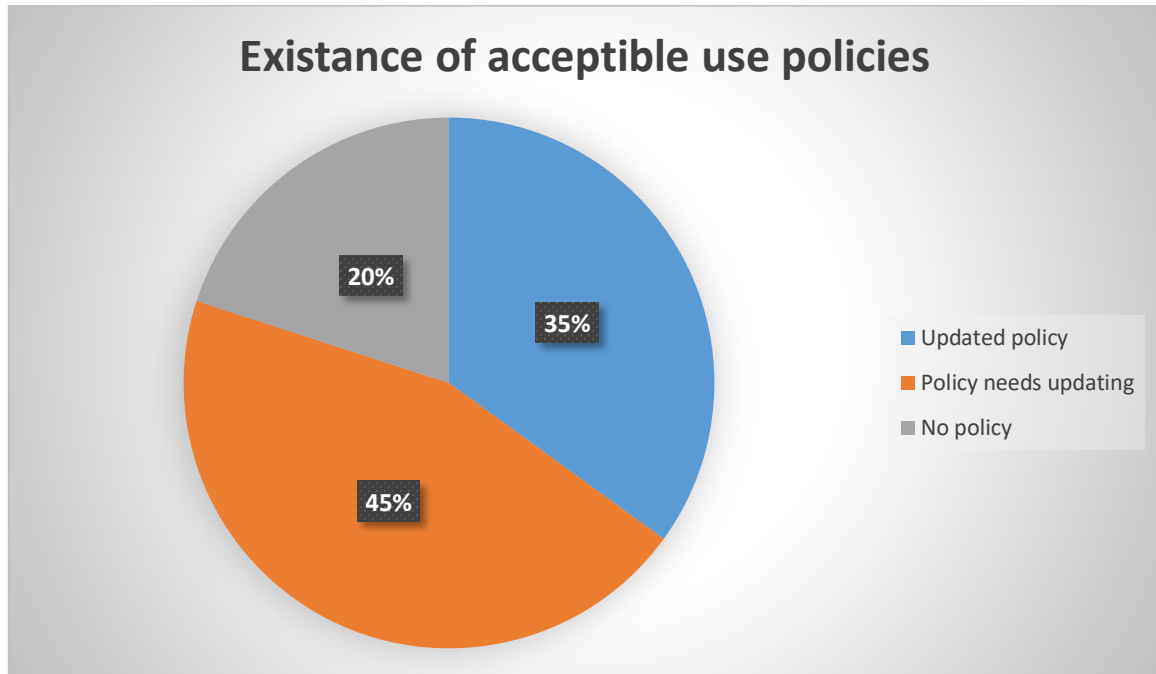


Figure 4.13 Existence of Policy

80% of the universities have acceptable user policies, even though some of the policies need updating. However, to ensure compliance with the university security policies users indicated that: they complied with policies during configurations, deployment and implementation of different authentication mechanisms. On a further follow up it was noted that 67% of the universities did not have a well-defined WLAN security policy. A security policy is the foundation on which subsequent security controls are based. This leaves the institutions at a vulnerable situation given the fact that without a policy it is easy to overlook important security requirements.

ii. User training

During the interview the researcher sought to find out if the user had undergone a security awareness training and the frequency of such training with the results from the transcribed responses being as given in Figure 4.13

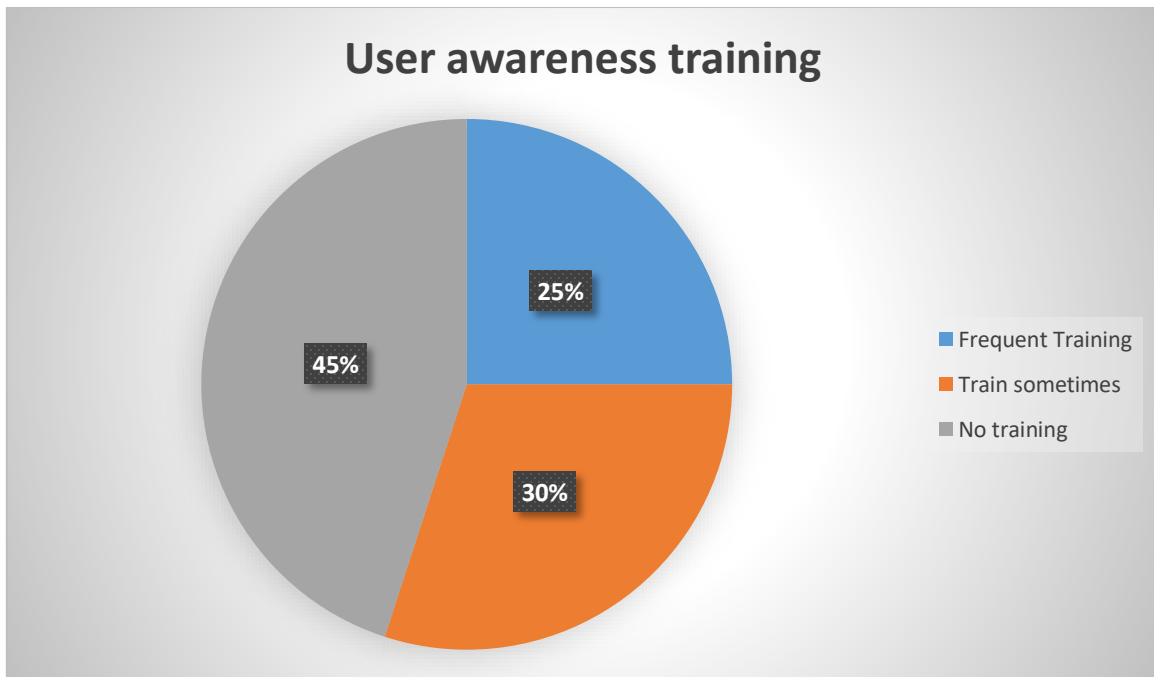


Figure 4.14: User Awareness Training

From the results it can be concluded that a majority of the users had not undergone security awareness and training, this may imply that the users were not able to establish good security practices to prevent inadvertent or malicious intrusions into universities network and information systems. This means some of the users may unintentionally perform actions that can create security risk to the universities.

iii. Physical security

To ensure physical security of the devices the respondents indicated that; they had placed them in secure places away from easy reach, put under lock and key or secured cabinets and also sometimes put in undisclosed places. The results can be summarized as given in Figure 4.14.

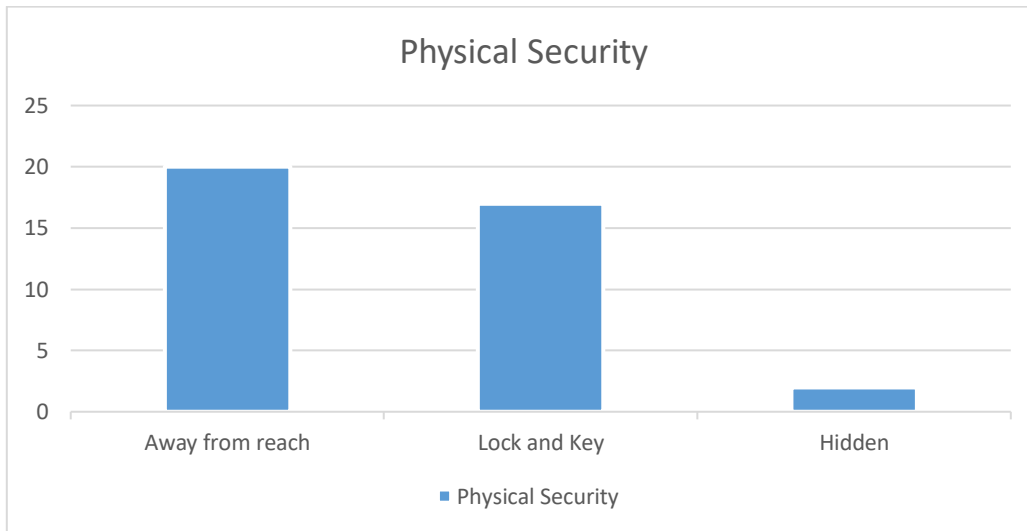


Figure 4.15: Physical Security

This was also observed when the researcher visited the institutions with sample images of wireless campus network devices put away from the reach of many users being shown in Figure 4.15 and 4.16. However, 3 institutions had reported cases of vandalism especially during the night in spite of the physical security measures that had been put in place by the universities.



Figure 4.16: Indoor AP Physical Locations



Figure 4.17: Outdoor AP Physical Locations

iv. Use of reset function

From the 20 interviewed network administrators 17 indicated that only the network administrators and approved support staff could use the reset function. It was however noted during the observation that in 4 universities there were physical devices that were within easy reach and anyone could use the reset function. In case this happens it may not only interfere with availability but also create a security risk.

v. Network Monitoring

For the purposes of network monitoring the network administrators from 19 universities indicated that they used; Simple Network Management Protocol (SNMP) which is a protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network. Others use open NMS which is an open source enterprise network management tool. It helps network administrators to monitor critical services on remote machines and collects the information of remote nodes by using SNMP. 11 universities also use Cacti, a complete network graphing solution designed to harness the power of RRD tool's data storage and graphing functionality, Smokping was used by 3 universities that keeps track of network latency and use of inbuilt router monitoring functionalities. It was however noted that 3 institutions did not have any network monitoring mechanisms. Without the insight that good monitoring tools and techniques provide, the universities cannot understand the effects that changes will make. Any change is likely to cause unintended damage to the network. Monitoring also helps the

administrators to constantly know how the network is performing and whether there are any security problems.

Figure 4.18 shows a screen shot of an output from cacti in one of the universities. The weekly graph can be used to monitor the traffic and in case there are any deviations from the norm further analysis can be conducted by the network administrators early enough to find out if the reason could be as a result of a breach in security of the wireless campus network.

