A MODEL BASED APPROACH FOR IMPLEMENTING AUTHENTICATION AND ACCESS CONTROL IN PUBLIC WLANS: A CASE OF UNIVERSITIES IN KENYA

BY
DAVID GITONGA MWATHI

A THESIS SUBMITTED IN FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF DOCTOR OF PHILOSOPHY DEGREE IN COMPUTER SCIENCE IN THE SCHOOL OF COMPUTING AND INFORMATICS, UNIVERSITY OF NAIROBI.

APRIL 2018

DECLARATION

I hereby declare that this thesis is my original work and has not been submitted in this or any other University for award of a degree. No part of this dissertation may be reproduced without the prior permission of the author or the University of Nairobi

Signature:...Date:...

Name: David Gitonga Mwathi

Registration No: ***P80/84661/2012***

This thesis has been submitted for examination with our approval as the Supervisors.

Signature:……………………………………..…Date………………………………

Name : Dr Elisha Opiyo T. Omulo, School of Computing and Informatics,
University of Nairobi, Kenya

Signature:…………………………………….…Date……………………………

Name: Professor William Okelo-Odongo, School of Computing and Informatics,
University of Nairobi, Kenya

DEDICATION

I dedicate this work to all ICT security practitioners and researchers who value secure WLAN environments.

ACKNOWLEDGEMENT

I have come to appreciate PhD studies as a long adventure in the forest with so many encounters that make it one of the most interesting adventures that a scholar undertakes. I give thanks to almighty God for making this adventure successful for me.

Thanks to the University of Nairobi administration for creating an enabling academic environment that made it possible for me to complete the adventure.

Special thanks to my two supervisors the late Prof William Okelo-Odongo and Dr Elisha Opiyo who tirelessly walked with me and directed me to safe routes through the entire adventure. Their academic prowess, critiques, advice, insights, encouragement and diligence helped shape the work to what it is currently. **Truly iron sharpens iron.**

Much gratitude goes to the faculty at School of Computing and Informatics. In particular, thanks to Dr Agnes Wausi for her wonderful leadership of the school. Prof. Wagacha for co-ordination of the PhD programs, Prof. Waema and Dr Wanjiku Ng'ang'a for enhancing my research knowledge and skills in the initial stages of admission for PhD studies. Your insights and encouragements fuelled the adventure. Regards to my employer and colleagues at Chuka University for creating a favourable working environment and providing encouragement that made my scholarly adventure smooth. To all friends, practitioners, researchers and all professionals who participated in making this research successful. I remain thankful.

Finally, I thank family members particularly my wife Angela Kinya for giving me the necessary support and remaining patient with me as I put many hours into this work. My Mum and Dad for your teachings on hard work and self-discipline in my formative years that have immensely contributed to this successful adventure. Truly, this is a confirmation of the biblical teaching that says "**Train up a child in the ways he should go and when he is old, he will not depart from it**" Proverbs 26:6. I passionately thank my two little children Rachael Makena and Adrian Mwathi for having endured a father who was many times unavailable.

ABSTRACT

Poor implementation of authentication and access control in large public WLANs such as those in universities is the main problem addressed in this research. Specific challenge include: lack of an appropriate model that enables design or selection of security features and their configuration leading to selection and configuration of vulnerable cipher suite, authentication and access control mechanisms, end-user and server system security features. The main focus of this study was development of a simulation model that facilitates implementation of WLAN authentication and access control security in a public WLAN.

The research process involved three phases: the first phase was preliminary studies which involved descriptive survey on selected university WLANs in Kenya as well as analysis of attack susceptibility of WLAN security features/configurations. The second phase involved design of model architectural components, component value function tables and model algorithms based on results of preliminary studies. The third phase involved prototyping the model design, model concept validation, computerized model verification and model operation validation.

The developed model was subjected to validation in order to give it enough confidence necessary for its results to be accepted.

Results from validation of the model concept using expert intuition show high expert confidence in the model while those from theoretical analysis show that the model obeys key operational laws. This indicates that the theories and assumptions underlying the model are correct and that the model's representation of the problem domain, its structure, logic and mathematical causal relationships are “reasonable' for the intended purpose of the model. Results from validation of model operation using parameter variability-sensibility analysis show high practitioner confidence in the accuracy, usefulness and applicability of the model. This indicates that the model behavior is valid for its intended purpose.

The main contribution of this work is generation of a simulation model that enables appropriate design or selection of security features and their configuration for WLAN authentication and access control in public WLANs. This contribution is major because no previous studies have been done with a view of developing a simulation model that can enable an implementer to visualize the security level expected from implementing a set of security features and their configurations. Another contribution is the application of attack tree modeling methodology combined with common vulnerability scoring system (CVSS) in analyzing severity of security vulnerabilities in a system. Lastly, implementation of an algorithm that enables one to predict security levels on WLAN authentication and access control implementation and the algorithm for selection of EAP method is an important technical contribution.

This research has demonstrated that deploying public WLANs because of their convenience and ease of deployment is not good enough. Given the potential loss that an organization can incur due to attacks, a good understanding of the important WLAN security components and relative security level provided by a combination of security features specific to the component is useful to enable implementers optimize WLAN security based on their resources and level of security required.

Keywords: Trusted computing base concept, attack tree methodology, common vulnerability scoring system, wireless authentication and access control security model.

DEFINITION OF TERMS

Attack Tree (Atree) Methodology: A methodology for describing security weaknesses of a system that uses a tree like representation of an attacker's goal recursively refined into conjunctive or disjunctive sub-goals.

Authentication: The process of verifying the claim that an entity is allowed to act on behalf of a given known identity.

Access control: Restricting the rights of an entity to access WLAN resource until authentication and establishment of confidentiality and integrity keys takes place.

Attack susceptibility: A measure of the level of severity of implementation vulnerabilities in a WLAN.

Implementation specific vulnerabilities: Specific systemic vulnerabilities within the way IEEE 802.11 or its supporting technologies have been designed or configured.

Public WLAN: A wireless local area network characterized by large population that dynamically changes and a large pool of uncontrolled, multi-vendor, multiplatform client devices.

Open WLAN: A WLAN that is deployed in public places and is set to broadcast its SSID such that any WLAN device in the range can detect it.

Closed WLAN: A WLAN which does not respond to clients with "Any" SSID assigned, nor does it broadcast the SSID to the clients at large.

Operational Security: Security for systems in real environments e.g WLAN infrastructure of a university.

Attacker Capability: refers to availability, to the attacker, of resources such as attack tools, knowledge, experience and funding necessary for launching WLAN attacks.

Trusted computing base: Small amount of software and hardware components that security depends on and that we distinguish from a much larger amount that can misbehave without affecting security.

Attack: Execution of a set of actions (plan) that lead to compromises in security objective(s).

Cipher Suite: Cryptographic algorithms used to encrypt messages as well as perform integrity check for possible modification of messages between a wireless client device and accesspoint.

LIST OF ABBREVIATIONS

CVSS	Common vulnerability scoring system
RFC	Request for comments
IEEE	Institute of electrical and electronic Engineers
IETF	Internet Engineering task force
MAC	Media access control
TCP/IP	Transmission control protocol/Internet protocol
EAP	Extensible authentication protocol
WLAN	Wireless local area network
CCMP	Counter mode with cipher block chaining message authentication code
TKIP	Temporal key integrity protocol
WAACS	**Wireless** authentication and access control Security

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER I: INTRODUCTION

1.1 Background of the Study

A Wireless Local Area Networks (WLAN) is a communication network that relies on radio frequencies for data transmission. Devices participating in this local area network broadcast data frames over a radio frequency interface. Any WLAN enabled device in the range will receive the data frames. Such networks are already available in coffee shops, hotels, fast food restaurants and many other public places such as universities, airports and urban areas (Dokurer, 2006; Wei-Lin & Quincy, 2010). WLANs are popular because they provide all services that a wired local area network can with added advantage of client device mobility while avoiding costs associated with cabling within the WLAN coverage area. Developments in the use of portable devices such as laptops and tablets have also made wireless WLANs popular.

When deployed in public places, WLANs provide greater flexibility and convenience for users when accessing the institutional network and network services. WLANs therefore enable organizations to expand their computer networks at a low cost. Unfortunately, these performance gains come with risks (Rakesh & Ankur, 2008).

According to (Rakesh & Ankur, 2008), WLANs are susceptible to certain inherent security threats when deployed in public places:

- The access point broadcasts its service set identifier (SSID), signal level, MAC address, security features and location to devices within its signal coverage. This allows client devices deployed by attackers within the range to detect it and possibly connect to the institutional network.
- Since there is no wiring to define membership to the WLAN, readily available WLAN sniffer tools can be deployed by attackers to capture data frames sent over the air. The captured data is then imported into encryption crackers for decryption. In situations where the captured frames are unencrypted, one can directly extract sensitive security data such as email and website passwords since they will be in clear-text.
- WLAN spoofing where rogue WLANs masquerade as real access points, establish connections and intercept or inject data into the real WLAN.

According to (Daniel & Edward, 2010), any data communication via wireless channels requires implementation of security standards and mechanisms that protect the confidentiality, integrity and availability of communicated data.

WLANs implement IEEE 802.11i standard whose focus is provision of appropriate integrity and confidentiality levels. This is achieved by implementing WLAN users' access control and encrypting all the data exchanged in the WLAN. However, (Daniel & Edward, 2010) argue that these standards when poorly implemented, fail to achieve appropriate levels of confidentiality and integrity consequently subjecting the WLAN to unwanted access by hackers/intruders. Once inside, the hackers make all information susceptible to sniffing and manipulation by exploiting the vulnerabilities in the implementation of the standard (Daniel & Edward, 2010).

Controlling user access and potential WLAN security attacks in public WLANs such as those in universities can be achieved through a secure authentication and access control approach because it is during this process that all security parameters are negotiated.

According to (Li-Chuan, Cheng, Shao-Wen & You-hua, 2009), the key technology of trusted network is authentication. Recent studies however indicate that many implementations of authentication and access control in public WLANs are easy to compromise (Alikira, 2012; Mwathi et al, 2016).According to (Alikira, 2012), an enterprise wide WLAN implementation in Kampala international university experienced a total denial of service. Alikira (2012) explains that this happened not because there were no security measures taken but the security measures that had been configured were weak and easy to compromise.

A survey carried out by (Mwathi et al, 2016) to investigate IEEE 802.11 implementation specific vulnerabilities that may contribute to poor WLAN authentication and access control security performance in WLANs in Kenyan universities revealed that many university WLANs have implemented confidentiality and integrity protocols and authentication and access control mechanisms that have well known vulnerabilities. It also established that most WLANs were not configured to support enhancements to IEEE 802.11 such as IEEE 802.11w (i.e management frame protection). These networks are therefore prone to many attacks that exploit lack of protection of management frames.

The survey also established that many users configure their end devices to ignore validation of authentication server certificate and the specific authentication server address (name) verification is also ignored. Additionally many of the devices are configured in such a way that users can choose for themselves the server that issues the certificate making the whole process prone to compromise.

Further the survey established vulnerable choices and configuration of authentication credentials and implementation of weak authentication servers. It was observed that all the universities sampled have implemented centralized user database for user names and passwords. In some cases, some universities have implemented MAC address filtering which make them vulnerable to denial of service attacks, replay attacks and impersonation attacks. This research tackles the challenges presented in the foregoing section with a focus on large public WLANs such as those in universities.

1.2 Problem Statement

Poor implementation of authentication and access control in large public WLANs such as those in universities is the main problem addressed in this research.

The problem has two sub-components which include:

- Lack of an appropriate model that enables design or selection of security features and their configuration for WLAN authentication and access control in a public WLAN.
- Selection and configuration of vulnerable cipher suite, authentication and access control mechanisms, end-user and server system security features.

The flexible nature of the provisions of IEEE 802.11 standards and supporting technologies create potential for selection of vulnerable cipher suite, authentication & access control, end-user and server system security features. Attempts to enhance security requirements provided by IEEE 802.11 standard have been made (IEEE 802.11i, 2004 & IEEE 802.11w, 2009). However, the standards provide a variety of options for various security features. This makes selection and configuration of the appropriate security features a challenge to many WLAN security implementers (Khidir & Ali, 2011). This issue is a major concern because several software attack tools targeting vulnerabilities in authentication methods, cipher suites and supporting technologies on client devices and server implementations continue to proliferate, effectively empowering attackers.

1.3 Objectives of the Study

The main objective of this research was to develop and prototype a model that facilitates implementation of WLAN authentication and access control security in the context of large public WLANs such as universities. The specific objectives of the study were to:

(i) Investigate IEEE 802.11 implementation specific vulnerabilities that may contribute to poor WLAN authentication and access control security performance of WLANs in Kenyan universities.

(ii) Analyze security offered by WLAN cipher suites, authentication and access control mechanisms, end user and server system software used in WLAN authentication and access control.

(iii) Establish relevant architectural components and use them to develop and prototype a simulation model that enables appropriate design or selection of security features and their configuration for WLAN authentication and access control in public WLANs.

(iv) Validate the model for its intended purpose over the domain of its intended applicability.

1.4 Research Questions

This study was driven by the following research questions:

(i) What are the implementation specific vulnerabilities that may contribute to poor WLAN authentication and access control security performance in selected university WLANs in Kenya?

(ii) What is the attack susceptibility of the vulnerabilities exploited by known attacks on WLAN cipher suite, authentication and access control mechanisms, end-user and server system software that implement authentication and access control in a WLAN?

(iii) What are the relevant architectural components of consideration for developing a simulation model for selection or design as well as configuration of security features for public WLAN authentication and access control?

(iv) Is the developed model valid for its intended purpose over the domain of its intended applicability?

1.5 Significance of the Study

The outcome of this research should be beneficial to several categories of entities. Specifically, the outcomes will:

(i) Shed new light to practitioners implementing security on public WLANs on security threats posed by WLAN networks and how best to manoeuver them.

(ii) Shed new light to researchers on the development of secure WLAN implementation models

(iii) Help both experienced and inexperienced network administrators configure secure public WLANs.

(iv) Be used to boost the concerted response to the expanding network security challenges facing networks of public institutions consequently raising awareness within governments of their risks to enhance financing of network security initiatives.

(v) Provide a WLAN security measurement tool (research tool) for researchers interested in WLAN security

(vi) Act as an impetus and catalyst for further research about WLAN security.

1.6 Thesis Overview

The remaining sections of this thesis are structured as indicated:

Chapter 2 which follows next is a synthesis of the background to the problem of poor security in WLAN authentication and access control implementations. It explores and analyses attacks to WLAN security, vulnerabilities exploited and attack tools employed to realize the attacks. It also explores and analyses WLAN IEEE 802.11 security standards and protocols. The chapter delves into related works that focus on developing approaches that address poor implementation of authentication and access control security. Further a review of theories, concepts and research relevant to the analysis, design, implementation and evaluation of simulation models is made. The chapter ends with identification of gaps in knowledge and shortcomings of previous approaches/methods that need to be addressed by the proposed solution and finally conceptual architecture is presented and discussed.

Chapter 3 provides the details of various research strategies and specific research actions geared towards the design of a model that enables design or selection and configuration of security features for WLAN authentication and access control in a public WLAN. A comprehensive analysis of resources selected, methods, tools and techniques for data gathering, analysis, model development process and validation is provided.

Chapter 4 presents findings of discovery of security features and configurations related to architectural components, analysis of attack susceptibility of security features & configurations, model design description, model validation, discussion of the results and research contribution.

Chapter 5 presents a summary of the research carried out. In particular it revisits the focus of the problem, main objectives, approaches followed and the main results, contributions, achievements, study limitations, recommendations for furtherance of this work and research, policy recommendation and conclusions.