Interface <Administrative_Buildings> Statistics

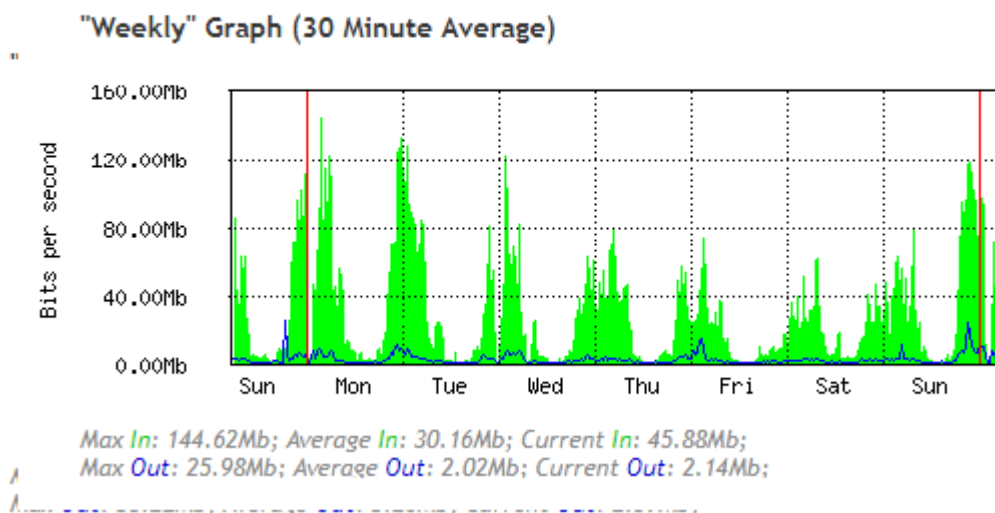


Figure 4.18: Router Traffic Statistics

v. Authentication

For authentication the network administrators from the universities indicated that they used the following techniques; Radius servers, MAC address access control, captive portal, passwords, WPA2, 802.1x authentication with DES and 3DES, 802.1x EAP, PEAP-

MSCHAP v2. There was an institution that had no authentication enabled for users, allowing anybody on campus and neighbouring community to access their network. Authentication methods used in 11 of the 20 universities where the interviews were conducted were not very secure and were not combined with any encryption methods. It was also interesting to note that the universities put more emphasis on access to the network; once the users are authenticated there were limited measures in place to ensure security of the connected users and systems.

vi. Firewalls

From the interview conducted and a practical experiment with kismet and LANguard it was noted that even though in all the universities firewall had been installed in the core network routers and servers, the universities were still at a risk because they did not have personal firewall and anti-virus software for all STA platforms for which such security products are commercially available. It was also noted that remote connectivity to the devices (e.g., file sharing, open network ports) was not limited as recommended. So as to determine this the researcher with permissions from the network administrators was able to do various scans from nmap, LANguard and kismet that he had installed. From 16 universities where this was tried all the universities had open ports that were not used for the provision of any services and providing backdoors for possible breach in security of the network. Figure 4.18 gives a screen shot of an output from nmap tool. In the diagram below 3 ports were open for a router while only 1 was in use:

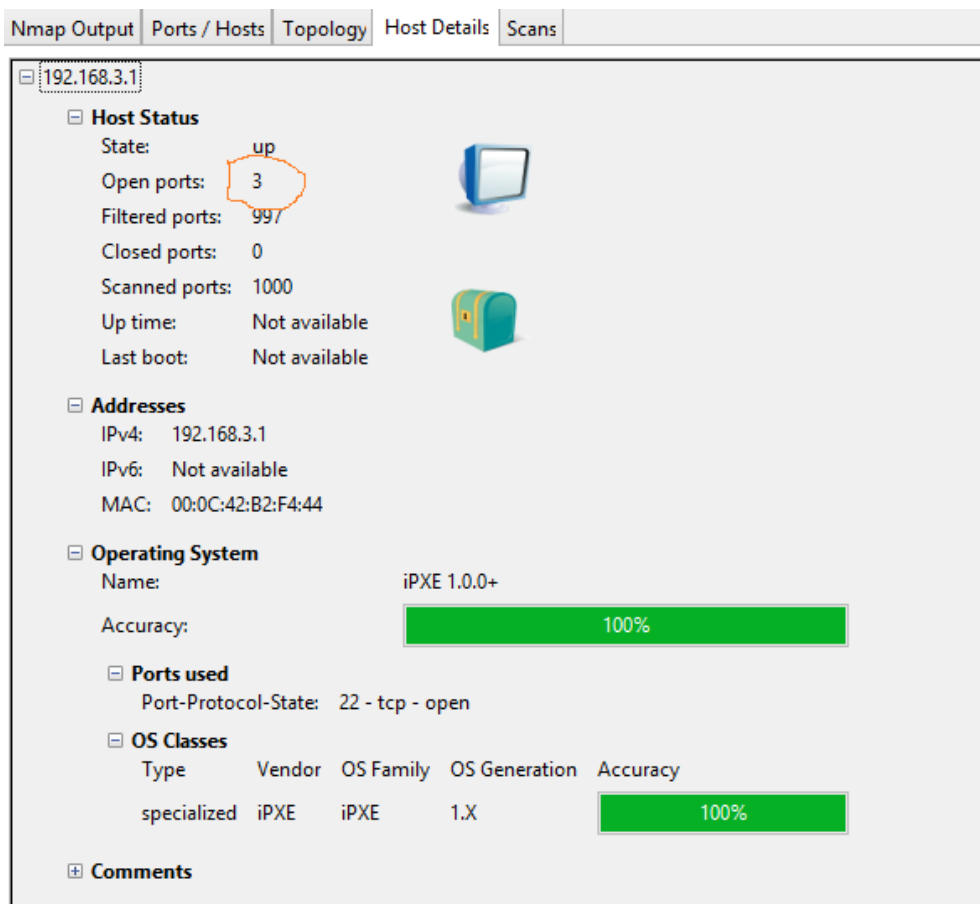


Figure 4.19: Nmap Host Details

vii. Passwords

In the interview the researcher sought to find out if the network administrators had changed the passwords used when configuring the wireless campus network devices, 11 of the respondents had never changed the passwords for the access points since installation. This makes many universities to be exposed to dictionary attacks, administrator passwords on APs should be hard to guess and should be changed often. In addition, a practical experiment was also conducted using the following steps; First a network scan was done using the acrylic network scanner so as to identify the type of network access point in use,

After the type of device had been identified, the researcher used the default settings and set up the computer to the default network, the researcher then tried to log into the wireless access point using the default IP, password and user name. After the test it was noted that in 9 of the universities the network administrators used a common and/or default password for multiple Aps making them vulnerable. This meant that anyone could easily access such devices and reconfigure or use the same to obtain traffic information as unaware users use the device to access the wireless campus network

viii. Intrusion detection

During the interview the researcher sought to find out if the network administrators had deployed intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity. From the responses it was noted that 15 of the 20 universities had intrusion detection systems deployed on the wireless network. The use of intrusion detection systems can help detect and respond to potential malicious activities, including unauthorized WLAN vulnerability scanning and the installation of rogue Aps. Figure 4.19 shows a screen shot of an intrusion detection log from one of the universities. From the intrusion detection screen shot all activities that were taking place are displayed with red alerts being issued when a rogue access point was detected ensuring the users can be able to take corrective actions on time.

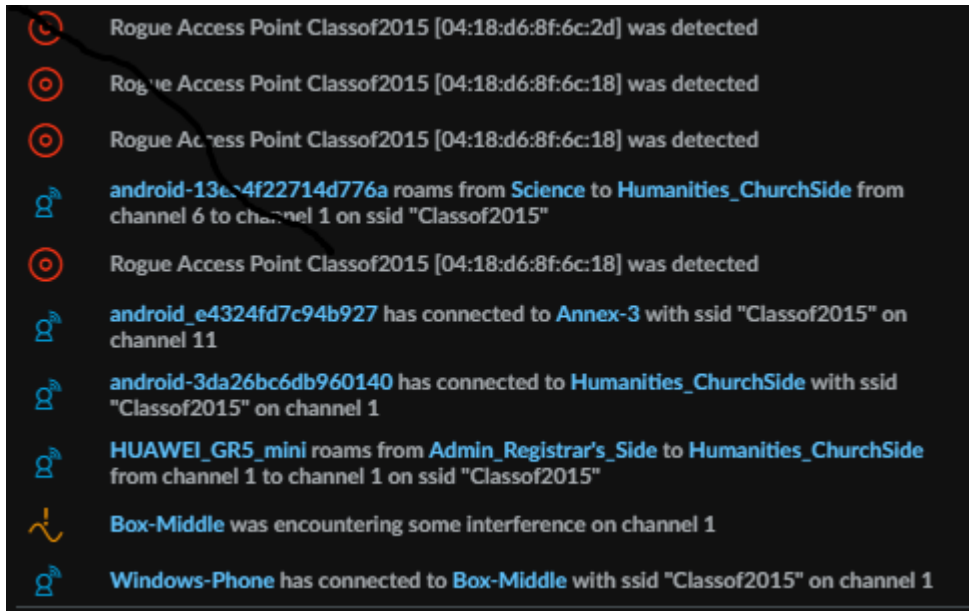


Figure 4.20: Intrusion Detection Logs

4.4 Vulnerabilities of the Wireless Campus Networks

i. Site survey and AP range

From the interview 12 of the network administrators had indicated that they had conducted a site survey to establish AP coverage and tested AP range boundaries to determine the extent of wireless coverage. However, the researcher carried out a practical check using a wireless network SSID scanner and a scan on an IPAD device. From the practical survey the researcher found out that APs broadcasted further than the boundaries in 9 of the universities where the network administrators had indicated they carried out network scan to identify the AP boundaries. The estimated usable range of each AP should not extend beyond the physical boundaries of the facility whenever possible to ensure security of the networks. Figure 4.20 show a screen shot of a network that had broadcasted beyond its boundary to neighbouring buildings.

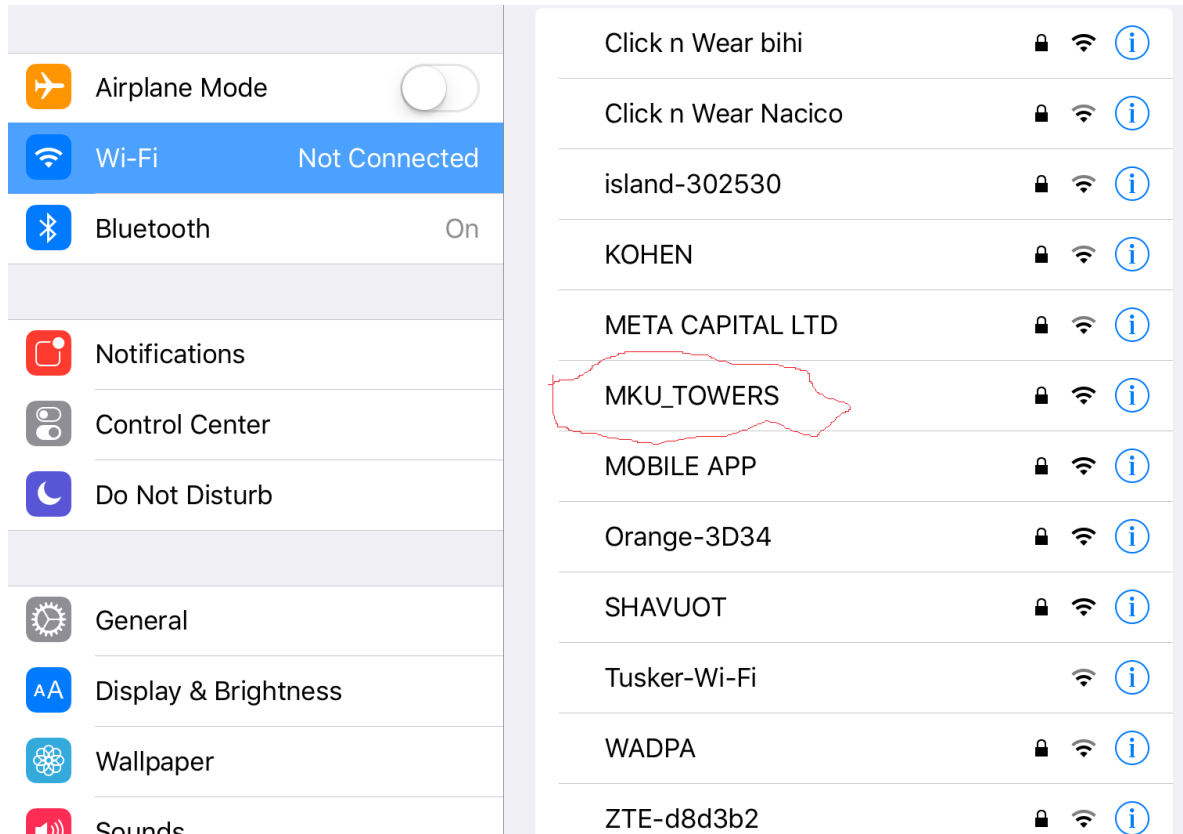


Figure 4.21: AP Broadcast beyond Boundary

A practical test was also conducted using the network scanner so as to determine the network broadcast channels. It was also found out that channels were overlapping for different APs especially in towns and around student hostels broadcast causing interference in the networks. All the respondents stated that the APs run all day and night even if they are in use or not. Figure 4.21 gives a screen shot of the scan in a given location. The results show that three Aps were broadcasting on channel one and channel six each in spite of the fact that some channels were not being used in the scanned location.