CHAPTER 2: LITERATURE REVIEW

This chapter focuses on literature that has been reviewed from previous studies on wireless networks, WLAN attacks and tools, WLAN security standards, protocols and implementation architectures, research related to WLAN implementation, theories and concepts related to model development and validation. The review also identifies gaps and finally presents a conceptual framework for the research. According to Ellis & Levy (2008), any scholarly inquiry begins when a clear literature supported problem has been identified. Therefore, the existing body of knowledge is a key pillar upon which a research inquiry is built (Ellis & Levy, 2006). The goal of this literature review is to synthesize and integrate theories, methods, outcomes, practices or applications of published research work relevant for this study.

2.1 General Principles of WLAN Operation

Wireless Local Area Network (WLAN) technologies, specifications and standards are defined in IEEE 802.11(1997) and later amendments. IEEE 802.11, also referred to as WIFI, is one of IEEE 802 family of protocols that provide specifications for Local Area Network technologies. According to IEEE 802.11(1997) and subsequent amendments, each device in a WLAN infrastructure is designed to operate in one of four possible modes; master, managed, ad hoc or monitor mode.

When operating in master mode, the device is an access point operating on a specific channel frequency and configured with a unique service set identifier (SSID). When in managed mode, the device is a client and can join any WLAN created by an access point. When it joins a WLAN, it must tune its frequency channel to that of the master (access point). When in ad hoc mode, the device creates peer to peer connections with other devices creating a multipoint to multipoint network. When in monitor mode, the device does not transmit any data but passively listens to all radio frequency traffic on a given channel (Sheila, Bernard, Les & Karen, 2007).

The general mechanism used by WLAN is to allow client devices e.g laptops and workstations to establish a connection with the WLAN through a wireless access point. The client device will periodically scan the environment looking for an access point. The device will use either active scanning or passive scanning approach. If the device is using active scanning, it will transmit a probe frame on all available frequency channels. When an access point operating within the client's range receives the probe frame, it returns a probe response. The probe response contains information such as SSID, security parameters supported by the access point, transmission rate, channel frequency which the client device needs to associate itself with the access point. Communication will only be established if the client device will agree to join/associate with the access point (Sheila et al, 2007).

On the other hand if the client device is using passive scanning, it listens on all available channels, for a beacon frame from a nearby access point. The beacon frame contains information similar to that of the probe response. Once a client device detects a beacon frame, it may choose to associate itself with the access point that transmitted the beacon frame (Sheila 2007).

The type of information required to associate a client device with an access point includes the Service Set Identifier (SSID) and the wireless network's transmission rate. Every device on a wireless network must share the same SSID and transmission rate (Dean, 2006).WLANs may operate as either ad hoc network or infrastructure network. Ad-hoc network does not use any access points and client devices communicate directly with each other via their wireless cards (Dean, 2006).Infrastructure network on the other hand must use access points. Figure 2.1 shows an ad hoc network, while figure 2.2 shows infrastructure network.

.

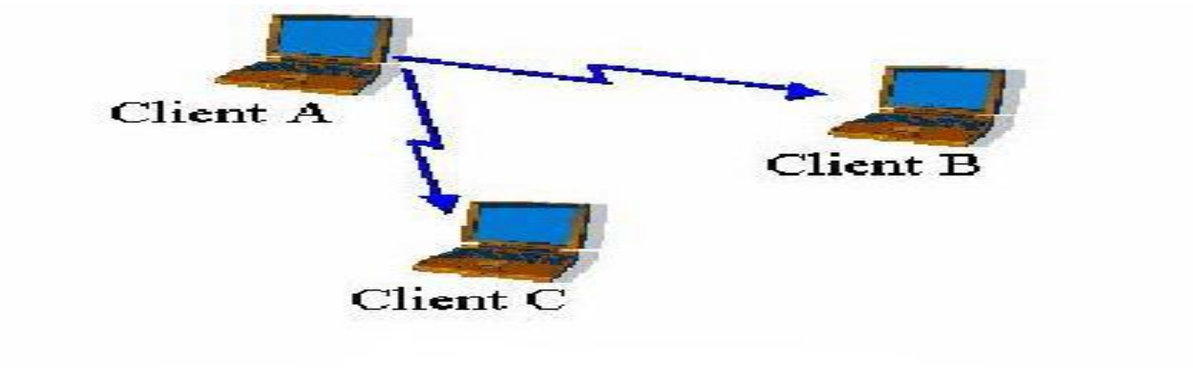


Figure 2.1: Ad hoc Network (Dean, 2006)

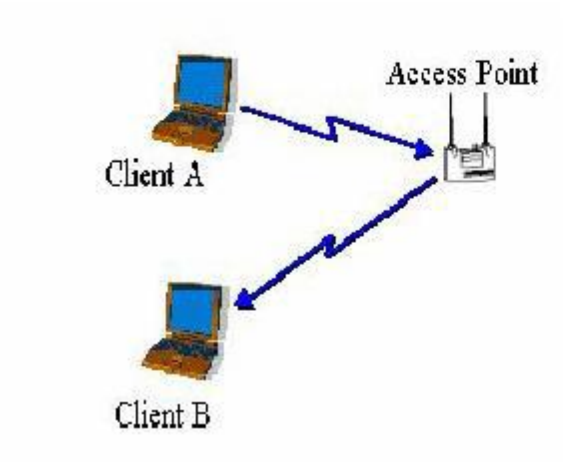


Figure 2.2: Infrastructure network(Dean,2006)

Two or more infrastructure networks may be joined by a backbone link to form extended service set (ESS) within which individual client stations can roam. Figure 2.3 shows such a network.

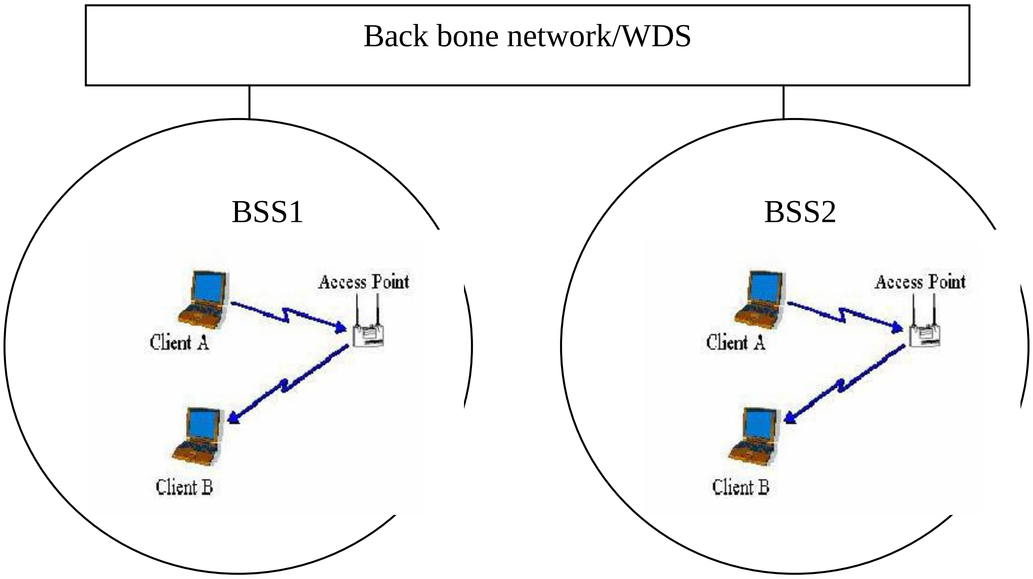


Figure 2.3: Extended service Set (Dean,2006)

A public WLAN, which is our focus, would be set up to use the infrastructure or extended service set mode. Infrastructure and extended service set mode allows central management and a dynamic host configuration protocol (DHCP) server is usually included as part of this architecture. The DHCP server provides IP addresses and other required information to allow wireless network client devices to communicate on both the WLAN and the attached wired network without any additional support from network administrators which brings about possibility of enhanced security (Maiwald, 2003).

2.2 WLAN Security Objectives, Attacks and Vulnerabilities

WLAN security features should be able to achieve well known literature supported objectives: confidentiality, integrity, availability, access control and authentication (Sheila et al, 2007). Confidentiality ensure that all pre-authentication and post-authentication data frames are not read by unauthorized entities while integrity ensure no modifications are made on the data frames by unauthorized entities. Availability ensures that whenever legitimate client devices or individual users need to access a WLAN resource, they are able to do so without interruption. Access control restricts the rights of client devices or individual users to access a WLAN resource until they are duly authenticated. Authentication is the process of proving that a device or individual is what it claims it is (Sheila et al, 2007).

Unlike a wired local area network where an attacker must either gain physical access to the LAN or compromise network hosts remotely, a WLAN attacker only needs to be within range of the access point coverage. For a client station or user to connect to a WLAN, it is necessary that its access rights are controlled until proper and secure authentication takes place (Sheila et al, 2007). During authentication process, integrity and confidentiality of authentication traffic must be guaranteed to ensure secure authentication has taken place. Pfleeger (1997) identified interruption, interception, modification and fabrication as the main threats that threaten confidentiality, integrity and availability on network systems.

Research has revealed a number of attacks on the WLANs. These attacks exploit weaknesses in authentication mechanism in place, IEEE 802.11 confidentiality and integrity mechanisms used to protect authentication information, supporting technologies and user(technical and non-technical) misconfigurations. The attacks generally compromise availability of a WLAN, confidentiality and/or integrity of the authentication and access control traffic.

2.2.1 Denial of Service Attacks (Availability)

These are attacks that make the services of WLAN unavailable to legitimate users. They include; disassociate flooding, De-Authentication, Authentication / Association Flooding, Extensible Authentication Protocol (EAP) Attacks, TKIP Countermeasure and WPA Hole 196 Denial of service (John, Ann & Robert, 2002; Scott, 2011; Airtight networks, 2010).

(i) Disassociate attack involves a rogue station replaying a previously captured DISASSOCIATE message. Figure 2.4 illustrates the attack setup. The objective of the attacker is to cause denial of service to a legitimate client device by forcing it to disassociate from an access point in order to stop flow of data frames to and from the client (John et al, 2002). This attack works where client station's management frames lacks integrity protection mechanism making it difficult to prove frame authenticity.

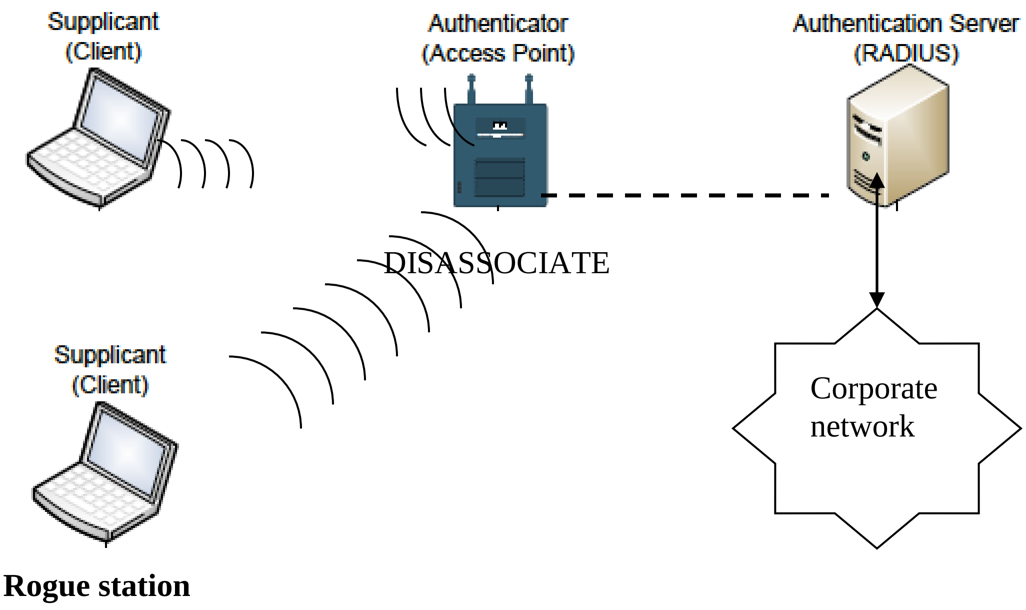


Figure 2.4: Disassociate attack(John et al, 2002).

(ii) De-authentication attack involves an access point sending de-authentication frames to client devices connected to an access point. The attacker can target a single client device or access point (Scott, 2011). In a single client device attack, a rogue access point sends a DE-AUTHENTICATION frame to a client station forcing it to de-authenticate from the access point immediately (Scott, 2011). This leads to denial of service to the de-authenticated client device. The attacker can also configure a rogue client device with the MAC address of the de-authenticated client device and attempt to access a WLAN. In an access point attack (also called mass de-authentication), a rogue access point spoofs MAC address of a legitimate access point and then broadcasts de-authentication frames to the connected MAC addresses. This will disconnect all client stations validly connected on a certain access point (Scott, 2011). Lack of mutual authentication between the client device and access point creates a loophole that gives room for rogue access points to be set up. Where DE-AUTHENTICATE frames are not protected, DE-AUTHENTICATE frames are spoofed for later replay.

(iii) Authentication/Association flooding attack mimicks existence of many client devices attempting to authenticate or associate to an access point at the same time**.** Figure 2.5 illustrates the setup. This is achieved by the attacker setting up an attacking device that sends authentication or association messages in rapid succession and each time using a different MAC address. When this happens, the access point's memory and processing ability is overwhelmed by the large number of authentication or association frames that exhaust its memory and processing ability. Effectively, legitimate clients are denied access (Scott, 2011).

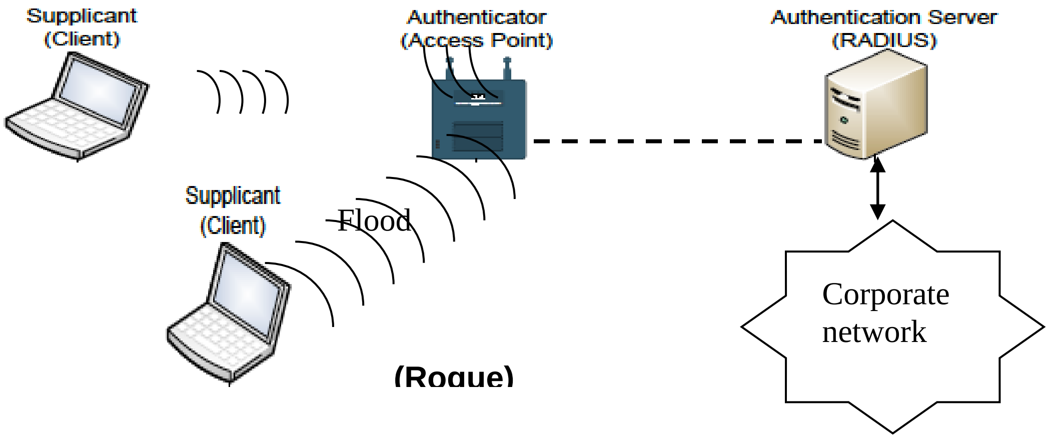


Figure 2.5: Authentication / Association Flooding(Scott, 2011).

(iv) Extensible Authentication Protocol (EAP) flooding attacks work by deploying a single or multiple rogue devices to flood a WLAN with EAP authentication requests. The large volume of the traffic effectively overwhelms the RADIUS server causing a denial of service (DoS) on legitimate client devices wanting to connect to the WLAN resource. The attacker may configure an attacking tool to send EAP authentication requests through the entire EAP identifier space which can crash the access point. The access point can also be crashed by flooding them with EAP over LAN (EAPOL)-Start frames (Scott, 2011).