| MAC Address | RSSI | Chan | 802.11 | Max Speed | Vendor | First | Last |
|-------------------|------|------|---------|-----------|-------------------|----------|----------|
| 44:D9:E7:21:1B:94 | -91 | 1 | b, g, n | 130 Mbps | Ubiquiti Networks | 16:35:16 | 00:00:07 |
| D4:CA:6D:CE:4C:45 | -37 | 3+7 | b, g, n | 300 Mbps | Routerboard.com | 16:35:17 | now |
| 44:D9:E7:21:1C:7D | -88 | 6 | b, g, n | 130 Mbps | Ubiquiti Networks | 16:35:18 | now |
| E4:8D:8C:6D:68:7B | -91 | 3+7 | b, g, n | 300 Mbps | Routerboard.com | 16:35:26 | now |
| 44:D9:E7:21:1B:E1 | -91 | 6 | b, g, n | 130 Mbps | Ubiquiti Networks | 16:35:26 | now |
| D4:CA:6D:FC:92:89 | -88 | 6+10 | b, g, n | 300 Mbps | Routerboard.com | 16:35:28 | 00:00:49 |
| 44:D9:E7:21:1B:ED | -90 | 1 | b, g, n | 130 Mbps | Ubiquiti Networks | 16:35:44 | 00:00:06 |
| 04:18:D6:8F:6C:18 | -91 | 1 | b, g, n | 130 Mbps | Ubiquiti Networks | 16:35:59 | 00:00:05 |

Figure 4.22: Overlapping AP Channels

ii. SSID broadcast

From the interview with the network administrators and from the practical results using the network scanners. It was found that all the institutions broadcast their SSIDs. The SSIDs include university names, location names, students, staff, lectures, Department names, School names, Eduroam (a common SSID given as an initiative by the Kenya National Education Network to enable roaming of students and staff across campuses) and in 12 customized naming in assigning SSIDs were also noted. Broadcasting SSID with leading name such as office and department names are likely to attract attention of potential hackers. Figure 4.21 show a screen shot of a sample SSIDs as broadcasted in one of the universities

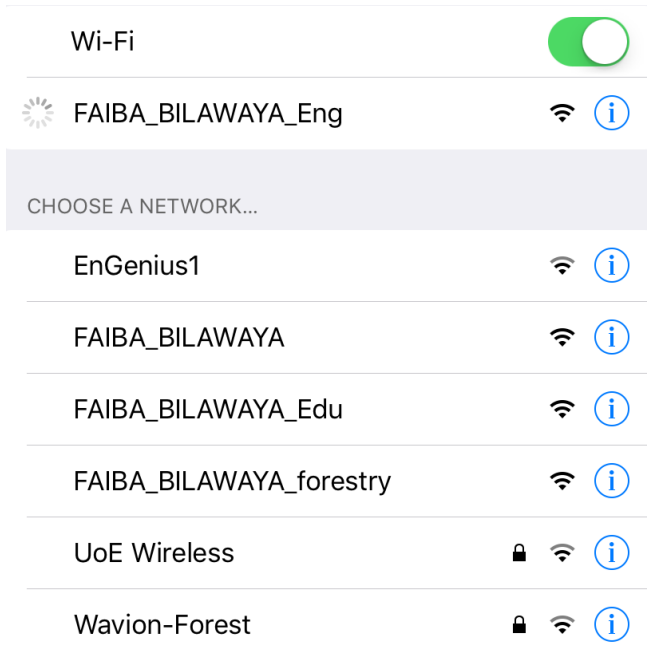


Figure 4.23: AP SSID Broadcast

iii. SNMP version

From the interview with the network administrators, it was found out that 19 of the universities use SNMP to manage the devices. However, 14 of the network administrators had their devices use SNMP versions one and two and other insecure and nonessential management protocols which are potential methods that an adversary can use when attempting to compromise an AP. 5 of the universities used the more secure versions. However, in 3 universities where SNMPv3 was used the network administrators did not configure it for least privilege (i.e., read only) even when write access was not required creating security loop holes.

4.5 Measures and Tools for Ensuring Improved Security of Wireless Networks

To ensure improved security of campus wireless network the respondents proposed: Use WPA2 Enterprise for authentication and use of separate VLANs, user management and

authentication, Mac Lockdown, all campus unified monitoring, frequent device monitoring and re-configuration, RADIUS authentication of users, Deploy of authenticated and encrypted wireless networks. Use of an online tool for measuring wireless security parameters against university settings will be helpful in ensuring maximum protection of the campus networks

4.6 Conclusion

It is evident from the results presented in this chapter that most campus wireless networks in universities in Kenya are insecure. Network administrators play a major role in ensuring security of university networks. Most of the time they make use of recommended security measures that are not unique to the individual institutions and in the process ignore important elements of ensuring wireless security. Many recommendations have been made by different authors to help organizations improve their wireless security posture. However, there is no tool or model that consolidates these recommendations that can be used by the universities to help find out areas of deficiencies with an aim of improving the same. Hence, as one of the objectives of this study, an automated tool and a model for ensuring improved wireless security is developed. The tool is based on the recommendations of the American National Institute of Science and Technology and can be accessed online by both the universities and other organizations that have wireless networks and would like to know how secure the networks may be. With this tool, the network administrators will be able to determine their threats, risks and vulnerabilities and get recommendations on what should be done to improve on security of the networks.

CHAPTER FIVE

SYSTEM DEVELOPMENT AND IMPLEMENTATION

5.0 Introduction

This chapter describes the development process of the Online Wireless Network Security Assessment Tool (OWNSAT). The Hypertext Preprocessor (PHP) has been used for designing the web-based interface; MySQL for system database and the Unified modelling language (UML) in design specifically to represent object-oriented system. The analysis of data from the previous chapter led to the first prototype. The OWNSAT developed accepts data systematically and analyzes to ease the burden of assessing the security of wireless networks. The technical aspects of the OWNSAT are also analyzed in this chapter. It covers the kind of technologies used and why they were chosen, and in what way the considered solutions could contribute to the study.

5.1 System Development Method

The Software prototyping approach was selected as the software development method for the development of the Online Wireless Network Security Assessment Tool. The selection of this model was guided by the need to understand the needs of the users and come up with system requirements at an early stage. In addition, it was possible to get user feedbacks enabling the researcher to understand what is expected from the solution.

Advantages of software prototyping;

- The prototype is a representation of the projected solution with reduced functionalities

- The users are able to evaluate the performance of the system and make recommendations for improvement before implementation
- The system developer gets the opportunity to understand the requirements that may have been considered in the initial stages
- Makes the system development process to be faster
- Clear and detailed understanding of requirements possible

The prototyping process consists of four main processes; functional selection, system construction, system evaluation and use of the system. The first step involves the selection of functions to be prototyped this is followed by the construction of the prototype. After construction the system is evaluated and the prototype is further used as a part of the new system or for outlining future system specifications. Prototyping is an iterative process that involves a four step involving users and developers:

- i. Initial requirement specification.
- ii. Prototype development.
- iii. The prototype is implemented, tested and used.
- iv. Revision and enhancement of the prototype.

During the process several iterations are undertaken with the third and fourth steps being repeated until the system is accepted by the user as shown in Figure 5.1

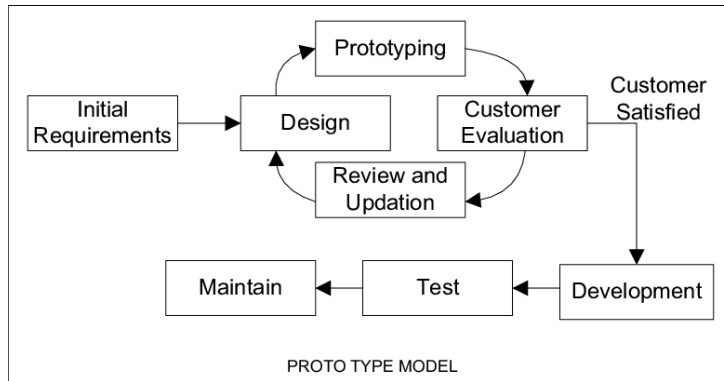


Figure 5.1: Prototype Model

5.2 System Requirements

In this section both the functional and non-functional requirements for the system are specified. Based the results of the data collection process and collected data presented in chapter 4.

5.2.1 Functional Requirements

The end goal of a software development project is to deliver a high quality tool. Functional requirements are the primary ways that the requirements are communicated to a project team. Functional requirements help to keep the project team going in the right direction. They include product features or functions that developers must implement to enable users to accomplish their tasks. The functional requirements for the proposed Online Wireless Network Security Assessment tool were derived from the interview, observation and practical experiments and were as follows:

- The system should be able to determine if the security measure in place are adequate enough to ensure the wireless networks are secured

- The system should be able to collect information from the network managers on the available configurations in their wireless networks.
- The system should be able to compute the possible vulnerabilities in a wireless network based on information provided by the network administrators.
- The system should be able to integrate a state of the art wireless security assessment criteria to be used as a basis of evaluation existing networks.
- The system should be able to give recommendations to users on areas they need to improve on to ensure their networks are more secure.
- The users of the system should be able to create accounts, reset passwords and update their details from time to time.
- The system should be accessible through a web page so as to widen access and usage
- The system should be able to keep history of assessments done by the network administrators from time to time.
- The system should be able to compute and present an analysis of all assessments done within a period of time.
- The system should also have an option for guest access.

5.2.2 Non-Functional Requirements

Non-functional requirements are quality attributes that describe the ways the system should behave. They include the following:

- **Availability:** the system's functionality and services should be available for use with all operations 99.99% of the time.

- Usability: the system should be easy to use by the farmers, the extension officers, and the administrator.
- Reliability: The system should work without failure for at least 10 years
- Scalability: The system must grow without negative influence on its performance.
- Data Integrity: the system should be in a position to secure access to confidential data for the users.
- Performance: the system should ensure optimal responsiveness to various user interactions with it at all times
- Recoverability: In case of failure, the system should have a self-recovery backup procedure
- Flexibility: Flexible service based architecture will be highly desirable for future extension
- Security: ensure that the software is protected from unauthorized access to the system and its stored data.
- Size: the system should be designed using miniaturized devices for portability
- Regulatory requirements: the system should confirm the traffic regulatory requirements

5.3 System Development

The development of the system was based on the above listed functional and no functional requirements. This was mainly guided by the findings of the study and specifications based on recommendations of the National Institute of Science and Technology. This provided a practical approach to the problem that started with a simple initial subset of the problem

and iteratively enhanced existing versions until a full system was implemented. At each step of the process, not only extensions but also design modifications were made. In fact, each step made use of stepwise refinement in a more effective way as the system became better understood through the iterative process. When users used the prototype a fuller understanding of the requirements was gained. New requirements were then implemented. The final system evolved in a continuous. Each successive prototype explored new user needs, and refined functionality that had already been implemented.

5.2.1 System Design

The Unified Modelling Language (UML) a standard language for specifying, visualizing, constructing, and documenting the artefacts of software systems, as well as for business modelling and other non-software systems was used. The UML has various diagrams such as Use Case diagrams, Sequence diagrams, and Class diagrams. For the design of the OWNSAT use case diagrams were used.

The use diagram the main actors and actions performed in the system. The main actors are the network administrators and other users who have information about their wireless network configurations and the system administrators who set different parameters to enable the system to function. Details of actions are specified in the diagram.

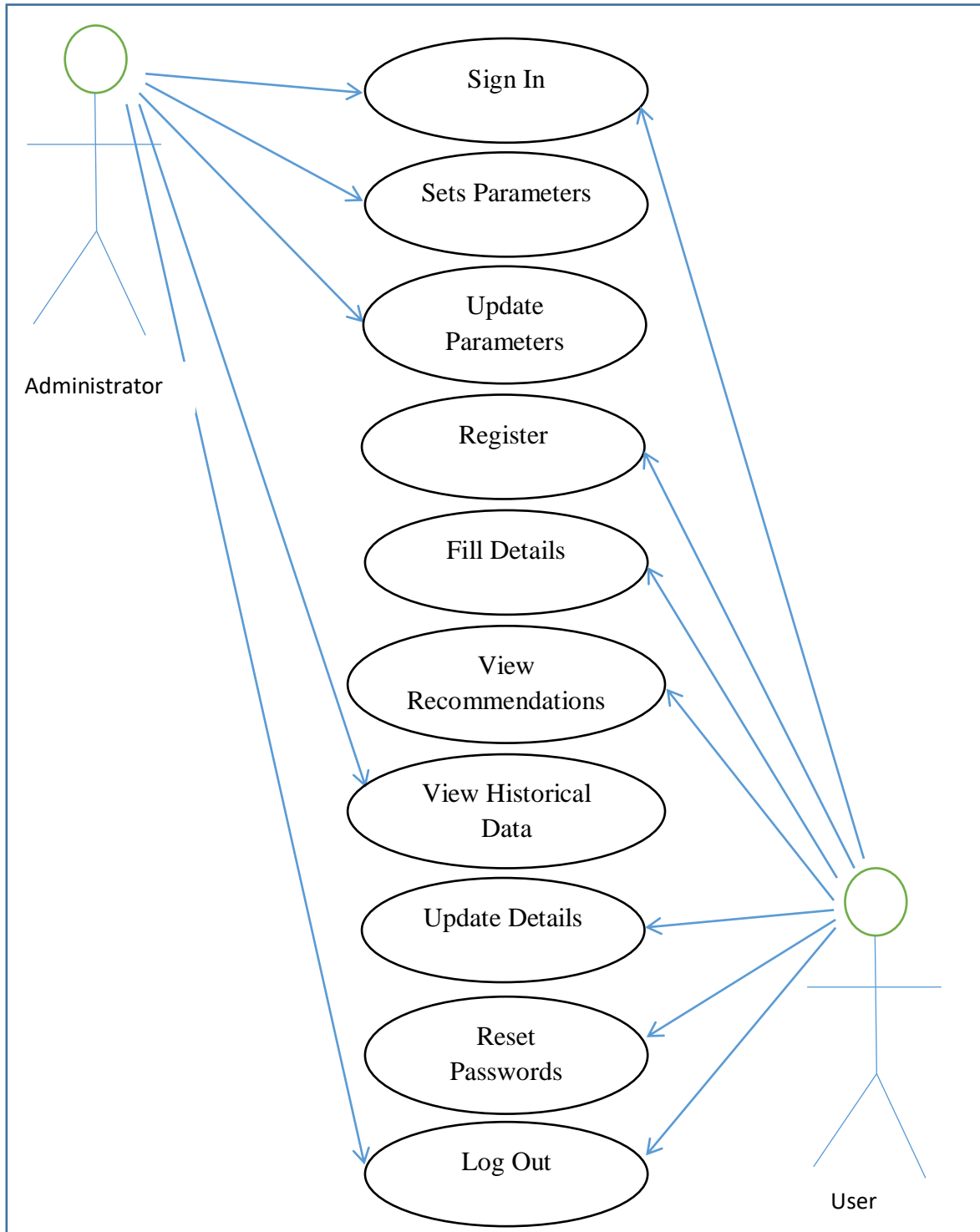


Figure 5.2: OWNSAT Use Case Diagrams

5.2.2 User Interface Design

PHP5 (Hypertext Preprocessor) was used for designing the web-based interface for the OWNSAT. This interface must be friendly and easy to use.

User Interface design Process

The design of the user interface for the system followed the steps below:

- ❖ Selection of the elements for the user interface;

The elements that were used for the user interface included the following;

- i. Input control: Some of the input controls used in the user interface design were; toggles, buttons, checkboxes, radio boxes and text fields
- ii. Navigational components: So as to ensure the users can navigate the system with ease different navigation styles were applied including the following; pagination, icons, search fields, tags, slider.
- iii. Informational components: Some of the informational components used in the user interface included; progress bar icons, tooltips, message boxes, and modal windows.

- ❖ Things to be considered for a best user interface were then listed

What was important so as to ensure a good user interface was the understanding of users, their goals, priorities and tendencies. Some of the consideration included the following;

- I. A simple interface for users: The first consideration was to ensure that the interface was clear to the users by rejecting of all unneeded elements ensuring a clarity in the language used throughout the system

- II. Ensuring consistency and use of know UI design elements: So as to ensure users can do thing quickly and that they are comfortable navigating through the system, common user interface design elements listed above were used. A pattern in design and layout was created and maintained so as to ensure efficiency.
 - III. Well-designed page layout; Different areas of network security were presented on different pages and present based on a systematic structure with each page being linked to others. In addition, items were placed in such a way as to draw the attention of the users and to aid navigation.
 - IV. Ensuring attractiveness: So as to attract the users a mixture of colours, images, icons texture, light and contrast were used
 - V. Selection of typeface; the type face used was also considered to enhance legibility and scan ability as the user use the system
 - VI. Prompt feedbacks to users; considerations were also made so as to ensure the users get appropriate information and feedback from the system including error and information messages from time to time.
- ❖ The user interface was then designed following the set elements and guidelines
 - ❖ After designing the system usability was then tested and refined. For the purposes of testing the researcher observed the users and also got feedback from them on areas that they experienced difficulties while using the system.

5.2.3 OWNSAT Database Management System (DBMS)

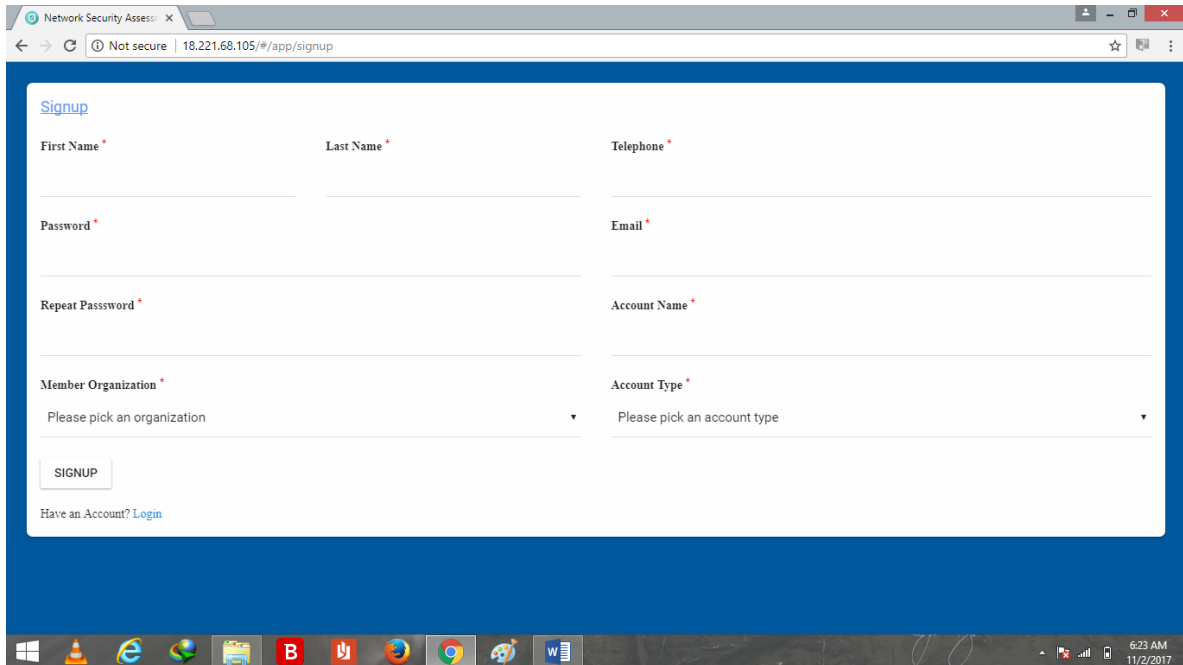
The success of an online based system relies on a good DBMS. MySQL is a popular choice of database for use in web applications. It is a fast and robust relational database management system enabling persistent storage, manipulation and retrieval of data. A database is essential for storing persistent data. MySQL was selected for the OWANSAT data, because it provides for our needs by efficiently storing and retrieving data. Another strong advantage was that MySQL is free open source software.

5.2.4 The Main Application and Interface

The OWNSAT is an online application accessible through a web browser (URL: <http://www.ownsat.ueab.ac.ke>); the prototype application was created in PHP using a MySQL database. The tool has several windows with components such as buttons and fields.

User Registration

The first step is to register as user in the system. Once a user is registered, the username and password is sent to his/her email.



The screenshot shows a web browser window with the address bar displaying "18.221.68.105/#/app/signup". The page title is "Network Security Assessment". The main content area is a registration form with the following fields:

- First Name *
- Last Name *
- Telephone *
- Password *
- Email *
- Repeat Password *
- Account Name *
- Member Organization * (dropdown menu with "Please pick an organization")
- Account Type * (dropdown menu with "Please pick an account type")

At the bottom of the form is a "SIGNUP" button and a link: "Have an Account? [Login](#)". The Windows taskbar is visible at the bottom of the screen, showing the time as 6:23 AM on 11/2/2017.

Figure 5.3: Registration Screen

User Log In

The user then clicks on a link to confirm registration by entering a user name and password.

If the correct user name and its accompanying password are entered, the user gains access to the system and can the access the easement tool or edit details.

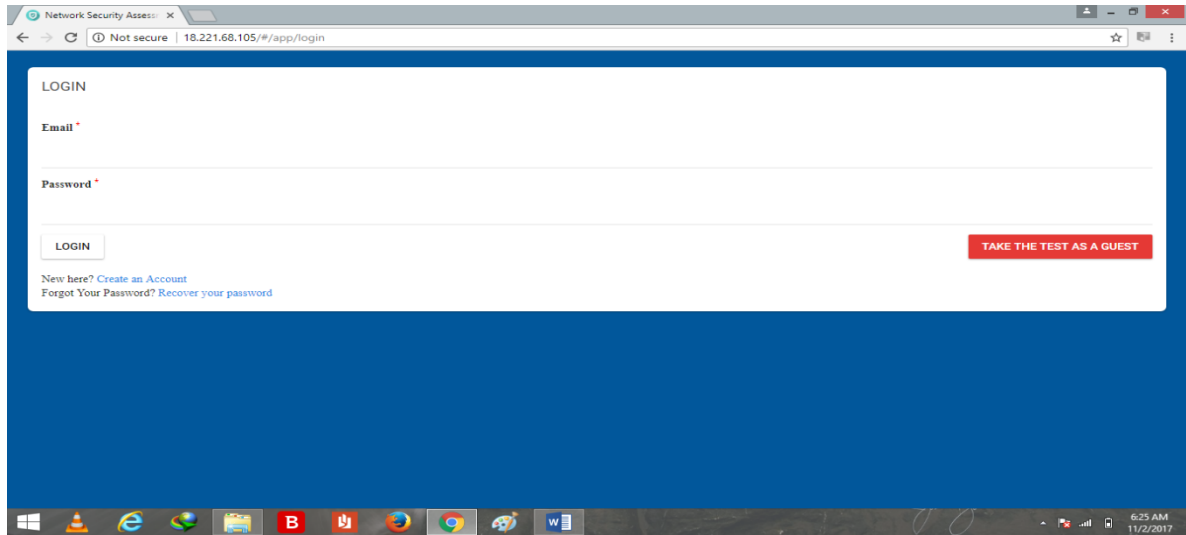


Figure 5.4: Log in Page

A user is able to reset his password in case it is forgotten. A link to reset the password will be sent to the users' email account.