(v) Temporal Key Integrity Protocol(TKIP) Countermeasure attacks exploit temporal message integrity check (MIC) mechanism on TKIP where the protocol ceases all activity for one minute and then renegotiates both group and pairwise keys following receipt of two invalid MIC frames within a minute (IEEE 802.11i, 2004). Attackers deny service to the access point by sending several invalid MIC frames. This attack will always work in a network that uses only TKIP for encryption or that which uses a combination of both TKIP and CCMP even when the most secure 802.1x authentication and access control mechanism is employed (Scott, 2011). This is because existence of any TKIP client device on a WLAN will force the access point to use the TKIP group key even on CCMP client devices.

(vi) WIFI protected access (WPA) hole 196 Denial of service attack exploits group transient key where an attacking device broadcasts/multicasts spoofed data frames with a high packet number. When this happens, victim client devices in the WLAN ignore legitimate frames with packet numbers that are lower than the number sent by the malicious device (Airtight networks, 2010). For this attack to occur, the attacker must have been properly authenticated into the WLAN. However, an attacker can circumvent authentication by implementing virtual soft access point (Airtight Networks, 2010).

2.2.2 Confidentiality Attacks

This comprises of attacks that lead to the attacker capturing confidential information from two parties as they communicate. These attacks can be achieved in two ways: the attacker can be man in the middle (attacker being on the communication path of users on the WLAN) or the attacker can crack the cipher suite’s confidentiality protocol mechanism.

(a)Man in the Middle Attacks

This comprises of attacks that rely on an attacker being on the path of users communicating on WLAN. The attacker captures confidential information from both parties as they communicate. These attacks include: Resource stealing, MAC spoofing, Captive Portal- Evil Twin, Traffic redirection and RADIUS certificates attacks.

(i) MAC Address Spoofing Attack is illustrated in figure 2.6. It works by setting up a rogue access point which sniffs the MAC address and then the network interface card of an attacking client device's is configured with the sniffed MAC address. The attacking client device waits until the client device whose MAC address was sniffed disassociates from the WLAN access point. The attacking client device then attempts to associate to the access point and if successful will have gained access to the network illegitimately. The attacker can then intercept traffic for offline analysis or use the WLAN to gain access to the internet, just like a legitimate WLAN client would (John et al, 2002).

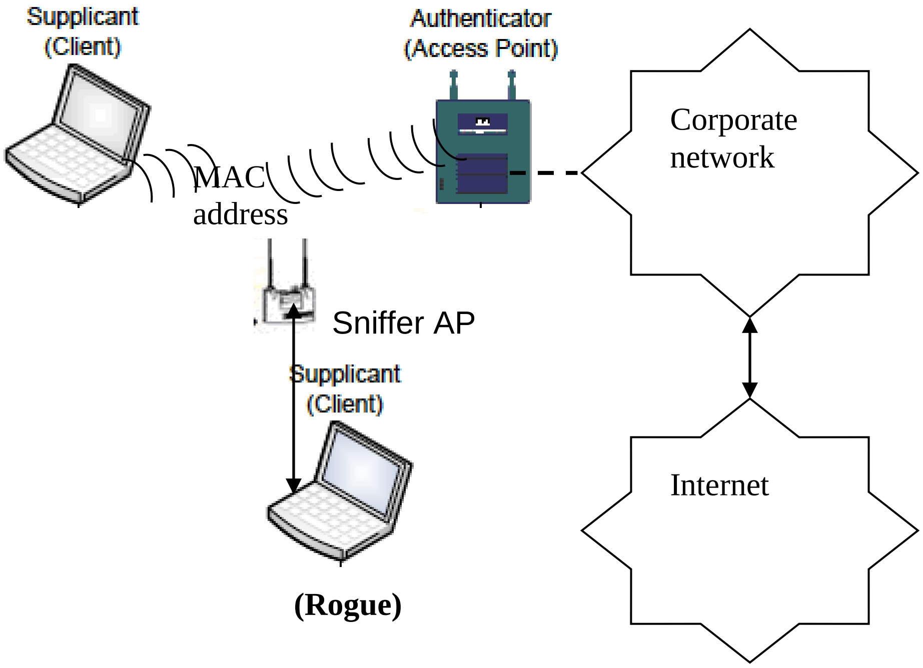


Figure 2.6: MAC Spoofing (John et al, 2002).

The attack can be implemented using a device that is configured to act as both access point and client device. Such device will have two wireless cards, one acting as a valid client device to the WLAN while the other card spoofs SSID to act as an access point to other client stations (John et al, 2002). Some of the vulnerabilities exploited by this attack include; lack of management frame protection, lack of mutual authentication between access point and client station and client station-access point secret being rarely changed in pre-shared secret implementations (John et al, 2002).

(ii) Captive Portal Circumvention/Evil Twin attack work by an attacker setting up a parallel authentication server with an identical login page to the real one, and uses it to harvest/capture credentials as legitimate users attempt to login (Scott, 2011). The attack setup is illustrated in figure 2.7.

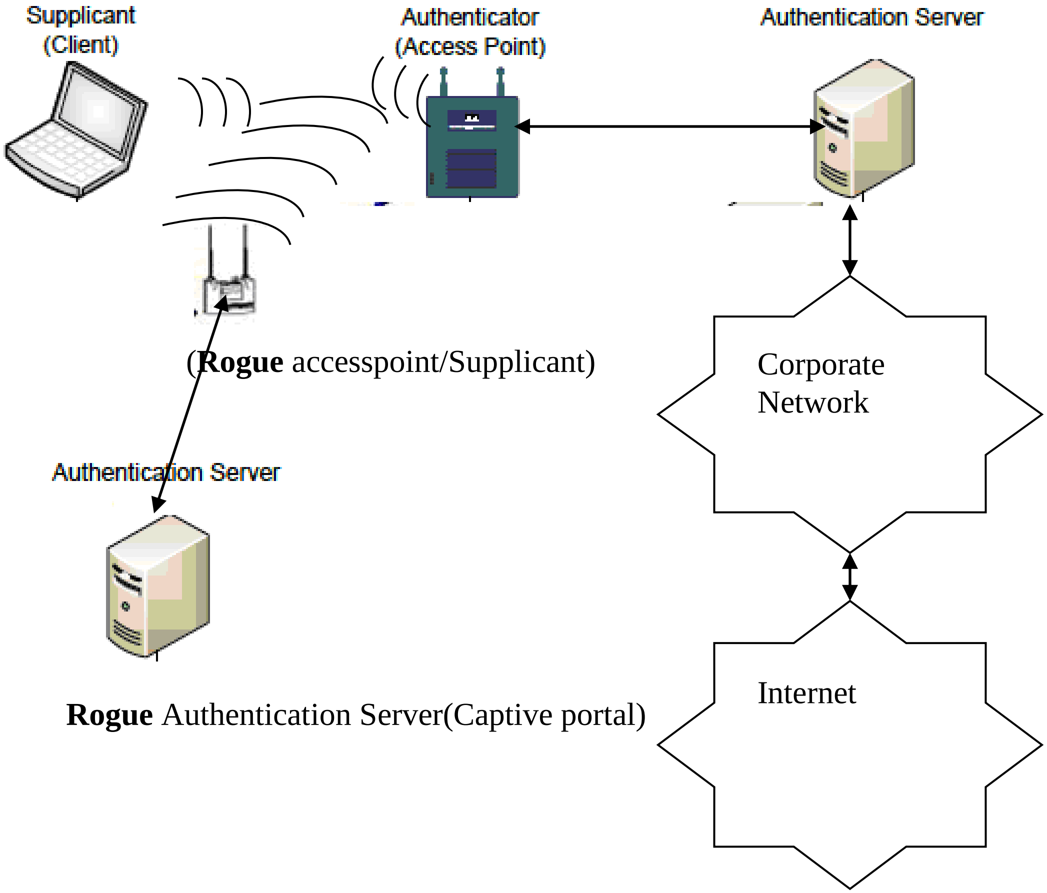


Figure 2.7: Captive Portal Evil Twin(Scott, 2011).

According to AirDefense (2006), the implementation of this attack will usually have an attacking access point spoofing a valid Service Set Identifier (SSID) that hotspot users connect to. The access point will broadcast its SSID to fool unsuspecting users into connecting to it. Once connected the, user is re-directed to the parallel captive portal server (authentication server) containing a login page created to look authentic. As the hotspot user enters password or creates new identity information, it is captured and logged. If the hotspot user is legitimate, then the attacker would have a valid user name and password to connect to the WLAN and once connected can steal critical information, and/or use the institutional network to launch a downstream attack (AirDefense, 2006). Vulnerabilities exploited by this attack include: lack of mutual authentication between the user and captive portal server and lack of validation of the certificate provided by the authentication server.

(iii)Traffic Redirection /ARP Poisoning attack works by an attacking device interfering with a switch's address resolution protocol (ARP) tables through the access point such that data frames headed to various destinations are re-directed to the attacking device. The attacking device can then capture these frames for later analysis or can use them to execute man-in-the middle related attacks. This attack can compromise even devices on the wired network. Another possible approach to implement this attack is via WPA hole 196 ARP spoofing where an authenticated device masquerades as an access point and uses the group transient key (GTK) to broadcast or multicast data frames directly to other wireless clients on the WLAN. The victim client devices in the WLAN will recognize the rogue access point as the default router and will channel all traffic through it creating a man-in-the-middle attack (Airtight networks, 2010).

(iv) RADIUS certificates attacks work by exploiting vulnerabilities associated with use of digital certificates by client devices to verify the RADIUS server. Many client devices are configured not to reject certificates provided by the RADIUS server (Mwathi et al, 2016). Such client devices may therefore accept digital certificates that may have been signed by the incorrect certificate authority may have the wrong common name or may even be self-signed. Therefore, a rogue RADIUS server can provide such digital certificate to a client device which will automatically accept it allowing the two to connect. Once authenticated and connected, the RADIUS server will intercept credentials. This attack is an easy to implement because many WPA/WPA2 Enterprise network using 802.1x clients are incorrectly configured (Mwathi et al, 2016).

(b) Cipher Attacks

These are attacks that target the cryptographic algorithms (cipher suite) used during authentication. The attacks lead to decrypting encrypted packets or recovering the key. Scott (2011) identifies some of these attacks as: WEP, WPA-PSK Dictionary, WPA/TKIP and LEAP Attacks.

(i) WEP Attacks

Borisov et al (2001) was the first researcher to seriously publish WEP insecurity. His works were later supported by Gast (2005) who argued that, it was trivial to crack WEP key. Pyshkin et al (2007) published new WEP attacks referred to as PTW attacks. These attacks are easy to execute because tools to perform them e.g KoreK and PTW attacks have already been developed (Aircrack-ng, 2010).Other Methods for breaking WEP include: FMS and Korek which exploits the ability to predict the first few bytes of a WEP frame and ChopChop which has ability to decrypt WEP data frames even without the knowledge of the key (Poorinma, Gowri & Abinaya, 2015).Despite its weaknesses, WEP remains widely deployed in organizations e.g. universities to make it easy for students to connect to university's hot spots (Alikira, 2012; Mwathi, et al, 2016).

(ii) WPA-PSK Dictionary attack exploits weaknesses in the selection of pre-shared key. When configuring WPA/WPA2 security, implementers have been known to often choose short, dictionary based pre-shared keys leaving them susceptible to this attack (Mwathi, et al, 2016). An attacker can implement this attack by intercepting frames before the four-way handshake phase immediately a client device joins a WLAN. The attacker, using offline dictionary attack techniques can then obtain the pre-shared key (Poorinma et al, 2015). If the key is weak, WPA2 can also be broken by capturing handshake messages Snonce, Anonce and some additional information.

(iii) WPA/TKIP Decryption attack is based on attacker knowledge of most of the bytes of the IPv4 address range in use on the WLAN. Its operation mechanism is similar to that of WEP and involves decrypting WPA/TKIP frames without knowledge of the key (Sheila et al, 2007).

(iv) Light Weight EAP (LEAP) Dictionary Attack targets WLANs implementing LEAP as an authentication mechanism because this EAP authentication method has weak credentials (Scott, 2011). This enables captured packets to be analyzed offline to obtain the user’s credentials.

2.2.3 Integrity Attacks

Data integrity ensures that no alteration of transmitted data takes place between the source and the destination. Integrity attacks therefore interfere with transmitted data so that what arrives at the destination is not what was sent from the source. Integrity attacks in a WLAN take the form of man in the middle. They include: Tunneled MITM attack, rogue access point attack and ARP Poisoning (Sheila, 2007).

2.2.4 Analysis of Vulnerabilities Exploited to Attack a WLAN

Attacks associated with WLANs compromise confidentiality, integrity and denial of service security objectives. Confidentiality and integrity attacks exploit vulnerabilities on a WLAN such as: authentication mechanism that does not support secure mutual authentications, client utility and access point firmware configurations that lack protection for management frames during authentication, access point secret being rarely changed in pre-shared implementations, client utility’s configuration to ignore validation of the digital certificate from captive portal authentication server, use of Virtual Wi-Fi soft access points, incorrect client utility configuration e.g. allowing self-signed certificates.

Inability of the client utility to correctly validate server certificates lead to attacks such as resource stealing, captive Portal evil twin and RADIUS certificate attacks. Other vulnerabilities include; configuring a weak passphrase in pre-shared WPA implementations which is exploited to cause WPA-PSK dictionary attack of the WPA key. WPA2 can also be broken by capturing handshake packets and with knowledge of IPV4 address range of WLAN if the passphrase is weak. Use of LEAP as upper layer authentication mechanism can also be exploited to cause LEAP attacks.

Various cipher suites have vulnerabilities that are exploited to cause confidentiality attacks e.g. wired equivalent privacy (WEP) is a soft target for many attacks which either decrypt WEP protected data frames or recover the WEP key.

Denial of service attacks which include: disassociate, deauthentication, authentication flooding, EAP flooding and TKIP countermeasure attacks and WPA 196 mainly exploit lack of support for protection of management frames to cause disassociate flooding and deauthentication attacks on a WLAN. Management frame protection is provided in IEEE 802.11w but has not been widely implemented in network interface card drivers, client utility (operating systems) and access point firmware. Additionally its implementation is optional. Therefore the configurations on the client driver, access point firmware and client utility software are crucial determinants of the ability to exploit denial of service WLAN attacks.

Driver fingerprinting attacks are as a result of vulnerabilities in the way various WLAN drivers operate. Inability of IEEE 802.11i to provide a mechanism for choosing an EAP method and cipher suite blending leads to choice of weak EAP methods and cipher suite combinations which can be exploited to cause EAP authentication flooding and TKIP countermeasure attacks. Operating systems support for features such as virtual WLANs creates a vulnerability that can be exploited to make it easy for WPA 196 denial of service attack to be realized. The location of the user database plays an important role in determining how easy it is to exploit attacks. When the user database is integrated into the access point or on a centralized database, it becomes trivial to launch denial of service attack such as EAP flooding attacks.

In general attacks on a WLAN target the following features: cipher suite, authentication mechanism, client utility, access point utility, client driver, authentication server, authentication credentials and user database. Whereas researchers have been able to reveal the attacks to WLAN together with their vulnerabilities, the information available is not sufficient enough to enable implementers make appropriate decisions related to selection of security features in a WLAN, for example, no researcher has made attempts to assess the severity of the attacks in relation to security objectives.

2.3 WLAN Attack Tools

This consists of software tools that are used to exploit various vulnerabilities on a WLAN in order to realize attacks.