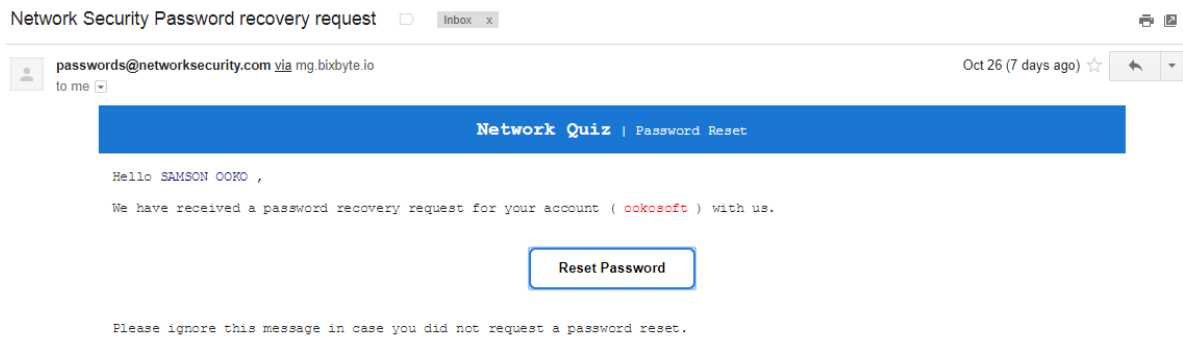


Figure 5.5: Password Reset Link

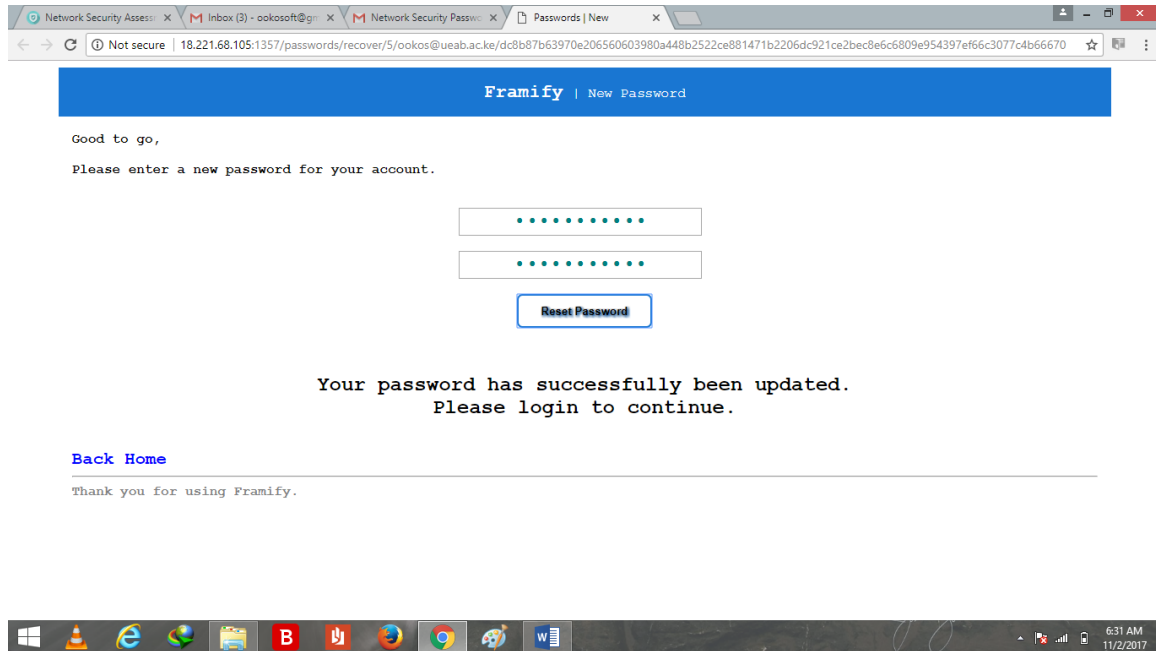


Figure 5.6: Password Reset Screen

In order to use the system, the Administrator's user name and password must be entered to unlock the system and connect it to the database. The administrator can then add new assessment parameters into the database. The database is used to store, adjust, retrieve and otherwise manipulate information. The database has tables and each table has related fields.

When the login button is clicked, the user name and password are checked in the database, if the user name and password are correct, the user is logged on and the main page is displayed. From the main page the user can edit his/her details or perform assessments

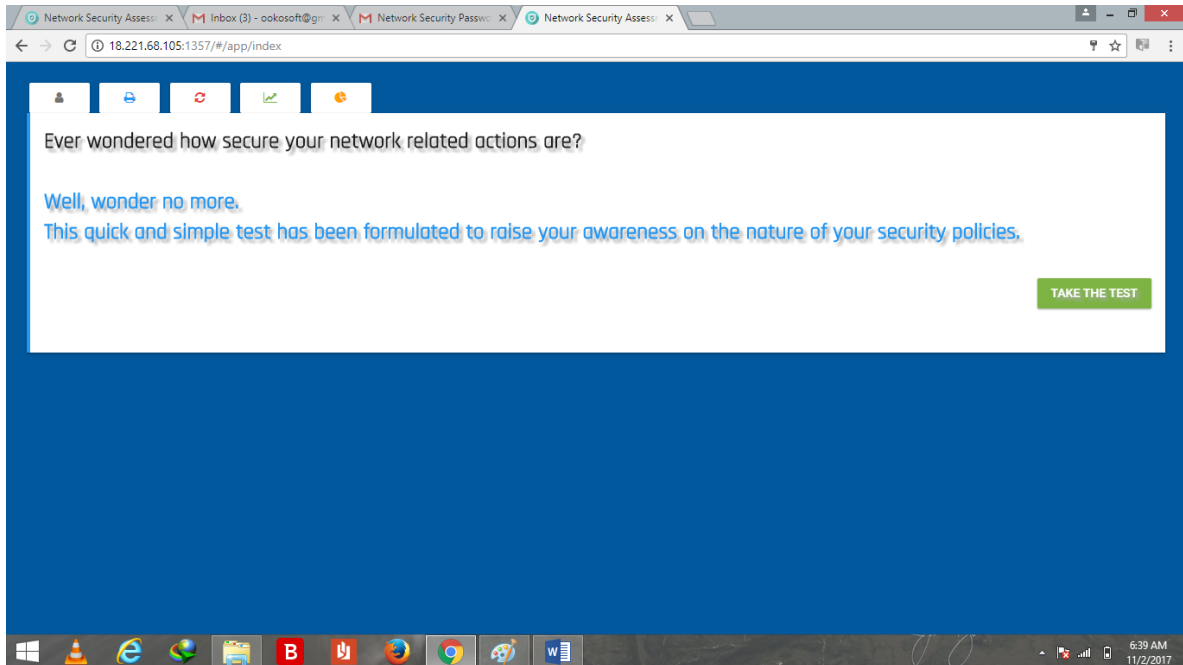


Figure 5.7: Users Main Page

Assessment Page

On the user's main page as shown above there is a link to the assessment page where the user will be able to fill in the network set up details and other the organizations parameters. Once all the parameters have been fully populated the user clicks on the submit button and the recommendations page is then loaded

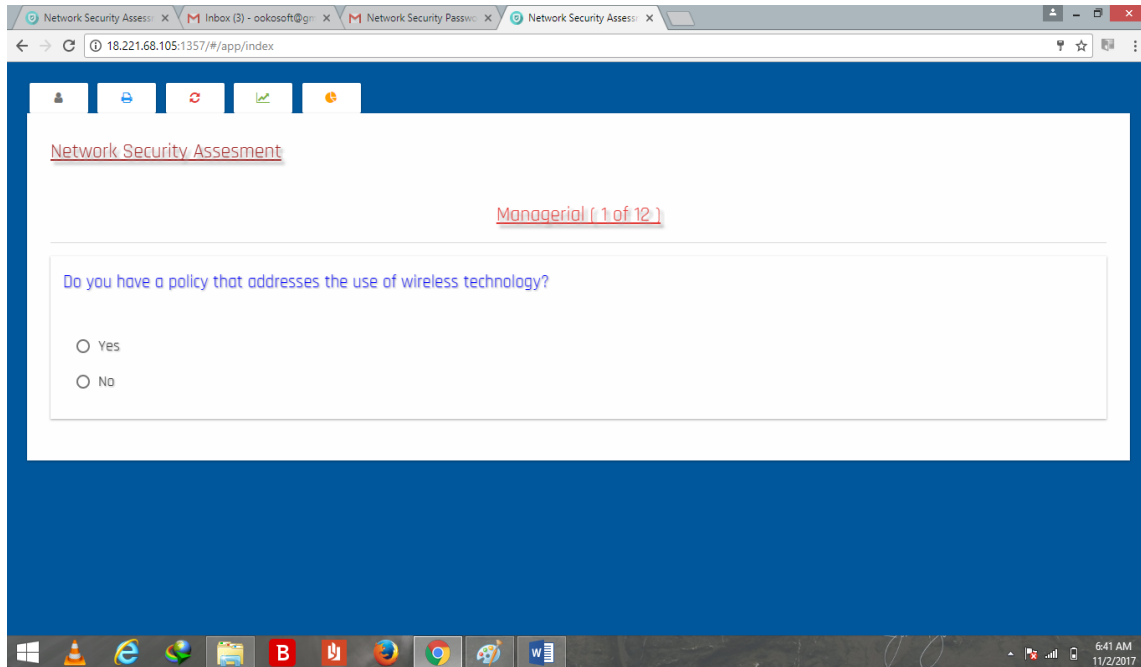


Figure 5.8 Assessment Page

Other areas of assessment included the following;

- ❖ Training of network users on computer security awareness and risks associated with wireless security
- ❖ Risk assessment to understand the value of the assets in the university that need protection
- ❖ Firmware upgrade on Aps and client NIC
- ❖ Security assessment to understand the wireless security posture
- ❖ Measures in place to physically secure your wireless devices
- ❖ Site survey to establish AP coverage for the university
- ❖ Inventory of all wireless devices
- ❖ compliance with the universities security policy
- ❖ APs locations

- ❖ Guest User Policy
- ❖ AP range boundaries to determine the extent of wireless coverage
- ❖ handling APs that are not used (e.g. After Hours)
- ❖ use of the reset functions
- ❖ SSID used for your APs
- ❖ broadcasting of SSID for APs
- ❖ network monitoring tools
- ❖ authentication methods used for devices and wireless users and which encryption methods
- ❖ firewalls and access lists configured on APs
- ❖ antivirus software on wireless clients
- ❖ firewall on wireless clients
- ❖ separation of the wireless network from the wired infrastructure
- ❖ change of passwords for wireless devices
- ❖ use of static or dynamic IP addressing
- ❖ disposal of wireless devices no longer in use
- ❖ review of device logs
- ❖ version of SNMP used
- ❖ intrusion detection agents on the wireless part of the network to detect suspicious behaviour or unauthorized access and activity
- ❖ cases of security breach on wireless networks
- ❖ recommendations to ensure improved security of campus wireless networks

Recommendations Page

Recommendations are populated best on assessment scores. For each of the response given by the users a related recommendation is give so that the network administrators can make use of the recommendation to improve on that specific area in their network. Such a strategy ensures there is no generalization and that all vulnerabilities are taken care off

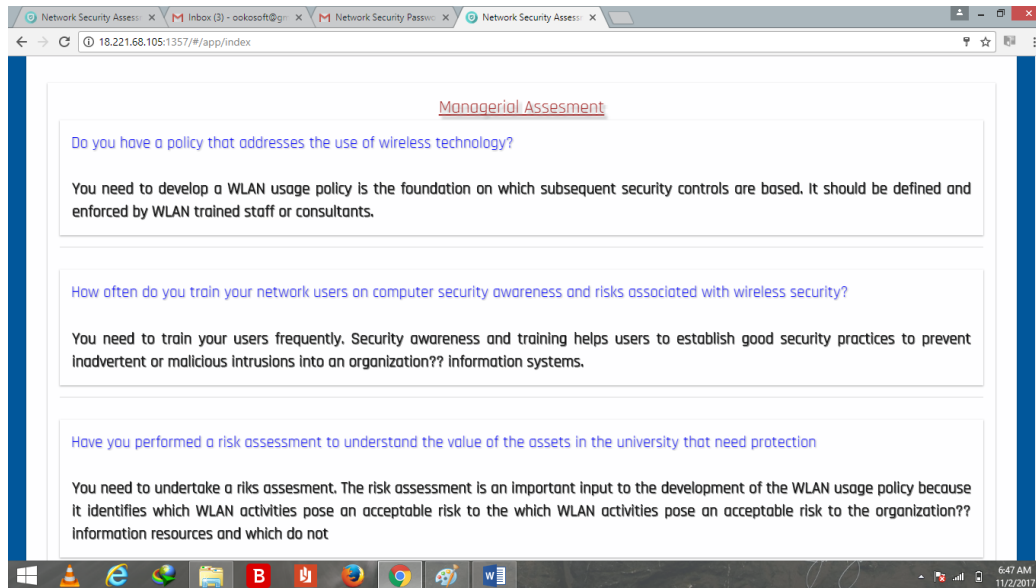


Figure 5.9: Recommendations Page

Review Page

A registered user can review score and recommendations as well us how the overall status of responses. This can only be reviewed by a registered user so as to ensure that only authorized users can view the results of their assessment thus enhance privacy.

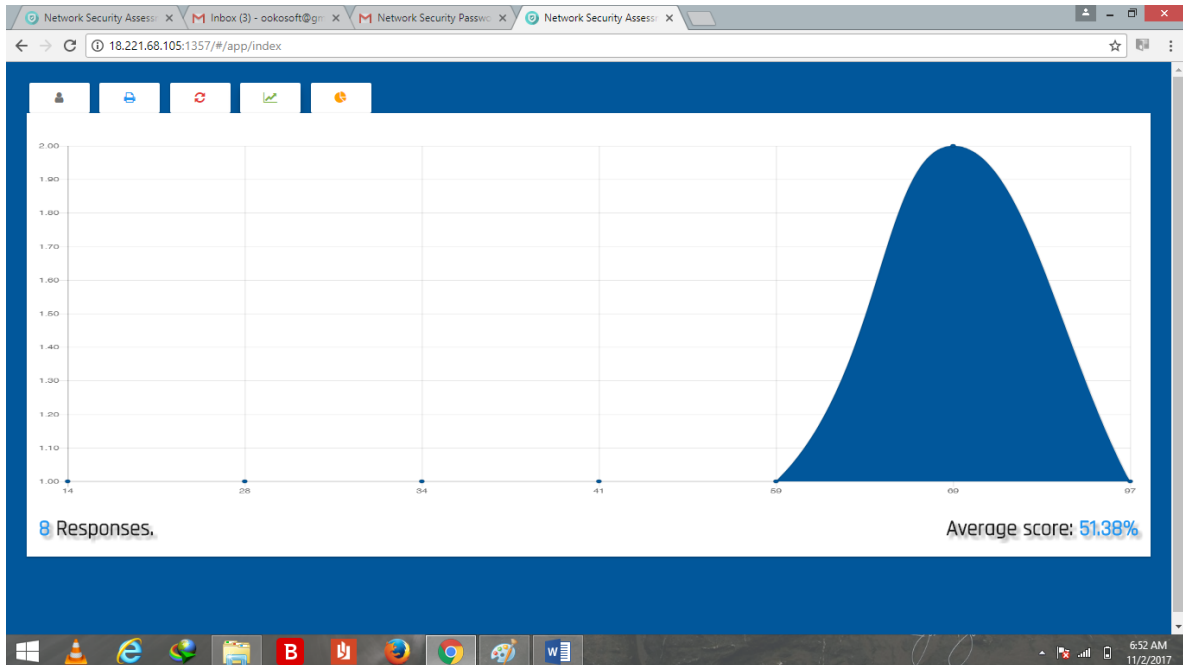


Figure 5.10: Responses Review Page

5.2.5 System Implementation

This stage builds on the results of all the prior stages. This phase involved deploying and making the OWNSAT available for the users. Deploying the tool involved executing all the necessary steps necessary to educate the users on the use of the software, developing user manuals, placing the tool into production, confirming availability of the tool and the accuracy of operation. All the hardware and software requirements were adhered to.

5.2.6 System Validation and Verification

Verification and Validation (V&V) was done to check that OWNSAT meets specifications and that it fulfils its intended purpose. This was the only way to ensure software quality control. There were two ways used to perform the software validation: internal and external. During internal software validation involved ensuring that the goals of the

stakeholders who were mainly the network administrators were correctly understood and that they were expressed in the requirement artefacts precise and comprehensively. In doing this a checklist was used to compare the performance of the system against the functional and non-functional requirements.

External validation involved asking the stakeholders if the software meets their needs. External validation is a continuous event. External validation was successful since all the stakeholders accept the software product and express that it satisfies their needs. This was done by allowing the network administrators to use the system and see if it compares to other available wireless security assessment tools.

Verification was done by reviewing the system associated specifications, based on the review it was concluded that the specifications were met.

5.2.7 Difference with other Tools

The OWNSAT is different from other available assessment tools in the following ways.

- ❖ It covers all areas of wireless security unlike most tools that focus on a given area
- ❖ It available online and free for use
- ❖ The users can registrar and perform several assessments while history of the assessment are kept
- ❖ Guest assessments are allowed
- ❖ The user get feedback for each specific item of assessment thereby avoid generalization

CHAPTER SIX

SUMMARY, CONCLUSION AND RECOMMENDATIONS

6.0 Introduction

This chapter presents the conclusions, recommendations and directions for future study. The chapter is divided into five sections which include: summary, findings, conclusion, recommendations and directions for future research

6.1 Summary

The purpose of this study was to investigate the security of wireless campus networks for selected universities in Kenya based on research parameters which could lead to the development of an OWNSAT. This was mainly necessitated by the fact that use of wireless devices are becoming popular and so are security threats related to wireless networks that have been witnessed in all sectors including universities in Kenya.

From the reviewed literature security was a major challenge to wireless networks. However, limited research has been conducted on security of wireless networks in Kenya. Even though recommendations have been made on how to assess the security of wireless networks, there are no online tools that can be used to assess the security of wireless networks making it difficult for network administrators to conduct assessments if any.

A qualitative study was conducted by use of interviews, observation and practical tests from twelve public chartered and seven private chartered universities in Kenya. The respondents were purposively selected based on known investment in wireless technology

and distribution in the country. Data was descriptively analyzed and findings presented in relation to the research objectives and research questions.

An online wireless security assessment tool was then developed using the software prototyping development method. The OWNSAT was based on PHP with MySQL being used as the database management system.

6.2 Findings and Discussion

The findings have been grouped based on the research questions that guided the study. The research questions were:

- i. What are the security risks associated with wireless campus networks in the selected universities in Kenya?
- ii. Which measures are in place to ensure security of wireless networks in the selected universities in Kenya?
- iii. How vulnerable are wireless campus networks in the selected universities in Kenya?
- iv. Which is the best model and tool to ensure security of wireless campus networks?

Based on the respondent's profile more public universities than private universities participated in the study. This was because in general there are more public universities in Kenya

6.2.1 Findings on Research Question 1

On Risk Assessment

Network administrators from 16 of the 20 universities are not aware of the risks that they face during the day-to-day operation of the networks and are therefore not likely to make informed decisions on how to protect themselves and even user from the threats they face.

On Patches and Upgrades

60% of the network administrators installed patches and upgrades frequently, while 35% of them installed the patches sometimes even though some network officers install the patches without testing, this can lead to security problems in case the patches have bugs.

On Security assessment

55% of the network administrators have not performed security assessments and are therefore not able to identify the corrective actions on time, thus are not able to maintain an acceptable level of security.

On Inventory

Many institutions had an inventory of their wireless devices

On Disposal

The methods of disposals pose a security risk for the universities especially when the devices are not reset so as to conceal organizational settings

On System logs

18 out of the 20 network administrators reviewed their security logs, this enabled the security and support staff to identify potential security issues and respond accordingly. Frequent reviews of audit logs allowed security and support personnel to identify security issues and take corrective or preventative measures quickly.

On Network separation

86% of the universities had separate wireless and wired networks with 43% of them using dedicated VLANs which facilitated the use of network access control lists, which identified the protocols and services that were allowed to pass from WLANs to the DS. Different VLANs were defined within the wireless connections to further separate varying security policies.

On Guest access

Based on data from 16 universities did not offer the best policies and solutions and allowed the guest users to access the same network as the organization staff and students thus may be faced with challenges of hacking from guest accounts

On IP Addressing

76% of the universities used dynamic addressing due to convenience, this method makes it difficult to track and control access based on IP addresses creating a security management challenge to the administrators.

6.2.2 Findings on Research Question 2

On Policy

65% of the universities from which data was collected do not have a well-defined WLAN security policy. This leaves the institutions at a vulnerable situation given the fact that without a policy it is easy to overlook important security requirements.

On User training

Over 45% of the users had not undergone security awareness and training with 30% of the user being trained only sometimes, this may imply that the users were not able to establish good security practices to prevent inadvertent or malicious intrusions into universities network and information systems. This means some of the users may unintentionally perform actions that can create security risk to the universities.

On Physical security

Many institutions have put measures that were effective in ensuring the physical security of the devices in spite of few cases of theft reported.

On Use of reset function

In 17 of the universities from which data was collected only authorized personnel could use the reset function. Given the fact that the devices were physically secured it was difficult for any other user to reset.

On Network Monitoring

For the purposes of network monitoring the universities indicated that they used; Simple Network Management Protocol (SNMP) which is a protocol for network management.