2.3.1 Confidentiality Attack Tools

Confidentiality attack tools can mainly be categorized into four based on the functions they perform; WLAN detectors, sniffers, crackers and vulnerability detectors. Wireless network detectors are tools used to capture details of nearby access points such as signal level, type of security configured, SSID and MAC address. Some of these tools place the access points on a Google Earth map and even produces graphs that show signals by channel, usage rating and history (Michael, 2007). WIFI detectors also called WIFI stumblers can also reveal access points set with a hidden SSID. Although these tools may not be necessarily attack tools, they can detect access points set with weak security e.g. WEP which is then cracked. They can also be used to find the wireless access point information and then use it for setting up 'evil twin' access points near these legitimate ones. However, these tools can also be used to detect rogue access points and fix them. Common WIFI detectors/stumblers include android based WIFI analyzer, windows based open source Vistumbler , KNSGEM, APhunter, Hotspotter and APsniff(Michael, 2007).

WLAN sniffer tools on the other hand capture data frames sent over the air which is then imported into encryption crackers for decryption. In situations where the captured frames are unencrypted, one can directly extract sensitive security data such as email and website passwords because they will be in clear-text. A popular example of a sniffing tool is wireshark which is a multi-platform, multi-protocol analyzer with ability to sniff many popular WLAN security protocols including Wi-Fi Protected Access, Secure Sockets Layer(SSL), Wired equivalent privacy, IPsec, Internet Security Association and Key Management Protocol and Kerberos(Anh and Shorey, 2005). Wireshark is sufficient when frames are sent in plain text but requires encryption key cracker when frames are sent in ciphertext (Anh & Shorey, 2005). Ettercap is another multiplatform, multiprotocol sniffer with ability to sniff live connections and content filtering, network as well as host analysis. It can however be used in auditing and penetration testing (Michael, 2007).

Crackers are tools that monitor and capture encrypted wireless traffic and after collecting sufficient data frames, they compute the encryption key. These tools also crack encrypted passwords using dictionary, brute-force and cryptanalysis, decode scrambled passwords, uncover cached passwords and password hashes. Some common crackers include airsnort WEP cracker, Cain & Abel, Cloud, commercial online Linux based reaver for

WPA/WAP2 PSKs, aircrack-ng WEP and WPA-PSK keys cracker which implements FMS, PTW and Korek attacks(Anh & Shorey, 2005).These tools can however be used positively for auditing WLANs.

FreeRadius-WPE is an enhancement to the open source Free RADIUS server whose design objective is to perform man-in-the-middle attacks for WLANs implementing IEEE 802.1x authentication. A server configured with Free RADIUS-WPE accepts all client devices configured for whichever EAP method and logs their usernames and challenges/responses from them. The logged challenge/response will then be entered into a cracker tool called Asleap to crack the encrypted password. Therefore a rogue WLAN that uses FreeRADIUS –WPE can be set-up by attackers targeting unsuspecting WLAN users to harvest their credentials.

Vulnerability detectors are used to identify vulnerable WLAN components. WiFish Finder is a Linux based open source vulnerability detector that passively captures WLAN traffic and then produces a list of names and security settings of WLANs/access points that client devices probe for. It then actively probes the WLAN to identify WLAN client devices vulnerable to man in the middle attacks such as evil twin access points (Michael, 2007). This process enables it to identify client devices probing for unencrypted networks or those client devices probing for a WPA/WPA2 protected enterprise WLAN that are susceptible to man-in-the-middle attacks.

Jasager is firmware based on Linux with ability to identify vulnerable client devices. On the other hand, the tool can be used to execute evil twin or honey pot attacks by creating a soft access point with SSIDs that nearby client devices commonly probe for. The attacker could then run common network services such as DHCP, DNS, and HTTP. Requests to HTTP server could then be redirected to a web site which captures and displays any unencrypted passwords or other login information from the victims (Michael, 2007).

Windows based WiFiDEnum is a tool that captures details of device drivers implemented on the client network interfaces together with potential vulnerabilities. The objective is to identify WLAN drivers that are susceptible to driver exploit attacks (Laurent & Julien, 2007). Tools such as Kismet act as wireless network detector, sniffers and intrusion detection system. Linux based HermesAP and OpenAP can be used to setup rogue access points. Also Open source OpenWRT and HyperWRT tools that are used to replace the factory firmware for Linksys's WRT line of access points can be used by attackers to create rogue access points (Michael, 2007).

2.3.2 Data Integrity Attack Tools

Two main approaches employed by data integrity attack tools to execute integrity attacks are frame injection and frame replay. Both approaches manipulate data frames so that the receiver only receives what the attacker chooses. Simple-replay is a data integrity attack tool that injects into the WLAN previously captured 802.11 frames(Michael, 2007) While Ettercap and dsniff tools are mainly sniffers, they have ability to modify data transmitted between client devices and access point (Jiang & Garuba, 2008).

Airpwn is a WLAN attack tool for IEEE 802.11 frame injection that listens for specific patterns of frames coming from the access point to the client device. If there is a match with what is specified in the configuration file, then customized spoofed frames are injected from the access point. The valid frames, replaced by the spoofed frames, will be discarded so that they don’t reach the client device (Michael, 2007). File2air is an injection tool similar to airpwn except that it is the user who specifies a file that will be used for the payload of the injected packets. However, File2air runs on top of another tool called Airjack that executes actual frame injection (Michael, 2007).

2.3.3 Denial of Service Attack Tools

Besides performing data integrity attacks, frame injection tools are also utilized by attackers to execute denial of service attacks. One way of doing this is by setting up an attacking client device that sends many authentication frames purported to be coming from different MAC addresses. The objective is to have the authentication table of the access point filled up so that legitimate client devices do to connect to the access point One tool that can perform such attack (called authentication flooding) is Void11(Scott, 2011). This tool can also perform association flooding attack which is executed the same way as authentication flooding. Void 11 performs deauthentication attack by sending very many deauthenticate frames to random MAC addresses. The legitimate client devices connected to a particular access point and with matching MAC addresses will automatically disconnect on receiving the deauthenticate frame(Scott,2011).

Tools such as FakeAP are designed to generate thousands of 802.11 access points with each access point generating its beacon signals. The huge number of beacon signals generated is then used to execute beacon signal flooding attack (Michael, 2007).

2.3.4 Analysis of the Tools Used to Attack a WLAN

Attack tools associated with WLANs can generally be grouped into three; Denial of service (Availability), confidentiality and integrity tools. Most of the tools available to facilitate exploitation of WLAN vulnerabilities are open source and readily downloadable from vendor sites or are integrated in some versions of open source operating systems (e.g. backtrack). The attack tools target weaknesses in security features or configurations flaws on the following features; cipher suite, authentication credentials, client utility, access point firmware, client driver, authentication server, authentication mechanism and user database.

2.4 WLAN Security Standards

While WLAN technology provides several benefits to organizations that deploy them, their features should be able to achieve well known literature supported security objectives of; confidentiality, integrity, availability, access control and authentication (Sheila et al, 2007). While WEP originally provided security features meant to achieve these objectives(IEEE 802.11,1997), it can de deduced from the previous section, that WEP is insufficient because it is susceptible to various cryptographic attacks that either recover the shared encrypt and authenticate key or perform the attacks even without knowledge of the key. Execution of these attacks has been automated via several attack tools such as Airsnort and WEPCrack. WEP’s use of a static key requiring manual rotation is not practical for a WLAN with large number of client devices e.g. in a public WLAN. Authentication built into WEP only authenticates a client device and not the actual user accessing the machine consequently opening a loophole that allows many unauthorized individuals to access the WLAN. Because of the aforementioned issues, the original IEEE 802.11(1997) standard from which WEP is derived has undergone several amendments which include IEEE 802.11i (2004) and IEEE 802.11w (2009).

2.4.1 IEEE 802.11i

Prior to IEEE 802.11i (2004) amendment, IEEE 802.11(1997) security weaknesses had elicited several proprietory amendments. In order to patch these security inadequacies, many vendors incorporated additional security features to their IEEE 802.11(1997) implementations. Consequently, due to lack of a common secure and open standard, interoperability became limited. IEEE 802.11 therefore created an open standard that incorporated security enhancements that were at par with mature and proven security technologies (Sheila et al, 2007).

IEEE 802.11i(2004) came with new authentication mechanisms such as IEEE 802.1x with EAP together with more secure algorithms to offer better confidentiality and integrity protection of WLAN data. It also introduced mechanisms to ensure derivation of unique encryption keys in every session and per frame. The four way key handshake mechanism which validates that both access point and client device share a pair-wise master key (PMK), synchronizes the installation of temporal keys and confirms the selection and configuration of data confidentiality and integrity protocols was a key enhancement made. IEEE 802.11i (2004) introduced a concept commonly referred to as robust security network association(RSNA) which is a logical connection between WLAN entities(client device, access point and authentication server) established through the four-way handshake mechanism. A network created this way is called robust security network (RSN) and is considered very secure.

IEEE 802.11i (2004) allows pre-shared master key (PMK) to be configured on each client device in pre-shared key implementations. In IEEE 802. 1x access control with EAP authentication, the key is automatically distributed after successful authentication. While IEEE 802.11i protects data frames with strong confidentiality and integrity algorithms, it does not protect control or management frames (Sheila et al, 2007).

2.4.2 IEEE 802.11w

While IEEE 802.11i (2004) enhancements resulted in reduced vulnerabilities associated with the initial IEEE 802.11(1997), its protection mechanisms only targeted data frames. Management frames were excluded from these protection mechanisms leaving such WLANs prone to deauthenticate and disassociate attacks (Sheila et al, 2007).

IEEE 802.11w (2009) enhancement consequently was developed to provide a framework for protection of management frames. This standard enhances the security by providing data confidentiality of management frames, mechanisms that enable data integrity, data origin authenticity, and replay protection. IEEE 802.11w (2009) does not create new security scheme nor new management frame format, instead it relies on existing security mechanisms to provide security to specific IEEE 802.11 management frames. Its use in a WLAN implementation is negotiable between client station and access point firmware. Though it is designed to be an optional feature in IEEE 802.11, it is required/ mandatory in all WLANS that have been configured with temporal key integrity protocol (TKIP) or counter mode with CBC- MAC protocol (CCMP).

Whereas there are many types of management frames, the only frames protected by IEEE 802.11w are those sent after four-way handshake. These frames include: disassociation, deauthentication and action frames such as radio measurement action for IBSS (IEEE 802.11k frames), QoS action frame (IEEE 802.11e frames) and IEEE 802.11v frames. The frames are protected using key hierarchy established after the four-way handshake.

WEP encrypted, unencrypted frames or management frames sent before the four-way handshake such as beacon, probe request/response, announcement traffic indication message (ATIM), authentication request/response, association request/response and spectrum management action are not protected (Eian, 2009). This is because they are sent prior to encryption key establishment. CCMP is used by IEEE 802.11w to provide integrity, confidentiality and sender authenticity for unicast management frames while broadcast integrity protocol (BIP) is used to provide integrity for broadcast management frames.

IEEE 802.11w(2009) enhancements protects against denial of service attacks that may be caused by rogue client devices that send forged disassociation requests so that they appear to be sent by valid client devices. It also protects against denial of service caused by rogue access points that send de-authenticate frames to random MAC addresses forcing the affected client devices to disconnect. Protection from these attacks is achieved through providing integrity protection for de-authentication and disassociation frames. If management frame protection is enabled in an access point and unprotected deauthentication, disassociation or action frame is received, the access point silently discards the frame (Eian, 2009).

2.5 IEEE 802.11 Confidentiality and Integrity Protocols (Cipher Suite)

Confidentiality and integrity protocols are also referred to as cipher suite. During the discovery phase of client device-access point association, the negotiated cipher suite becomes the security policy used during that particular communication session once authentication is successful. The cipher suite is responsible for generating dynamic encryption keys specific to a particular association, managing them and providing data encryption and integrity mechanism (IEEE 802.11i, 2004).

2.5.1 Wired Equivalent Privacy (WEP)

WEP is a cipher suite that was originally designed to provide reasonable strength, self-synchronization and processing efficiency that leverages a wired network (IEEE 802.11, 1997). It uses 32-bit cyclic (CRC-32) as a data integrity mechanism and RC4 as encryption algorithm that uses 40-bit encryption key. Prior to transmission of a WEP protected frame, CRC-32 mechanism computes a checksum value on each payload, encrypts both payload and checksum value using RC4 and then transmits them as one frame. On arrival, the received frame is decrypted, checksum value is recomputed based on the received payload and then the result is compared with the received checksum value. If the two checksum values are not identical, then the received frame is discarded because it is taken to have been altered along the way.

According to Sheila et al (2007), WEP has the following known weaknesses: weak encryption algorithm, short static keys, unencrypted initialization vector (IV), weak implementation of RC4 algorithm, inability to specify how the IV should be set or changed, CRC-32 being susceptible to bit flipping attacks and CRC integrity mechanism only detecting random bit errors and not intentional modifications. These weaknesses pose many threats such as: sniffing of data frames for offline analysis in order to recover the key, reveal parties communicating and at what times, determine the content of communications and determination of the operating system in use by the client device.

Other threats include; identification of the original plaintext and replay of previously captured frames.

To enhance the encryption strength of WEP, many vendors have enhanced WEP implementations with key sizes of 128 and 256 bits. While this improves strength to a small extent, it limits interoperability (Sheila et al, 2007).

2.5.2 Temporal Key Integrity Protocol (TKIP)

TKIP is a cipher suite designed to enhance security of WEP implementations without causing significant performance degradation. According to Sheila et al (2007), TKIP was designed to enhance the security of already deployed WEP devices. It does not require any hardware replacements of access points or client devices but only requires software updates to implement.

Security features of TKIP comprise RC4 for encryption and Michael digest algorithm that implements message integrity code (MIC) for integrity protection. Some of the threats it protects include: modifying the destination address in bit flipping attacks, modifying source address in impersonation attacks, fragmentation and iterative key guessing. Other security features include: protection from replay attacks by giving each frame a sequence number and a different encryption key for every frame. This prevents attacks such as FMS (Fluhrer, Mantin and Shamir, 2001) common in WEP based WLANs. TKIP also implements some countermeasures whenever a client device or access point encounters a frame with a message integrity code (MIC) error to thwart possible active attack.

2.5.3 Counter Mode with Cipher Block Chaining-MAC Protocol (CCMP)

CCMP is a cipher suite designed to enhance security performance of WLAN by addressing the inadequacies of predecessors WEP and TKIP. However, unlike TKIP, CCMP required change of hardware when deployed where WEP or TKIP implementations exist (IEEE 802.11i, 2004). CCMP is a very strong cipher suite because it is based on a generic authenticate and encrypt block cipher mode of AES called counter mode with cipher block chaining message authentication (CCM) protocol .CCM combines two proven techniques; counter mode (CTR) for confidentiality and cipher block chaining message authentication code (CBC-MAC) for both authentication and integrity protection. CCMP protects the integrity of both the frame data and portions of IEEE 802.11 frame header. CCMP uses a 128 bit key size for encryption and a 48 –bit packet number (PN) to construct a nonce that is used to prevent replay attacks. The construction of the nonce therefore allows the key to be used for both integrity and confidentiality without compromising either.

2.6 WLAN Access Control and Authentication Mechanisms/Protocols

The original IEEE 802.11(1997) provided only two means to prove the identities of client devices attempting to gain access to WLAN: open system authentication and pre-shared key authentication with pre-shared key being optional. With security enhancement IEEE 802.11i(2004), more secure authentication and access control approaches were incorporated as alternatives to pre-shared key and open authentication.

2.6.1 Open System Authentication

Open system authentication is where a client device authenticates to an access point (AP) by providing the service set identifier of the access point and its media access control (MAC) address. Since access points broadcast their SSIDs in plain text, any device configured in managed mode will capture the SSID for an access point. Therefore in this case there is nothing to prove identity of the client device.

One IEEE 802.11(1997) mechanism used to implement access control in open system authentication is MAC address filtering where network administrators add a list of authorized MAC addresses on the access point memory. When configured this way, the access point will only allow devices whose MAC addresses exist in the authorized list to access the WLAN resource. One major weakness of this method when open authentication is used is that client device’s MAC address is not encrypted. A client device can therefore be set in monitor mode to intercept traffic of the devices connecting to the WLAN and consequently be able to establish allowable MAC address.

Once allowable MAC addresses have been established, the attacker will configure their client device with one of these allowable MAC addresses to gain unauthorized access. Since open authentication does not authenticate the access point, the client device may associate with a rogue/imposter access point that is set to the SSID of the real access point. Therefore open system authentication is an extremely weak authentication mechanism that should not be configured on any WLAN that is meant to prove real identities of the users accessing a WLAN (Martin, 2008).

2.6.2 Pre-Shared Key (PSK) Authentication

Pre-shared key authentication mechanism is based on secret key cryptographic approaches where a secret key is shared by legitimate client stations and access point. The mechanism applies a challenge–response scheme that is meant to prove that the client device trying to gain access to a particular WLAN knows the secret key. When a client device initiates this process by sending an authentication request, the access point generates a random 128–bit word called challenge and sends it to the client device. The client device is expected to encrypt this challenge using the pre-shared key. After encrypting, the client device returns the result to the access point as response. On receiving the response from the client device, the access point decrypts this response using the same key as that expected to have been used by the client device. The client device is allowed to access the WLAN only if the decrypted value is the same as the challenge.

While the design of pre-shared key authentication mechanism is more robust than open system authentication, it has been established that it is prone to security attacks (Sheila et al, 2007). The mechanism only authenticates the client device to the access point. The mechanism does not authenticate access point to the client device which makes it possible for a rogue access point to pretend that the authentication was successful even without knowledge of the secret key (Gast, 2005).Also because the access points cannot identify the individuals using the WLAN, the clients are relatively anonymous.

Most large enterprise public WLAN deployments such as those in universities will not use pre-shared key because of the difficulty of managing security of manually distributed pre-shared keys (PSKs) on numerous devices (Sheila et al (2007).

The challenge handshake protocol (CHAP) used to encrypt the challenge has known vulnerabilities which are exploited by password recovery, cracker and sniffer tools such as Cain and Abel to recover weak pre-shared keys (Gast, 2005).

2.6.3 IEEE 802.1x Port Based Access Control and Authentication

IEEE 802.1x controls access to WLAN resources by blocking user access until authentication is successful. Originally designed for wired networks, IEEE 802.1x was revised later for use on WLANs after flaws and vulnerabilities in the authentication schemes proposed in IEEE 802.11(1997) standard were discovered (Shumman & Ran, 2003).

Because all links to a WLAN are publicly accessible, it is prudent to implement access control at the point at which a user joins the network through port security which will protect network connections even where these connections might be accessible in a non-secure area (Edney & Arbaugh, 2004).

Port based access control was introduced by IEEE 802.11i (2004) amendment which provided a framework for centralized, mutual authentication and access control that could leverage Extensible Authentication Protocol by(Aboba, Blunk, Vollbrecht, Carlson & Levkowetz ,2004).

IEEE 802.11i requires that the Extensible Authentication Protocol (EAP) method used with IEEE 802.1x provides mutual authentication. IEEE 802.1x describes how to transport user credentials from the supplicant(client device) to the authentication server transparent to the authenticator(access point) or any other device along the path by leveraging on EAP.

The encryption between the supplicant (client device) and authenticator (access point) can be done using rotating WEP keys, WPA with TKIP or WPA2 with AES. Until successful authentication occurs between supplicant (client device) and authentication Server (AS), all supplicants communication is blocked by the access point/authenticator. The technique used to block the communication is known as port-based access control. IEEE 802.1x controls data flows by analyzing the frame types and then passing EAP frames through an uncontrolled port and non-EAP frames through a controlled port, which blocks access. IEEE 802.11i (2004) extends this to block the access point‘s communication until after the four-way handshake when all security keys are in place to ensure all communication thereafter is protected.Figure 2.8 illustrates IEEE 802.1x components.

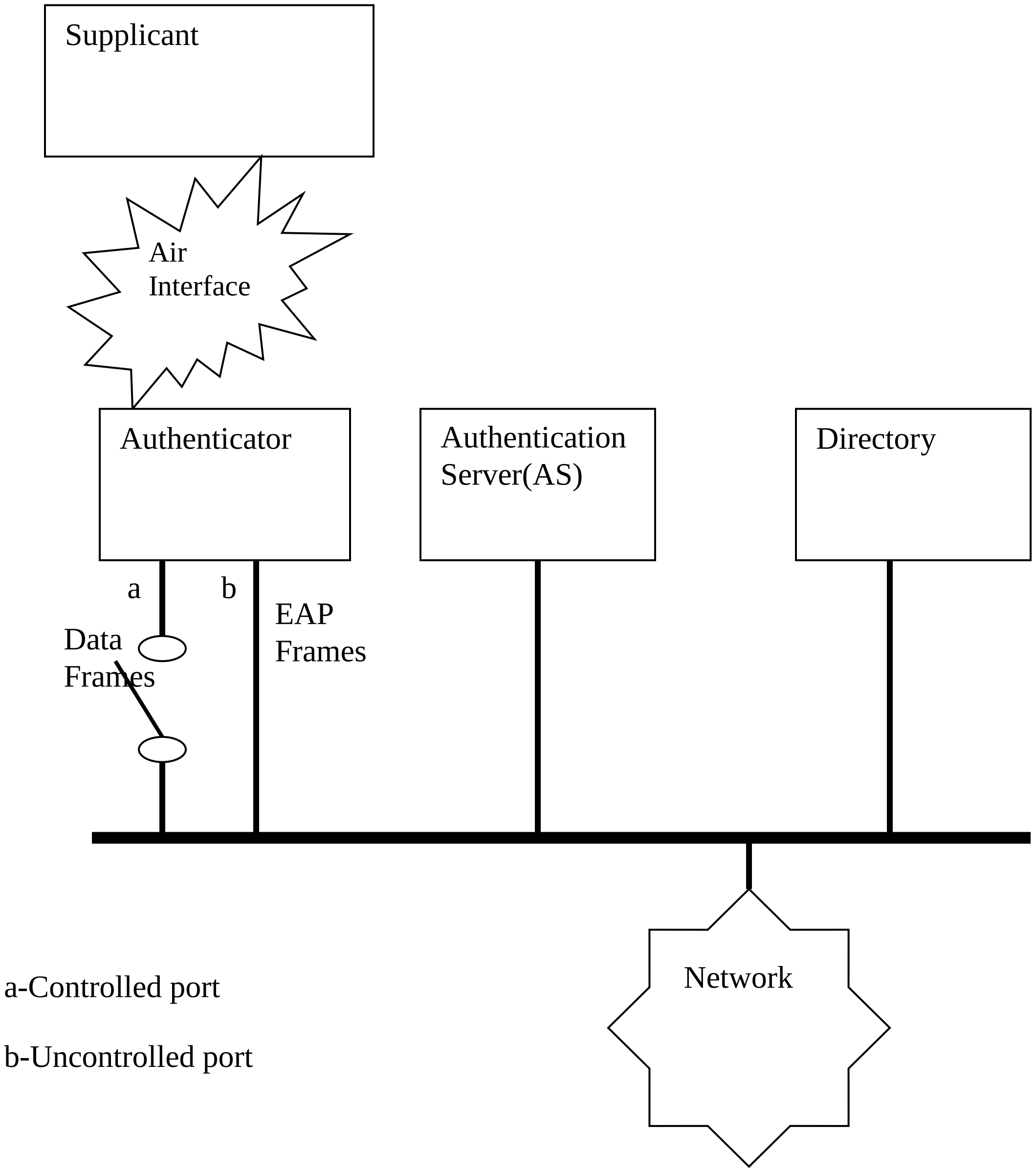


Figure 2.8: Wireless LAN Security with 802.1x(Edney & Arbaugh, 2004).

The major limitation of using IEEE 802.1x in its original form is that its mutual authentication is optional meaning that if the default set-up is not changed to mutual authentication, then the wireless network will be open to attack(Edney & Arbaugh, 2004). Another limitation is that IEEE 802.1x does not provide continuous authentication but provides one time authentication at the beginning of a session. Therefore if an attacker learns the MAC address of a legitimate user's workstation, then the attacker could impersonate the legitimate user. This means that implementers of this authentication scheme need to do configurations that seal these vulnerabilities (Edney & Arbaugh, 2004).

While various EAP methods exist, IEEE 802.11i does not recommend any EAP authentication method for RSNs but gives implementers discretion in choosing authentication method to use in their WLANs. This means that an implementer may select a weak EAP authentication method or implement a strong method improperly, consequently weakening the RSN protection. Security breaches at this level could also compromise other network assets as well especially in networks implementing single sign in (Sheila et al, 2007).

2.6.4 Review of Extensible Authentication Protocol (EAP)

Extensible authentication protocol is developed to provide authentication to all IEEE 802.11i networks employing 802.1x port-based access control through various EAP methods (Aboba et al, 2004). EAP supports a wide variety of authentication methods that also use various credentials. These credentials include; static passwords, certificates, secret key, one time passwords etc. These methods can also combine various authentication techniques such as a certificate and a password. Through EAP an access point forwards authentication messages between the client and a back-end authentication systems that comprises of one or a small number of authentication servers. EAP is also used to enable both client device and authentication server to agree and distribute keying material which can be mutually derived or distributed by the authentication server. Subsequently the authentication server distributes the keying material to the access point which signal to the access point that the client device is authorized to gain access to the WLAN.

RADIUS protocol works with EAP to transport back-end EAP authentication and key distribution traffic. The EAP method deployed in an implementation influences the security of the WLAN because other than authentication, EAP methods also generate the key material used to protect subsequent communications.

Many types of EAP methods are available. They include EAP-MD5 by Aboba, et al. (2004) which uses Message-Digest algorithm 5 (MD5) hash to authenticate client.

However, the wireless network security provided by this EAP method in most situations is inappropriate (Agni, Azween & Low-Tan, 2008).

EAP with Transport Layer Security (EAP-TLS) by Aboba & Simon (1999) is a mutual authentication mechanism that uses both client and server digital certificates as authentication credentials(Dierks & Allen, 1999).In terms of WLAN security, EAP TLS is considered the strongest EAP method (Khidir & Owens 2007)).

EAP with Tunneled TLS (EAP-TTLS) by Funk & Blake-Wilson (2007) is an EAP method that can be implemented on IEEE 802.1x.While server side certificate is mandatory for EAP-TTLS, client side certificate is not and can use legacy authentication methods. Because EAP TTLS skips authenticating a client using a certificate, it is not prone to complexities of public key infrastructure associate with public key infrastructures. However, it offers strong security.

Protected EAP (PEAP) by (Kamath, Palekar &Wodrich, 2002) also uses server side certificates as authentication credentials and leaves client authentication to other authentication methods just like EAP-TTLS. However, it is not compatible with legacy methods and platforms which EAP-TTLS is compatible with.

Lightweight EAP (Sankar, Sundaralingam, Miller & Balinskyl, 2005) is a proprietory method developed for authentication only on Cisco WLAN devices. It offers support for mutual authentication and changes keys dynamically every time there is re-authentication to make its security stronger.

EAP-SIM is a SIM card based EAP method developed by (Haverinen & Saloway, 2006) that uses a 2G GSM network SIM. EAP-AKA (Authentication and Key Agreement) developed by Arkko & Haverinen (2006) is also a SIM based EAP method but uses 3G UMTS Subscriber Identity Module (USIM).

In general, EAP authentication methods can be thought of as taking three approaches; Secret-Key approach where the authentication server and the client device establish trust through proving to each other knowledge of a shared secret. EAP methods in this category include; LEAP and EAP-Secure Remote Password (EAP-SRP).While LEAP is widely deployed, it has since been established that it has vulnerabilities that expose it to dictionary attacks(Kwang-Hyun, Sean & David, 2004).This vulnerability of LEAP was overcome by EAP-SRP which uses temporary asymmetric keys that are based on the shared symmetric key. However, not many implementers use EAP-SRP (Kwang-Hyun et al, 2004).

The second approach is Public-Key methods where authentication server and the client device establish trust through a certification Authorities (CAs). Certificate authorities sign their certificates using their private key so that a client device can verify the validity of the certificate using their public key. Client devices are assumed to have, in advance, a copy of the certificate authority's public key to use for validating certificates. Certificate-based protocols are hard to implement due to the requirement of certificate authorities(Kwang-Hyun et al, 2004).EAP-TLS is one of the popular methods in this category.

The third approach is the use of tunneled methods which operate with two authentication phases. In the first phase, the client authenticates the authentication server using a certificate credentials provided by the authentication server and establishes a session key which is used to establish an encrypted tunnel to encrypt their communication. In the second phase, the authentication server authenticates the client through the encrypted tunnel. EAP methods in this approach are; PEAP and EAP-TTLS. Asokan et al (2002) discovered a man-in-the-middle attack in these tunneled protocols. Because EAP-TTLS support legacy authentication methods that may not create session keys, the protocols require that the session key from the first phase i.e the key used to encrypt the tunnel, be the session key for the message protection process. However, because some clients using back level operating system and software may not be able to perform EAP-TLS authentication, EAP-TTLS will allow the client to forego the tunneling and proceed to the second phase.

This scenario creates a vulnerability that can be exploited to launch a man in-the-middle attack with which an attacker can steal a legitimate client device's session. Therefore, implementers of such EAP methods need to incorporate appropriate solutions to resist the attack. Other EAP methods include; token based authentication protocols, EAP one time password (EAP-OTP) and EAP-SIM (John & Robert, 2002).

According to (Kwang-Hyun et al, 2004)EAP-TTLS and PEAP offer security similar to that provided by EAP-TLS with additional characteristics such as identity privacy while overcoming EAP-TLS's difficulty of requiring the client to possess certificates issued by certificate authority that the authentication server trusts. Additionally, TTLS provides support for existing legacy RADIUS servers to authenticate client devices .This is achieved by inserting a RADIUS/EAP-TTLS server between the wireless access points and the legacy RADIUS server (John & Robert, 2002).

EAP methods support a number of different types of configuration that implementers need understand e.g. while authentication between client device and an authentication server is mutual, it doesn't have to be necessarily symmetric e.g the authentication server might authenticate to the client station using a certificate but the client station might authenticate to the authentication server using biometric information. In all these cases, the nature of authentication depends on the EAP method employed.

Some EAP methods support mutual authentication while others do not. While EAP only allows one authentication method to protect against certain types of attacks, complex authentication architectures such as EAP multiplexing and EAP tunneling can still be supported within this framework. A typical EAP implementation requires the three entities; supplicant/client device, authenticator/access point and authentication server to reside in three separate devices. However, another approach where the authenticator embeds both authentication service and the authenticator is also supported. To support such functionality, the node that acts as the authenticator and authentication server must have high computational capabilities failure to which it will be susceptible to denial of service attacks (Sheila et al, 2007).

2.6.5 Captive Portals

The Captive portal authenticates users using a web interface that connects to an authentication server containing a database of valid users. Whenever an unauthenticated user tries to access the Internet, his/her web browser is redirected to the login page where the user is required to enter a username and a password. It both the user name and password match the details on the user database, the authentication server gives the user access to the internet through a WLAN.

Where a captive portal is used, one is not required to install additional software in their client device other than the web browser. Such is the convenience that makes many public WLANs to use captive portals for user authentication (Wei-Lin & Quincy, 2010).