Others use open NMS which is an open source enterprise network management tool. They also use Cacti, Smokping. It was however noted that some institutions did not have any network monitoring mechanisms.

On Authentication

For authentication the institutions use; Radius servers, MAC address access control, captive portal, passwords, WPA2, 802.1x authentication with DES and 3DES, 802.1x EAP, PEAP-MSCHAP v2. There was an institution that had no authentication enabled for users, allowing anybody on campus and neighbouring community to access their network. Authentication methods used in some of the universities are not very secure and are not combined with any encryption methods. It was also interesting to note that the universities put more emphasis on access to the network; once the users are authenticated there were limited measures in place to ensure security of the connected users and systems.

On Firewalls

All the universities from which data was collected are at a risk because they did not have personal firewall and anti-virus software for all STA platforms for which such security products are commercially available. It was also noted that remote connectivity to the devices (e.g., file sharing, open network ports) was not limited as recommended. There were many ports that were open but not in use providing backdoors for possible breach in security of the network.

On Passwords

In 11 of the institutions the network administrators had never changed their setup passwords this makes many universities to be exposed to dictionary attacks. In addition, many universities also used a common and/or default password for multiple Aps making them vulnerable. A compromised password on one AP could have much wider consequences.

On Intrusion detection

15 out of the 20 institutions from which data was collected had intrusion detection systems deployed on the wireless network. These help detect and respond to potential malicious activities, including unauthorized WLAN vulnerability scanning and the installation of rogue Aps

6.2.3 Findings on Research Question 3

On Site survey and AP range

Aps in 9 institutions broadcasted further than the boundaries indicated by the respondents. The estimated usable range of each AP should not extend beyond the physical boundaries of the facility whenever possible to ensure security of the networks.

In addition, channels were overlapping for different APs especially in towns and around student hostels broadcast causing interference in the networks.

On SSID broadcast

All the institutions broadcast their SSIDs some of which had leading names. Broadcasting SSID with leading name such as office and department names are likely to attract attention of potential hackers.

On Management Protocols

14 of the universities from which data was collected used insecure and nonessential management protocols which are potential methods that an adversary can use when attempting to compromise an AP.

6.2.4 Findings on Research Question 4

There was an attempt by the universities to put varied measures in place to ensure security of the wireless campus networks. There are few tools that can be used to measure certain aspects of security of the networks. However, important areas as noted in the findings are left out mainly because there is no single tool that guides the process to comprehensively measure the total security of the networks. Use of an online tool for measuring wireless security parameters against university settings will therefore be helpful in ensuring maximum protection of the campus networks.

6.3 Conclusion

From the findings of the study it is evident that campus wireless networks in most universities in Kenya are fairly not secure with less than 7 of the universities proving to have set enough measures in place to secure their networks. Efforts, even though not

comprehensive, have been put in place by other different universities to ensure security of the networks.

Some of the major concerns are: limited risk assessments, installing patches and upgrades without testing, limited security assessments, Poor disposal practices, inadequate security and access policies, dynamic IP addressing, inadequate user awareness and training on wireless network security, insufficient monitoring strategies, insecure authentication methods, open unused ports, use of one off passwords, overlapping channels, broadcasting beyond boundaries, insecure management protocols and broadcasting leading SSIDs.

It was found out that the universities have however managed to; frequently review system logs, keep an inventory of network devices, Separate networks based on users, physically secure networks devices and deploy intrusion detection systems.

It was noted that even though there exist tools that can be used to measure the security of various aspects of wireless campus networks. There is however, no single tool to guide the network administrators to assess the security of their networks that covers all the aspects from managerial to technical aspects and many assumed they had put enough measures in place to secure the networks. The OWNSAT will therefore help not only universities but also other sectors to be able to assess the security of their networks and thereafter act on given recommendations/

6.4 Recommendations

The researcher recommends the use of a Wireless Network Security Model (WNSM). The WNSM is a modified version of the Network Security Model (NSM) developed by the

SANs Institute which is a seven-layer model that divides the task of securing a network infrastructure into seven manageable sections. The model is generic and can apply to all security implementation and devices. The WNSM makes use of the same number of layers in the NSM however the activities in each layer have be reorganized and customized to wireless networks. When an attack on a network has succeeded it is much easier to locate the underlying issue and fix it with the use of the WNSM. The WNSM provides a way to implement basic network security measures and devices as well as locate underlying issues that may have allowed an attack to succeed.

| | |
|------|----------------------|
| i. | Physical Layer |
| ii. | Network Layer |
| iii. | Authentication layer |
| iv. | Software Layer |
| v. | User Layer |
| vi. | Management Layer |
| vii. | Administrative Layer |

Figure 6.1 Wireless Network Security Model

The specific recommendations from the findings of the study have been classified into the layers of the WNSM in which they should be implemented with the research questions that each addresses being shown.

The research questions were:

- i. What are the security risks associated with wireless campus networks in the selected universities in Kenya? (Q1)
- ii. Which measures are in place to ensure security of wireless networks in the selected universities in Kenya? (Q2)
- iii. How vulnerable are wireless campus networks in the selected universities in Kenya? (Q3)
- iv. Which is the best model and tool to ensure security of wireless campus networks? (Q4)

1. The Physical Layer

The physical layer's primary focus is on physical security of all the wireless devices. Physical security is applied to prevent attackers from reaching the access point and other network devices. Physical security is the first chosen layer because it is a breaking point for any network. In any scenario providing other devices, such as firewalls, will not help your security if the physical layer is attacked.

From the findings of the study many universities had physically secured their networks however the researcher recommends the following:

1. Aps should be configured by the network administrators in different channels to avoid overlaps and located in appropriate places to prevent broadcasting beyond boundaries (Q1).
2. SSIDs should be hidden and when broadcast they should not reflect the institutions and departments they serve (Q1).

2. Network Layer

The network layer deals with the creation and maintenance of Virtual Local Area Networks. VLANs are used to segment networks for multiple reasons mainly to group together common hosts for security purposes.

The researcher recommends that wireless networks should be on separate VLANs for specific group of users (Q3).

3. Authentication Layer

The authentication layer is focused on the creation and maintenance of Access Control Lists. ACLs are created to allow and deny access between hosts on different networks, usually between VLANs.

The researcher recommends the following:

1. The Universities should undertake a risk assessment to enable them find out the risks that they face during the day-to-day operation of the networks (Q2)
2. Secure authentication methods should be integrated with secure encryption methods to ensure improved security (Q3)
3. Adequate firewalls that will ensure all ports not in use are blocked should be put in place (Q3)

4. Software Layer

The software layer is focused on keeping software up to date with upgrades and patches in order to mitigate software vulnerabilities.

The researcher recommends that all devices should be frequently upgraded and before installing any patches and upgrades the universities should conduct tests to ensure all bugs are eliminated (Q2).

5. User Layer

The user layer focuses on the user's training and knowledge of security on the network. The user should understand basic concepts in network security.

The researcher recommends that universities should conduct frequent trainings and introduce awareness programs on network security from time to time (Q3)

6. Management Layer

The management layer focuses on the training of administrative users. The administrative layer includes all members of management.

The researcher recommends that universities should train the staff on regular basis to keep up with the changing technologies (Q3)

7. Administrative Layer

The administrative layer contains all of the network security professionals, network technicians, architects, and support specialists. These are all of the people that make a network operational, and maintain the network, and all of the hosts that reside on that network. The administrative is like the management layer except the administrative layer has accounts to access any device on the network.

Based on the findings of the study the researcher recommends the following:

1. The universities should conduct frequent security assessments to be able to identify the corrective actions on time (Q1)
2. Appropriate policies should be formulated by the universities. These should include Security Policies, Access Policies, Acceptable use policies, Disposal Policies, Password Policies, Guest Access Policies (Q3)
3. The universities should use the online tool to assess the security of their networks so as to find recommendations specific to each university (Q4)
4. Universities should put in place efficient monitoring techniques and review from time to time (Q4)
5. Universities should use secure management protocols (Q2)

6.5 Suggestions for Future Research

This study examined the security of wireless networks in selected universities in Kenya.

The results of this study will serve as a baseline for ensuring security of wireless networks in general. Future research may be made in the following areas:

1. A study should be conducted on the security of information systems in universities in Kenya. Just securing the wireless network alone is not enough but security but also the security of information systems is mandatory
2. A study should be conducted on security of wired local area networks in the universities in Kenya
3. A study should be all carried out to determine hindering the implementation of security controls in universities

REFERENCES

- (USAO), U. S. A. O. (2011). *U.S. Attorney's Office - U.S. Department of Justice*.
- Alliance_WiFi. (2020). *Quarterly update (December 2021): Wi-Fi 6E devices driving technology innovation | Wi-Fi Alliance*. <https://www.wi-fi.org/beacon/the-beacon/quarterly-update-december-2021-wi-fi-6e-devices-driving-technology-innovation>
- Artit, K. (2012). Management Information System Implementation Challenges , Success Key Issues , Effects and Consequences : A Case Study of Fenix System. *Jokoping International Business School.*, 1(May), 7–67.
- Aspinwall, J. (2003). *Installing, Troubleshooting, and Repairing Wireless Networks*. John Wiley & Sons Inc.
- Aubuchon, K. (2014). *Universities Account for a Higher Number of Breaches*. <http://www.infosecisland.com/blogview/16161-Universities-Account-for-a-Higher-Number-of-Breaches.html>
- Bargh, M. S., Hulsebosch, R. J., Eertink, E. H., Prasad, A., Wang, H., & Schoo, P. (2004). Fast authentication methods for handovers between IEEE 802.11 wireless LANs. *Proceedings of the Second ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots, WMASH 2004*, 51–60. <https://doi.org/10.1145/1024733.1024741>
- Barron, E. N. (2013). *Game Theory: An Introduction - (Second)*. John Wiley & Sons, Ltd. https://books.google.co.ke/books?hl=en&lr=&id=BxzmawiCLGwC&oi=fnd&pg=PP6&dq=An+Introduction+to+Game+Theory&ots=BtQEYf1ks6&sig=lomO3rPrFI98CWnaRhSgdLCATU&redir_esc=y#v=onepage&q=An+Introduction+to+Game+Theory&f=false
- Bawiskar, A., Sawant, P., & Meshram, B. B. (2013). Wireless Security Threats, Vulnerabilities and Their Defense Mechanisms. *International Journal of Electronics and Computer Science Engineering*, 2(1), 385–394. www.ijecse.org
- Bodhe, A., Masuti, M., & Umesh, A. S. (2016). Wireless LAN Security Attacks and CCM Protocol with some best practices in Deployment of Services. *International Research Journal of Engineering and Technology (IRJET)*, 3(1), 429–436. www.irjet.net
- Burrowes, A. (2005). Core Concepts of Accounting Information Systems. *Issues in Accounting Education*, 2, 216–217. <https://www.wiley.com/en-us/Core+Concepts+of+Accounting+Information+Systems%2C+14th+Edition-p-9781119373667>