Research (Haidong & Jose, 2004) shows that when captive portals are not properly configured e.g. without SSL encryption or when SSL is misconfigured, then captive Portal are susceptible to man in the middle related attacks. A demonstration of this attack using ARP spoofing was illustrated by (Wei-Lin & Quincy, 2010).Captive portals only authenticate the client/user but not the server (no mutual authentication).

Captive portals provide no MAC layer encryption and therefore, it is up to the implementers to provide confidentiality and integrity protection of data frames at that level (Haidong & Jose, 2004). Failure to offer additional protection can lead to information such as MAC address being sniffed and later used to configure rogue devices to connect to the WLAN. Unless combined with other authentication methods described in this section, captive portals authentication is therefore susceptible to many attacks such as deauthentication, and deassociation. Captive portals are also susceptible to evil twin attacks.

2.6.6 Credentials Used for WLAN Authentication and Access Control

Authentication credentials refers to the information delivered to the authentication server by a client device or provided by the authentication server to the client device and used to verify a claim by an entity (client or authentication server) that it is authorized to act on behalf of a known identity.

Credentials used during authentication can be stolen and used to gain access to a WLAN. Dictionary and brute force attacks are the most common techniques in this category (Waliullah, 2015) .Other techniques include phishing and sniffing.

Analysis of various authentication methods show that the most common authentication credentials employed by authentication mechanisms include; password, secret key, preshared key ,SSID,MAC address, one time password, client and server certificates. Each of these credentials has its own vulnerabilities when used for authentication, most of which are due to misconfigurations. Many hotspots and guest WLANS operate in open mode allowing any station to connect to that network without any credentials while others have been configured with default passwords (SANS Institute Infosec Reading Room, 2003). Some open WLANs may rely on MAC address as credentials .However, various available open source attack tools e.g. Kismet can sniff MAC addresses of authorized client devices (Mathews & Hunt, 2007).

2.7 Concepts and Research Related to WLAN Model Development

This section reviews pertinent theories and concepts related to model development.

2.7.1 Security Measurement, Analysis and Security Metrics Model

Measurement is determination of the magnitude of a quantity which may involve data collection, repeated over time or at a single point in time. Measuring security level of an implementation provides vital information on its security performance that enables implementers to manage it. Katze (2001) identified three fundamental aspects of a **s**ecurity measurement model: planning on what is to be measured, how it will be measured and what to compare the measurement results with.

Savola & Holappa (2005) recommends that a security measurement model should comprise metric objects, measuring methods and a measuring rod. Metric objects are measured based on specified methods. A measuring rod derived from analysis of security features based on security objectives contain reference information classified according to the level of security and can include security level data that is generally known or gathered from statistical data. A measuring rod is used to compare the results of the measurement. There is need to put in place mechanisms that enable the measuring rod to update itself.

2.7.2 Assessing Level of Network Security

Daniel and Edward (2010) propose three parameters for assessing network security: attack susceptibility, penetration susceptibility and knowledge level. Attack susceptibility (AS) is a variable that assesses how susceptible vulnerability is to be exploited and how complex it is to develop a certain attack against the network implementation (Daniel and Edward, 2010).Attack susceptibility therefore measures the severity level of vulnerability. They measure attack susceptibility on a scale of 0-5 where value 0 means that the vulnerability is not susceptible to being exploited and a value of 5 means a highly susceptible vulnerability.

Penetration susceptibility (PS) evaluates and quantifies how susceptible the network is to be penetrated. It is based on the time taken by an attacker to exploit certain vulnerabilities to penetrate a network (Daniel and Edward, 2010). Penetration susceptibility is measured on a scale of 0-5 where 1 means it took 10 or less minutes to penetrate the network while 5 means it took more than one day to penetrate the network. If the network is not penetrable it is given 0.

The knowledge level (KL) measures the cumulative implementer's expertise to implement required security standards in order to protect against penetration (Daniel and Edward, 2010). Knowledge level is cumulatively measured on a scale of 1-5 where 5 means the implementer has expertise values of 1,2,3,4 and 5 and 1 is use of Internet, 2 is Windows Server operating system, 3 is Linux operating system, 4 is Servers configuration and 5 is Database management.

While attack susceptibility(AS) and knowledge level required(KL) can be reliably measured, penetration susceptibility(PS) is affected by so many other extraneous factors related to both hardware and software and so may not give reliable results. This variable can only be useful when the test environment is highly controlled. In general we emphasize that while existing approaches are applicable in practice, they are not comprehensive enough.

2.7.3 Attack Tree Analysis

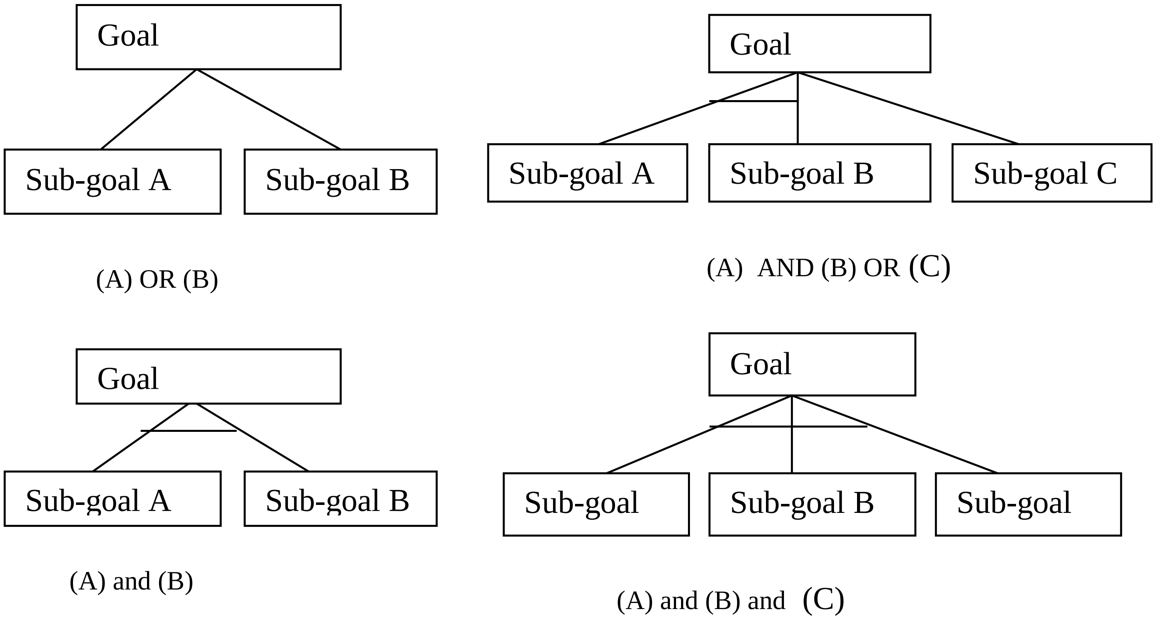
Attack tree was first used by Schneier (1999) to provide a formal way of describing the security of a system. It presents a formal methodical way of finding ways to attack the security of a system (Schneier, 1999). Schneier proposes to represent attacks against a system in a tree structure where a goal is the root node and different ways of achieving that goal are leaf nodes. More specifically, attacks are represented in a tree structure where the root node is the main goal, intermediate nodes are the subgoals, and leaf nodes are the ways to reach to the subgoals and finally to reach the main goal in turn. Children of a node in the tree can be of types: *AND* and *OR*. To reach a goal, all of its *AND* children or at least one of its *OR* children must be accomplished. This is similar for all subgoals down to leaves of the tree.

To construct attack trees, possible attack goals must be identified. Each attack goal becomes a root of its own attack tree. Then construction continues by considering all possible attacks against the given goal. These attacks form the *AND* and *OR* children of the goal. Next, each of these attacks becomes a goal and their children are generated. This process recursively goes down to leaves.

In such a tree structure, an attack scenario to reach a main goal is the subtree which includes root node and all its *AND* along with at least one of its *OR* children. Same selection is made for all selected children (subgoals) recursively down to leaves. These selections form subtree of the given attack tree. An attack tree is complete if it contains a subtree for all possible attacks to fulfill a given main goal.

It is possible to assign different attributes such as cost to nodes on the tree and consequently using such attributes to extract attacks with certain properties. Such information may be very useful in defining possible and feasible threats and invest for countermeasures.

Attack trees provide a systematic method used to characterize system security based on varying attacks (Scheiner, 1999) and have been used in varying situations to specify security requirements e.g. (Moore, Ellison & LingerMoore, 2001) proposed using attack trees to model security requirements for a specific domain of survivable systems. Convery et al (2004) applied attack tree to analyze potential threats to Border Gateway Protocol (BGP) from the adversary’s perspective. Figure 2.9 shows how attack trees are represented for different “OR” and “AND” scenarios.



(A) OR (B)

(A) AND (B) OR (C)

(A) and (B)

(A) and (B) and (C)

Figure 2.9: Attack trees (Karpinen, 2005)

An analysis based on attack trees has many advantages. Its adoption is easy because it does not require any special tool (Karpinen, 2005).It is applicable in many contexts and facilitates determination of any level of abstraction, depending on the need, while keeping track of the chain of actions. Where numerical analysis may be needed, attack trees can be used because one can assign values to the nodes of the tree, such as cost, impact or attack/vulnerability severity.

The attack tree approach can assist in analyzing the security of implementations and finding the weakest security features through documenting most of the potential attacks (Karppinen, 2005). Attack trees capture knowledge and expertise in a reusable form. Once the attack tree for a certain security feature has been built, it can be included as part of a larger attack tree for a system that uses the security feature (David, William, Sanders & Trivedi, 2004).Many approaches in security analysis are based on the idea of modeling the attacker's steps in attacking the system.

Most of the earlier work on computer security focused on details in complex protocols or details in complex systems, because the root causes of security gaps are often found in the failures associated with such details (David et al, 2004).Later work (Deswarte et al,1991) and (Dutertre et al,2002) ,(Cukier et al,2001)expanded the attention to system-level security, that is, to the study of how systems can be designed to be secure in the sense that they perform their intended function in spite of possible malicious attacks e.g intrusion tolerance. So far, most attempts at evaluation of security have been qualitative, focusing more on the process used to build a system that should be secure. The use of quantitative techniques is limited to analysis of small parts of an overall design based on formal methods or experimental approaches set up by white-hacker teams who try to compromise a system.

Since it is impossible in practice to build a perfectly secure system, there is much to be gained by developing a model-based approach for establishing and evaluating an approximate security level one can expect from a particular implementation of WLAN authentication and access control for decision making purposes. Attack tree (Schneier, 1999) approach can therefore be a useful tool for modeling attacks or vulnerabilities against a WLAN system and combined with other tools will help in constructing the overall measurement model for a WLAN authentication and access control.

2.7.4 Common Vulnerability Scoring System (CVSS)

Common vulnerability scoring system is an industry open standard designed to convey vulnerability severity and helps determine urgency and priority of response (FIRST, 2014). It solves the problem of multiple, incompatible scoring systems and is easy to understand and use. CVSS is a joint effort involving many technology companies; CERT/CC, Cisco, DHS/MITRE, eBay, IBM internet security systems, Microsoft, Qualys and Symantec. Many other companies have since joined and assisted in improving it. Currently, it is maintained by forum of incidence response and security teams (FIRST). The CVSS Model is designed to provide an overall score of an attack or vulnerability. The scores are derived from parameters that are in three distinct categories base metrics, temporal metrics and environmental metrics. These parameters can be quantitatively and qualitatively measured.

Base metrics constitute characteristics that are intrinsic to any given vulnerability and that do not change over time or in different environments (FIRST, 2014). These metrics are attack vector (V), attack complexity (AC), privileges required (PR), user interaction (UI), scope(S), confidentiality impact(C), integrity impact (I) and availability impact (A).

Attack Vector (AV) metric reflects the context in which the vulnerability exploitation occurs. The more remote an attacker can be to the target, the greater the vulnerability score, the rationale being the number of potential attackers for a remotely exploitable vulnerability would be much larger than that for an attack requiring local access.

Attack Complexity (AC) metric describes the conditions beyond the attacker's control or user interaction requirements that must occur in order to place the system in a vulnerable state.

Privileges Required (PR) metric describes the privileges an attacker requires before successfully exploiting the vulnerability, and the potential impact they could inflict on a system after exploiting it.

User Interaction (UI) metric captures the requirement for a user (other than the attacker) to participate in the successful exploit of the target system. This metric determines whether or not the vulnerability can be exploited solely at the will of the attacker, or if a user must participate by taking action.

Metric scope(S) measures whether the authorization scope of the vulnerable component is the same or different from the authorization scope of the component impacted by the vulnerability. If the vulnerable component is in the same authorization scope as the component impacted by the vulnerability, then the scope of impact is unchanged. However if the vulnerable component is in a different authorization scope from the component impacted by the vulnerability then the scope is changed.

Confidentiality Impact (C) metric measures the impact to confidentiality of a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. Increased confidentiality impact increases the vulnerability score.

Integrity Impact (I) metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and guaranteed veracity of information. Increased integrity impact increases the vulnerability score.

Availability impact (A) metric measures the impact to the availability of the affected impact Scope resulting from a successfully exploited vulnerability. While the

Confidentiality and Integrity impact metrics apply to the loss of confidentiality or integrity of data (e.g. information, files) used by a affected Impact Scope, this metric refers to the loss of availability of the affected Impact Scope, itself, such as networked service (e.g. web, database, email, etc). Since availability refers to the accessibility of information resources, attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of an affected Impact Scope. Increased availability impact increases the vulnerability score. In general, base metrics represent characteristics of vulnerable component as well as the consequence to the impacted component.

Temporal metrics contain characteristics of vulnerability which evolve over the lifetime of vulnerability (FIRST, 2014). They include exploitability, remediation level and report confidence

Exploitability (E) measures the current state of exploit techniques or code availability. Public availability of easy-to-use exploit code increases the number of potential attackers by including those who are unskilled, thereby increasing the severity of the vulnerability. Initially, real-world exploitation may only be theoretical. Publication of proof of concept code, functional exploit code, or sufficient technical details necessary to exploit the vulnerability may follow. Furthermore, the exploit code available may progress from a proof-of-concept demonstration to exploit code that is successful in exploiting the vulnerability consistently. In severe cases, it may be delivered as the payload of a network-based worm or virus. The more easily vulnerability can be exploited, the higher the vulnerability score.

Remediation Level (RL) measures the extent of remediation for a particular vulnerability. The typical vulnerability is unpatched when initially published. Workarounds or hotfixes may offer interim remediation until an official patch or upgrade is issued. Each of these respective stages adjusts the temporal score downwards, reflecting the decreasing urgency as remediation becomes final. The less official and permanent a fix, the higher the vulnerability score is.

Report Confidence (RC) measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details. Sometimes, only the existence of vulnerabilities are publicized, but without specific details. For example, an impact may be recognized as undesirable, but the root cause may not be known. The vulnerability may later be corroborated by research which suggests where the vulnerability may lie, though the research may not be certain. Finally, vulnerability may be confirmed through acknowledgement by the author or vendor of the affected technology. The urgency of vulnerability is higher when vulnerability is known to exist with certainty. This metric also suggests the level of technical knowledge available to would-be attackers.

Environmental metrics contain those characteristics of vulnerability which are tied to an implementation in a specific environment (FIRST, 2014). They include confidentiality requirement, integrity requirement and availability requirement. These metrics enable the analyst to customize the CVSS score depending on the importance of the affected component to a user's organization.

Measured in terms of confidentiality, integrity and availability, if the component supports a business function for which confidentiality is most important, the analyst can assign a greater value to confidentiality, relative to availability and integrity. Each security requirement has three possible values: "low," "medium," or "high." The full effect on the environmental score is determined by the corresponding base impact metrics. That is, these metrics modify the environmental score by reweighting the (base) confidentiality, integrity, and availability impact metrics. For example, the confidentiality impact (C) metric has increased weight if the confidentiality requirement (CR) is "high." Likewise, the confidentiality impact metric has decreased weight if the confidentiality requirement is "low." The confidentiality impact metric weighting is neutral if the confidentiality requirement is "medium." This same logic is applied to the integrity and availability requirements.