- Ceric, A. (2015). Bringing together evaluation and management of ICT value: a systems theory approach. *Electronic Journal of Information Systems Evaluation*, 18(1), 19–35. <https://academic-publishing.org/index.php/ejise/article/view/185>
- Comer, D. (2015). *Computer networks and internets*. http://h222767.temppublish.com/14_NW/175_Lecture_Notes.doc *Cyberoam Security Assessment Report*. (2015).
- Do, D. T., & Van Nguyen, M. S. (2019). Device-to-device transmission modes in NOMA network with and without Wireless Power Transfer. *Computer Communications*, 139, 67–77. <https://doi.org/10.1016/j.comcom.2019.04.003>
- Dobrilovic, D., Stojanov, Z., Jäger, S., & Rajnai, Z. (2016). A method for comparing and analyzing wireless security situations in two capital cities. *Acta Polytechnica Hungarica*, 13(6), 67–86. <https://doi.org/10.12700/aph.13.6.2016.6.4>
- Dongmei, Z., Changguang, W., & Jianfeng, M. (2007). A RISK ASSESSMENT METHOD OF THE WIRELESS NETWORK SECURITY 1. *JOURNAL OF ELECTRONICS*, 24(3). <https://doi.org/10.1007/s11767-006-0247-6>
- Firch, J. (2021). *Common Types Of Network Security Vulnerabilities In 2021*. Purplesec.Us. <https://purplesec.us/common-network-vulnerabilities/>
- Flickenger, R. (2002). *Building wireless community networks*. <http://www.tikismikis.org/wi/doc/bwcn.pdf>
- Gast, M. (2010). *802.11® Wireless Networks: The Definitive Guide*.
- Graneheim, U., & Lundman, B. (2004). Qualitative content analysis in nursing research: concepts, procedures and measures to achieve trustworthiness. *Elsevier*. <https://www.sciencedirect.com/science/article/pii/S0260691703001515>
- John Wack, Miles Tracy, M. S. (2003). Guideline on Network Security Testing. *Recommendations of the National Institute of Standards and Technology, NIST Special Publication 800-42, October*. <https://doi.org/10.6028/NIST.SP.800-42>
- Karygiannis, T., & Owens, L. (2002). *Wireless Network Security*. http://all.net/books/standards/NIST-CSRC/csrc.nist.gov/publications/nistpubs/800-48/NIST_SP_800-48.pdf
- Kashorda, M., & Waema, T. (2014). E-Readiness Survey of Kenyan Universities (2013) Report,. *Kenya Education Network*.

- Kavianpour, A., & Anderson, M. C. (2017). An Overview of Wireless Network Security. *Proceedings - 4th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2017 and 3rd IEEE International Conference of Scalable and Smart Cloud, SSC 2017*, 306–309. <https://doi.org/10.1109/CSCloud.2017.45>
- Kenya Cyber Security Report 2015*. (2015). www.serianu.com
- Kigen, M. P., Kisutsa, C., Muchai, C., Kimani, K., Mwangi, M., Shiyayo, B., Johnstone, F. A., Ceo, N., Research, T., Apudo, A. B., Mathenge, G., Muya, T., & Mathenge, J. (2014). *KENYA CYBER SECURITY REPORT 2014 Rethinking Cyber Security – “An Integrated Approach: Processes, Intelligence and Monitoring.”*
- Kim, S., Lim, H., Lim, S. M., & Shin, I. H. (2018). Study on cyber security assessment for wireless network at nuclear facilities. *6th International Symposium on Digital Forensic and Security, ISDFS 2018 - Proceeding, 2018-January*, 1–5. <https://doi.org/10.1109/ISDFS.2018.8355332>
- Legnitto, J. (2012). *Have You Been Hacked Using On Campus Wifi? – Private WiFi*. <https://blog.privatewifi.com/have-you-been-hacked-using-on-campus-wifi/>
- Liang, X., & Xiao, Y. (2013). Game theory for network security. *IEEE Communications Surveys and Tutorials*, 15(1), 472–486. <https://doi.org/10.1109/SURV.2012.062612.00056>
- Newman, R. E. (2017). *Computer and Network Security Introduction to Computer and Network Security*.
- Palmieri, F., Fiore, U., & Castiglione, A. (2011). Automatic security assessment for next generation wireless mobile networks. *Mobile Information Systems*, 7(3), 217–239. <https://doi.org/10.3233/MIS-2011-0119>
- Rawat, P., Singh, K. D., Chaouchi, H., & Bonnin, J. M. (2014). Wireless sensor networks: A survey on recent developments and potential synergies. *Journal of Supercomputing*, 68(1), 1–48. <https://doi.org/10.1007/s11227-013-1021-9>
- Roberts, C. (2013). *Student hacks Florida university’s wireless network — redirects users to porn site to expose security flaws - New York Daily News*. <https://www.nydailynews.com/news/national/student-hacks-school-wireless-network-redirects-users-porn-site-article-1.1286260>
- Ross, D. (2005). The Security of Wireless Computing Technologies. *AusCERT Conference*.
- Scarfone, K., & Dicoi, D. (2007). Wireless Network Security for IEEE 802.11 a/b/g and Bluetooth (DRAFT). *NIST Special Publication*, 800, 48. http://www.w1npp.org/events/2008/fieldday/UsbNet/IEEE_802.11n/WIRELE~1.PDF

- Stein, L. D., Boncella, R. J., Rubin, A. D., & Geer, D. E. (1998). Web Security: A step-by-step reference guide. In *Computer* (Vol. 31, Issue 9). Addison-Wesley.
- Stimpson, T., Liu, L., Zhang, J., Hill, R., Liu, W., & Zhan, Y. (2012). Assessment of security and vulnerability of home wireless networks. *Proceedings - 2012 9th International Conference on Fuzzy Systems and Knowledge Discovery, FSKD 2012*, 2133–2137. <https://doi.org/10.1109/FSKD.2012.6233783>
- Tadelis, S. (2013). Game theory: An introduction. In *Game Theory: An Introduction*. Princeton University Press. https://doi.org/10.1142/9789812835178_0009
- Và, T. H. (2018). *Hacking Exposed Wireless, 2nd Edition*. https://www.academia.edu/36056571/Hacking_Exposed_Wireless_2nd_Edition
- Wireless Security Assessment*. (2021). <https://securelayer7.net/radio/wireless-security-assessment>
- Wireless Security Assessment | GuidePoint Security*. (2021). <https://www.guidepointsecurity.com/wireless-security-assessment/>
- Xiao, Y., Chen, H., Yang, S., Lin, Y. B., & Du, D. Z. (2009). Wireless network security. In *Eurasip Journal on Wireless Communications and Networking* (Vol. 2009, Issue 1, pp. 1–3). SpringerOpen. <https://doi.org/10.1155/2009/532434>
- Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016a). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE*, 104(9), 1727–1765. <https://doi.org/10.1109/JPROC.2016.2558521>
- Zou, Y., Zhu, J., Wang, X., & Hanzo, L. (2016b). A Survey on Wireless Security: Technical Challenges, Recent Advances, and Future Trends. *Proceedings of the IEEE*, 104(9), 1727–1765. <https://doi.org/10.1109/JPROC.2016.2558521>

APPENDIX I: INTERVIEW SCHEDULE

The questions have been grouped according to the objective

1. To identify the security risks associated wireless campus networks in the selected universities in Kenya;
 - i. Have you performed a risk assessment to understand the value of the assets in the university that need protection?
 - ii. How often do you perform firmware upgrade on Aps and client NIC
 - iii. How often do you perform security assessment to understand the wireless security posture?
 - iv. Do you have an inventory of all wireless devices?
 - v. How do you dispose wireless devices no longer in use?
 - vi. How often do you review device logs
 - vii. How have you separated the wireless network from the wired infrastructure
 - viii. If you allow guest access, is it separate from the rest of the network?
 - ix. Do you use static or dynamic IP addressing

2. To assess the security measures in place for wireless campus networks in the selected universities in Kenya;

- i. Do you have a policy that addresses the use of wireless technology?
- ii. Do you have a Guest User Policy
- iii. How do you ensure wireless networks comply with the universities security policy
- iv. How often do you train your network users on computer security awareness and risks associated with wireless security?
- v. What measures do you have in place to physically secure your wireless devices?

- vi. At which areas/points in the buildings are your APs located?
- vii. Who can use the reset functions? and what do you do incase its is used
- viii. Which network monitoring tools do you use?
- ix. What authentication methods do you use for devices and wireless users and which encryption methods (if any) do you use along with the authentication methods
- x. Do you have firewalls and access lists configured on APs?
- xi. Have you installed antivirus software on wireless clients
- xii. Have you installed firewall on wireless clients
- xiii. How often do you change passwords for wireless devices
- xiv. Have you deployed intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity?

3. To determine the vulnerabilities of wireless campus networks in the selected universities in Kenya;

- i. Have you conducted a site survey to establish AP coverage for the university?
- ii. Have you tested AP range boundaries to determine the extent of wireless coverage?
- iii. How do you handle APs that are not used (e.g After Hours)
- iv. What SSID do you use for your APs?
- v. Do you broadcast the SSID for Aps
- vi. What version of SNMP do you use?

4. To propose measures and tools for ensuring improved security of wireless networks in the universities.

- i. What can you recommend to ensure improved security of campus wireless network?


APPENDIX II: OBSERVATION GUIDE

1. What are the wireless devices in use?
2. What are the locations of wireless network devices?
3. How physically are the wireless network devices secured?
4. How are the users interacting as the use wireless networks?
5. What documents are in place in relation to wireless devices?

APPENDIX III: NACOSTI CLEARENCE

| | |
|--|--|
|  <p>REPUBLIC OF KENYA</p> <p>Ref No: 092001</p> |  <p>NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION</p> <p>Date of Issue: 21/December/2021</p> |
| RESEARCH LICENSE | |
|  | |
| <p>This is to Certify that Mr. SAMSON OOKO of Moi University, has been licensed to conduct research in Kisumu, Nairobi, Nakuru, Nandi, Uasin-Gishu on the topic: Security of Wireless Campus Networks in Selected Universities in Kenya for the period ending : 21/December/2022.</p> | |
| License No: NACOSTI/P/21/14984 | |
| <p>492001</p> <p>Applicant Identification Number</p> | <p><i>Walter Ombui</i></p> <p>Director General</p> <p>NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY & INNOVATION</p> |
| Verification QR Code | |
|  | |
| <p>NOTE: This is a computer generated License. To verify the authenticity of this document, Scan the QR Code using QR scanner application.</p> | |

APPENDIX IV: SAMPLE STAKEHOLDER INPUT

 **Joan Masai** <jmasai@kenet.or.ke>
to me ▾

Wed, Aug 10, 2016, 5:00 PM ☆ ↶ ☰

Hello Samson,

I have shared my thoughts/comments and questions below.

At what point in the buildings are your APs located? * - You can rephrase this question to make it clear?

How do you handle APs that are not used (e.g After Hours) * - e.g. powering off the APs? Maybe you can provide choices?
What SSID do you use for your APs? * - why?

Do you broadcast the SSID for APs * - what does this mean?

Which management protocols have you enabled? * - Maybe - Which **network** monitoring tools do you use?

What authentication methods do you use for devices and **wireless** users * - Also ask about encryption methods (if any) that are used along with the authentication method

Also ask if firewalls and access lists configured on APs. This will ensure only authorised access to the APs

Also ask about Guest User Policy? Is there access for guests? Is the access separate from the rest of the **network**? Best practise is to ensure guests have NO access to the Institutional resources - only access to the Internet.

Have you enabled or disabled file sharing on **wireless** clients? * - Does this question imply that blocking file sharing on WLANs is a **security** measure?

Do you use static or dynamic IP addressing * - I am curious why ask this question :)

Kind regards,

Joan Masai
KENET

From: "Samson Ooko" <ookos@ueah.ac.ke>
To: "jmasai" <jmasai@kenet.or.ke>
Sent: Wednesday, 10 August, 2016 16:13:46