2.7.5 Trusted Computing Base (TCB)

Trusted computing base is a concept applied in design of operating systems and was originally defined by Rushby (1981) as the combination of Kernel and trusted processes.

Lampson et al (1992) defined trusted computing base as a small amount of software and hardware components that security depends on and that we distinguish from a much larger amount that can misbehave without affecting security. According to

Steven(2015),the orange book regards TCB of a computer system as totality of protection mechanisms within it, including hardware, firmware, software and controls the combination of which are responsible for enforcing a computer security policy.

Trusted communication path is a functional requirement of TCB in order to permit secure communication between users and the TCB. This fundamentally means that a TCB is a set of all hardware, firmware and software components of a computer system that are critical to its security such that any vulnerabilities occurring inside a TCB negatively influences the security level of the entire system. Therefore, TCB components must be trusted for a computing environment to be secure and that in order to break security, an attacker must subvert one or more of TCB components**.** A given piece of hardware or software is part of TCB if and only if it has been designed to be part of the mechanism that provides security to a computing system(Steven,2015).Systems that do not have a trusted computing base as part of their design do not provide security of their own. They are only secure in so far as security is provided to them by external means (Steven, 2015).

In operating systems, where this concept was originally applied, TCB consists of a kernel or micro-kernel and a select set of system utilities (Rushby, 1981; Hohmuth et al, 2004; Klein et al, 2009). Where a programming language has security features designed using TCB concept, TCB is formed from the language runtime and standard library. While this concept was originally applied in the design of operating systems security, it can be adopted and be applied in network security particularly when composing components that are key to secure computing in a particular environment e.g. WLAN.

2.7.6 Human Element in Design of Security Models

Human element is an important consideration in any security issue because it contributes heavily to realization of attacks. Attacker is a key human element relevant to security.

According to Gollman (1999), an attacker will always have an objective to penetrate and access resources of a system and will endeavor to achieve it by launching one or many attacks. Attacker motivation which refers to perceived benefits to the attacker after successful attack is therefore key to security. Danielle (2011) argues that even though many attacks are automated, a human attacker is behind the development of the attack tool and will still be the one run the first attack command. Besides motivation, the attacker also needs resources such as tools to execute the attack, funds to enable him/her procure the tools and knowledge, skills and experience (Danielle, 2011). The higher the availability of attack tools to an attacker, the higher the resources/capabilities.

A typical attacker/adversary model comprises the following elements; objectives, pre-attack capabilities and capabilities during the attack. An adversary can be a human being, network interface devices or a computer and the main objectives are to cause denial of service attacks, attacks on integrity and attacks on confidentiality. By achieving these objectives, the attacker will be able to break confidentiality, integrity as well as availability security goals of any system. Pre-attack capabilities include; ability to conduct reconnaissance and surveillance on a target WLAN to gain information as to where, when and how to conduct the attack. The adversary can sniff frames using a 802.11 compatible network interface card and tools such as wireshark, save the captured traffic and then analyze it. Capabilities during the attack include tools that achieve the targets.

With motivation and capability, an attacker can directly target users who (Schneier, 2000) argues is the weakest link on a network. Faced with threats related to social engineering (Mitnick & Simon, 2003), argue that security implementers need to focus on system users. With social engineering, system users can be lured by attackers to perform tasks that lead to capturing their passwords even on well-protected network. Users also create simple passwords such as their username, birthdays, spouse etc because they are easy to remember. However, hackers can easily guess or crack such passwords and consequently get unauthorized access during WLAN authentication. User education on such security issues that target them will enhance their risk perception which will in turn reduce social engineering related attacks (Gibson, 2007). In general, human component i.e. hackers and users play a significant role in security and they both have potential to cause security breaches even on very secure WLANs.

2.7.7 Expert Systems and Knowledge Representation

Newell and Simon (1972) proposed a production system model, the foundation of the modern rule-based expert systems. The production model is based on the idea that humans solve problems by applying their knowledge, in form of production rules, to a given problem represented by problem-specific information. The production rules are stored in the long-term memory and the problem-specific information or facts in the short-term memory.

Newell and Simon (1972) argued that humans are representable as information processing systems. The information processing system described is made up of; an active processor input (sensory) and output (motor) systems, internal long term memory, short term memory and external memory. This theory was made operational through use of expert systems which are computer programs that use human expertise that is contained within it to make decisions. This technology advances the capabilities of the computer beyond traditional use by allowing utilization of decision-making logic, heuristics as well as interpreting large amounts of data (facts) through an interactive computer- based decision tool.

Expert systems, which deal with both qualitative and quantitative data, rely on both facts and heuristics to solve decision problems based on knowledge acquired from an expert in a narrow, specialized domain (Penta, 2002). Thus, the most important feature expected from it is high-quality performance. Use of heuristics to guide the reasoning reduces the search area for a solution. Rule-based expert systems enable natural knowledge representation because an expert usually explains the problem-solving procedure with natural expressions like “in such-and-such circumstances, i do this and that” which can be represented quite naturally as IF-THEN production rules. These characteristics together with the ability of a rule based expert system to review and explain its decisions makes users feel comfortable with the systems (Mory and Meech,2000).The uniform if-then syntax of production rules associated with rule based expert systems enables them to be self-documented.

Expert systems separate knowledge from its processing. This means that knowledge base and inference engine are separate making it possible to develop different applications using the same expert system shell. Most rule-based expert systems are capable of representing and reasoning with incomplete and uncertain knowledge.

2.7.8 Model Validation Techniques and Approaches

Balci (1998) explains that for a model to be valid, it must be checked to ascertain whether its behavior is satisfactory and that it is consistent with study objectives. To check validity of a model one can elicit validity responses from the development team, model users, third parties (other than users or development team) or create a set of indicators which are given to subject matter experts to score (Sargent, 2011).

Experts' elicitation can validate the components of WLAN security and influences among component characteristics.Balci (2008) and Sargent (2011) provides several validation techniques which include: face validation, walkthrough, extreme condition tests, historical data validation, parameter variability-sensitivity analysis, predictive validation, validation using traces, simulation and turing tests.

Face validation involves experts on the problem domain providing their opinion on reasonableness of the model's structure, logic and input-output relationships. Interviews or surveys involving use of questionnaires may be used to elicit the responses.

Walkthrough involves validation based on a combination of model development team and another team independent of the developers

Extreme condition tests involves checking for any extreme and unlikely combination of levels/values of parameters in the system e.g if a value of one parameter is zero, then a process involving multiplication of this value should output zero.

Historical methods rely on data if available. Some of the data is used to develop the model and the other is used to check that the developed model behaves the same way as the actual system where data was derived from.

Parameter variability-sensitivity analysis involves varying input values to a model and then observing the corresponding change on its results/output or behaviour. The same relationships should occur in the model as they would in the real system. This technique can be used qualitatively which involves directions only of outputs or quantitatively where both directions and precise magnitudes of outputs are involved. Based on this analysis, parameters which cause significant changes in the model's behaviour or output should be made sufficiently accurate prior to using the model.

Predictive validation involves using the model to predict/forecast the actual system's behaviour and output. The actual system's data is then collected from an existing system or by conducting experiments on the system e.g. field tests. Comparisons are then made between the actual system's output behaviour and the model's forecast to determine if they are the same.

Trace testing involve tracing/following through different types of specific entities in the model to determine if the model's logic is correct and if necessary accuracy is obtained.

Simulation involves representing the model characteristics and relationship in a mathematical model where applicable. Input values and corresponding results collected from the actual system to validate the model is matched with the mathematical model results for similar input.

Turing tests on the other hand involve domain experts of the system being modeled being asked to discriminate between system and model outputs.

The validation approaches discussed in this section indicate that there are two major sources of validation data; actual system generated data or domain experts. While actual system generated data is the most appropriate, it may not be available or appropriate in some instances e.g. where the system being modeled is not directly observable. Danielle (2011) argues that many organizations will not disclose security data to outsiders because such data contain information such as IP addresses that can identify individuals and then be used to track their activities. However, those willing to disclose the data can avoid this situation by extracting only data that cannot identify individuals- a process called sanitization (Jaquith, 2007).

While an organization may collect a lot of data e.g. through an intrusion detection system, lack of widely accepted security metrics to analyze this data is a major challenge (Geer et al, 2003). Many of the metrics available are subjective and others qualitative (Wang, 2005; Nistir et al, 2009) and therefore no standardization of many of the tools that collect security data. Security data collected by intrusion detection or other security tools may also be incomplete. This is because the data collection tool may not capture all the interactions that led to the realization of the attack based on the fact that for every attack, there are several possible paths. An unauthorized access to a WLAN for example

could be as a result of several possibilities; password guess through brute force, password cracking, social engineering, password sniffing etc. Information captured by the security tools may not identify exactly which of the options was employed.
Therefore unavailability or incompleteness of validation data can impede ideal validation. Experts on the other hand may be unwilling to help and even if they do, they may not reserve enough time to do the validation (Kotulic & Clark, 2004). However, these two approaches when used together can bring out significant insights (Gable, 2010).

Kleijnen (1999) suggests use of domain experts and parameter variability-sensitivity sensitivity for validation where no actual system generated data is available. He also suggests use of statistical tools for validation where only actual system output data is available without corresponding input data or where both input and output data from the actual system is available. Three approaches for developing a valid model based on experts can be applied: showing the model, Delphi technique and consensus (Danielle, 2011).

Showing the Model involves developing the model first and then subjecting it to the experts for evaluation. While experts may be biased by the original model, this approach consumes lesser time for experts and analysis of results of questionnaires or interviews is easy.

Delphi technique involves three iterative rounds. In the first round, each expert is asked to independently list model components. In the second round each participating expert is provided with the list of components identified by other experts and then asked to draw a model based on them. The researcher aggregates all the models from the experts. In the third round, the aggregated model is given to the experts who are expected to give comments on it. While this approach removes bias associated with the previous approach, it consumes a lot of time for experts. Also, merging opinions from several experts which may be divergent can be difficult to the researcher.

Consensus involves inviting experts in a meeting to agree on a unique model. To the researcher, this approach is the simplest because one unique model results from the meeting. However, organizing all experts into one meeting has logistical challenges. Experts with dorminant personality may overshadow less confident ones.

2.7.9 Validation Framework for Simulation Models

An evaluation framework describes the environment, procedures and parameters used in determining the performance of a model. To evaluate a simulation model, an evaluation framework needs to be established.

Figure 2.10 shows a simplified view of how validation relates to the simulation model development as described by Sargent (2011).

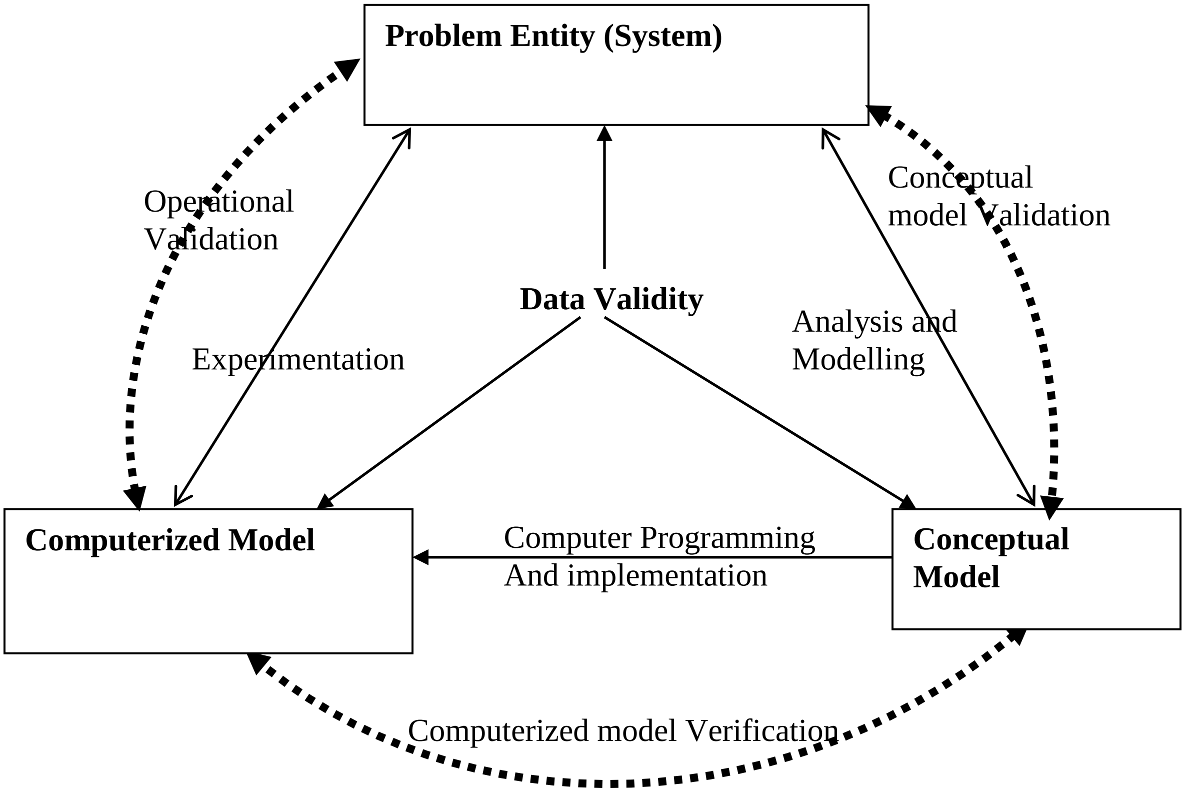


Figure 2.10: Link Between Model Development, Verification and Validation (Sargent, 2011).

The conceptual model is the mathematical or logical representation of the problem entity (system) and is developed for a specific study while the computerized model is the implementation of the conceptual model on a Computer. The conceptual model is developed through an analysis and modeling phase while the computerized model is developed through computer programming phase.

To be able to evaluate the model in relation to the problem entity, experiments are conducted on the computerized model. In all the three phases, building the conceptual model, validating the conceptual model and performing experiments with the validated conceptual model, appropriate, accurate and sufficient data is needed(Sargent,2011).

Various researchers have used different evaluation parameters and procedures. The dominant parameter observed from literature analysis is accuracy/correctness. However, there are no set of specific tests that can easily be applied to determine the ‘correctness’ of a model. In addition, no algorithm exists to determine what techniques or procedures to use (Sargent, 2011).

2.8 Related Works

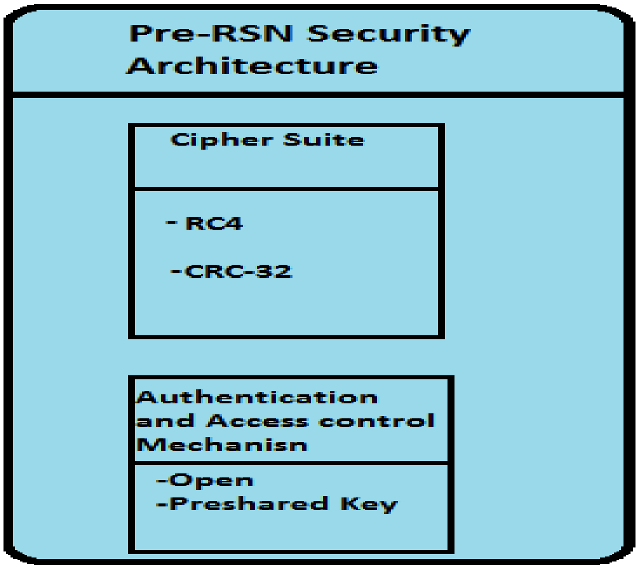
While the emphasis of the previous sections was on the background necessary to understand this work, this section discusses in detail, past efforts by researchers in trying to solve poor implementation of authentication and access control in large public WLANs.

2.8.1 Pre-Robust Security Network (Pre-RSN) Architecture

This was the first security implementation approach for WLAN Security. Designed by IEEE 802.11(1997), Pre-RSN architecture is characterized by a requirement to implement wired equivalent privacy (WEP) protocol. This security mechanism was designed to provide reasonable security strength that could leverage the security of a wired network against external attacks. While this solution initially appeared to have met its goal, it has since been established that its security features are very weak (Borisov et al, 2001; Gast, 2005; Pyshkin, Tews & Weinmann, 2007).

Despite its weaknesses, Pre-RSN WLANs are widely deployed in organizations like universities to allow students to connect to university’s hot spots (Alikira, 2012; Mwathi et al, 2016). A network discovery test conducted by Alikira (2012), established that 30% of the devices discovered were configured based on pre-RSN security features.

Figure 2.11 shows that pre-RSN model allows selection of RC4 as confidentiality protocol and Enciphered CRC-32 as the integrity protocol. In addition, it allows implementers to select from two authentication and access control mechanisms; open and pre-shared key. It therefore focuses on securing the wireless path between a client device and access point and therefore limited in scope.


Pre-RSN Security Architecture
Cipher Suite
- RC4
-CRC-32
Authentication and Access control Mechanisn
-Open
-Preshared Key

.

Figure 2.11: Pre-RSN Security Implementation Approach(IEEE 802.11,1997)

2.8.2 Wireless Group Network Policies Approach

This is a security features selection and configuration approach developed by Microsoft (2003). Consists of two subsystems; wireless module called wireless MMC snap-in which operates on the server side and where wireless group security policy settings are made. The other subsystem is wireless client side extension (CSE) which operates on the client side which pulls settings made on the server side to the client's registry.

Figure 2.12 shows the key components of Wireless Group Network policies approach. It has five components of WLAN security which are key to authentication and access control; wireless client, wireless access point, authentication server, authentication and access control mechanism and user database. Wireless network group policy approach allows security settings to be made on salient components of WLAN security and has the ability to enforce implementation of the set/configured security features on all client devices on a WLAN. However, besides being a proprietary design, it does not have a mechanism that can indicate the level of security provided by a particular set of security features and configuration on the security policy. Therefore an implementer cannot visualize the security level expected from implementing a set of security features and their configurations.

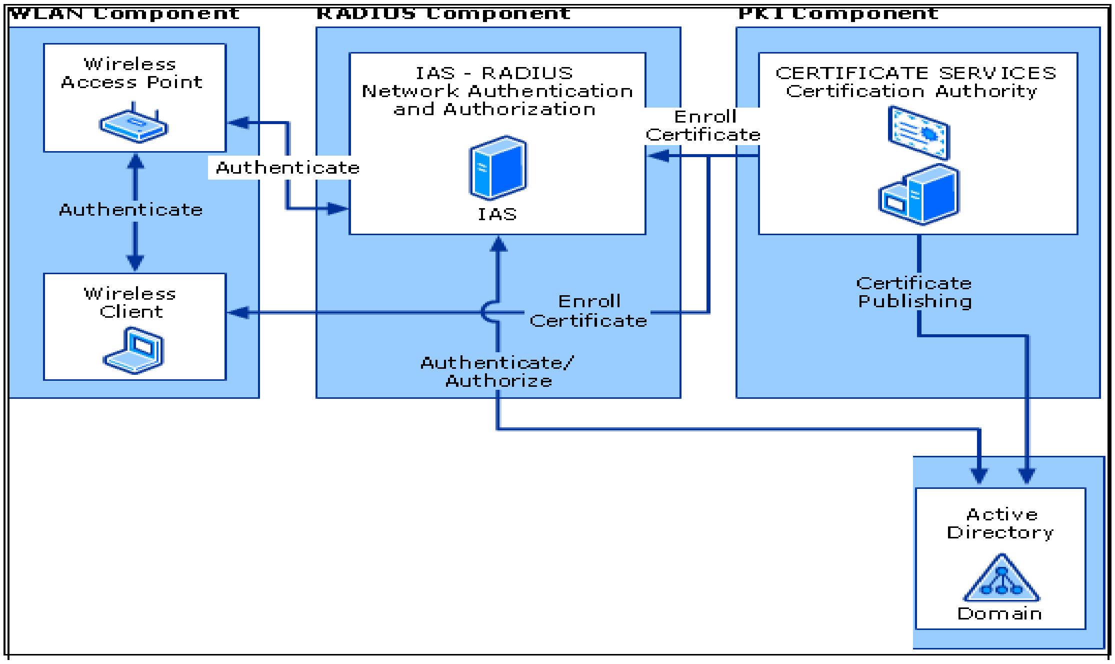


Figure 2.12: Wireless Group Network policies approach (Microsoft, 2003)

2.8.3 Robust Security Network (RSN) Approach

Robust security network (RSN) implementation approach was introduced by IEEE 802.11i (2004) enhancement. RSN provides enhanced authentication mechanisms for both access point and client station, session specific key derivation and management framework and enhanced data encryption .RSN architecture requires that all client devices on a WLAN should be configured with TKIP or CCMP cipher suites and should create pre-shared master key (PMK) security associations. It also requires implementers to configure access points to only support RSN associations (RSNA).

Although RSN allows selection of an EAP method for IEEE 802.1x authentication, there are many EAP methods with varying strengths and weaknesses. RSN however provides no guideline on how to select an EAP method for IEEE 802.1x authentication (Sheila et al (2007).This creates a possibility of choosing a weak authentication method or implementing a strong authentication method improperly.

Figure 2.13 shows that RSN security implementation model supports selection of RC4 or AES as confidentiality protocols while the integrity protocol is Michael MIC or CBC-

MAC. Authentication and access control mechanisms supported by RSN include pre-shared key and IEEE 802.1x with EAP.

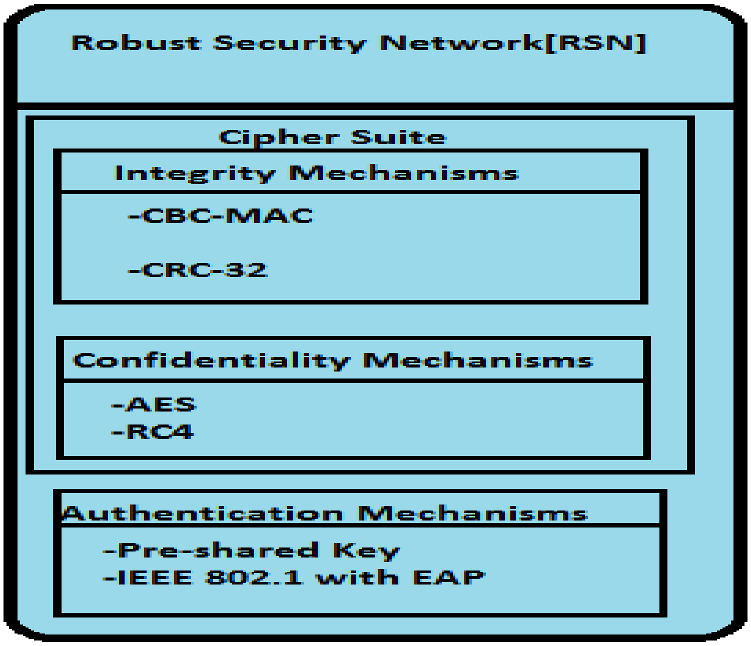


Figure 2.13: RSN Security Implementation Approach(IEEE 802.11,2004)

Unlike wireless group network policies approach, RSN is limited in that it does not provide any mechanism of selecting and/or configuring security features of important components like user database, authentication mechanisms, authentication server, client drivers or client utility.

2.8.4 Mechanism for Selection of an EAP authentication Method for a WLAN

Khidir and Owens (2007) proposed a mechanism to guide selection of EAP authentication methods based on four considerations; security level provided by the EAP method, possible attacks in a particular environment, existing network infrastructure and upgrade strategy. While the proposed selection approach takes into consideration important parameters(Khidir & Owens, 2007) only focus on EAP methods selection and fail to consider important configuration requirements relating to the EAP method selected e.g. client utility configuration to support EAP methods and selection strategy of appropriate cipher suite that would match the level of protection provided by the selected EAP method. The EAP selection approach also fails to consider more secure EAP methods such as EAP-flexible authentication via secure tunneling (EAP-FAST) which was developed as an improvement on LEAP to be implemented in environments where there are difficulties in enforcing password policy.

2.8.5 An Approach for Selection of EAP Authentication Method Based on its Security Features

Kwang-Hyun et al (2004) proposed eight EAP features that should influence an implementer into selecting an EAP authentication mechanism. These features are; mutual authentication, identity privacy, dictionary attack resistance, replay attack resistance, derivation of strong session keys, tested implementation, delegation, and fast reconnect.

Mutual authentication requires that an EAP method should enable both client device and authentication server to authenticate each other**.** Borisov et al (2001) showed that the absence of mutual authentication in WEP based authentication was responsible of many of its weaknesses.

Identity privacy means hiding the client's identity e.g. username from sniffers of the authentication process. However, identity does not mean Media Access Control (MAC) address since hiding such information would require major changes to the IEEE 802.11 WLAN standards. An EAP message flow starts with the Request-Identity from the server followed by Response-Identity message from the client device. Because these two EAP messages are sent before establishment of encryption keys they are not encrypted. This provides an opportunity for an attacker to sniff the communication in the beginning of the authentication process with an aim of discovering the client device’s identity. When selecting an EAP method, an implementer needs to establish whether protection of client identity needs to be hidden from sniffing.

An EAP method should be able to resist dictionary attacks. In such attacks, the victim must have some potentially guessable secret e.g. a password which the attacker only needs to verify or the attacker may have access to some data algorithmically derived from the secret from which to pre-compute a dictionary of likely passwords.

An EAP method should resist replay attacks by incorporating a nonce, a timestamp or a sequence number in the data frames exchanged during authentication process so that the parties doing the authentication can detect a frame that had previously been received.

Replay attacks can be executed even in the absence of attacker knowledge on the secret key required for the authentication process.

An EAP method should derive secret key that an attacker cannot derive after sniffing several messages encrypted it. To derive strong keys, a good authentication method should derive a unique key for client and access point in every session.

Tested Implementation means that the design and implementation of authentication protocol need a rigorous security analysis and its limitations need to be thoroughly understood for it to be used with confidence. If the authentication protocol is new, the protocol is likely to have more flaws in its design and implementation than existing protocols that have been tested.

An EAP method should have ability to enable valid users to delegate their right to access a WLAN to preferred parties e.g. guests in a conference (Goffee et al, 2004) .This solves the problem of creating one account for all guests which poses its own security issues or creating many temporary accounts. An EAP method should support fast reconnect to forestall a possible denial of service that occurs when a previously authenticated client device is forced to re-authenticate to another access point in the same WLAN after it disassociates with the access point that brokered the initial authentication.

While this approach is realistic for the intended purpose, it is narrow because it focuses on only EAP methods and ignores other aspects of WLAN authentication such as cipher suite, configurations on the client utility as well as authentication server.

2.8.6 Comparative Based Approaches to EAP Methods Selection

Many researchers have analytically compared various EAP methods based on key implementation parameters. This is done so that implementers may be able to choose a suitable EAP method based on desired features. Khidir and Ali (2011) present comparative study results of six key EAP authentication methods namely: message digest 5(MD5), transport layer security (TLS), tunneled transport layer security (TTLS), protected extensible authentication protocol (PEAP), lightweight extensible authentication protocol (LEAP) and flexible authentication via secure tunneling (EAP-FAST). The analysis is based on the following parameters; authentication attributes, deployment difficulties, dynamic re-keying, requirement for server Certificate, requirement for client certificate, tunneled, WPA compatibility, level of WLAN security and Security risks (attacks) associated with a method.

Kshitij et al (2013) in another study compares the same authentication methods based on the following parameters; implementation technique, authentication attributes, deployment difficulties, dynamic key delivery, server certificate requirement, supplicant certificate, tunneled, WPA compatibility, WLAN security level and vulnerabilities (attacks) associated with a method.

Umesh et al (2014) gives a detailed study of some of the commonly used EAP methods which include; MD5, LEAP, TLS, TTLS and PEAP. All these studies show that EAP supports a variety of upper layer authentication protocols each having its strengths as well as weaknesses.

The comparative approach helps implementers to choose between a suitable and unsuitable authentication methods. The detailed explanation of these methods makes it easy for implementers to understand them. However, these researchers address EAP methods in isolation without considering other security features that interact with these EAP methods. Therefore, while these comparative approaches help implementers to choose between suitable and unsuitable authentication methods, none of these approaches is able to provide a simulation that can enable an implementer to visualize the security level expected from implementing a set of security features and their configurations.

2.8.7 An Approach for Selection of Cipher Suite Based on its Features

Sheila et al (2007) proposes the following features for selection of appropriate cipher suite to support WLAN authentication and access control: core cryptographic algorithm, key sizes, per packet key, integrity mechanism, header protection, replay detection, authentication supported and mode of key distribution.

Core cryptographic algorithm refers to the algorithm on which encryption of authentication traffic is based on. IEEE 802.11i (2004) defines two encryption algorithms namely RC4 and AES.

Encryption key size refers to the number of bits on the encryption key which determines the strength of the algorithm from attacks associated with cryptoanalysis. The algorithms specified in IEEE 802.11 have 40,104 or 128 bits. Use of per packet key also reduces the risk of cryptoanalysis.

Integrity mechanism refers to the protocols in a cipher suite that secure authentication traffic from unauthorized modification. Integrity protocols specified under IEEE 802.11 are CRC-32, Michael MIC and CCM.

Replay detection refers to whether or not a cipher suite has inbuilt mechanisms to detect replay attacks. Header protection refers to whether the cipher suite used during authentication supports encryption of header information or not.

Authentication supported refers to the authentication mechanisms that can use the cipher suite used .Key distribution method is the mechanism used to distribute the encryption key to the access point and to the client device. The method used to distribute the key determines how secure the encryption key will be from unauthorized access. IEEE 802.11i (2004) provides two mechanisms of key distribution, manual (static) or dynamically using IEEE 802.1x mechanism.

Based on this criterion, (Sheila et al, 2007) places WEP as the least secure cipher suite, followed by TKIP and CCMP as the most secure. While Sheila et a l(2007) have addressed the issue of cipher suite selection, the approach is narrow because it attempts to address a small piece of what constitutes WLAN authentication and access control implementation.

2.9 Gaps that Need to be Addressed by the Proposed Solution

This research aims to make a contribution by addressing the following gaps identified after review of the literature.

(i) The flexibility of the provisions of IEEE 802.11i (2004) and IEEE 802.11w (2009) security standards create potential for selection and configuration of vulnerable cipher suites, authentication & access control mechanisms, end user and server system security features.

(ii) Previous approaches to WLAN authentication and access control implementation lack important security components and therefore none is comprehensive enough to address many security issues related to authentication and access control implementation.

(iii) Besides having several attacks discovered through various experimental team based approaches that try to compromise a WLAN, severity of these attacks has not been studied. Knowledge of severity of an attack is particularly necessary because it helps determine priority of response through selection and configuration of security features that are consistent with the priority.

(iv) While comparative approaches help implementers to choose between a suitable and unsuitable authentication methods, none of these approaches is able to provide a simulation that can enable an implementer to visualize the security level expected from implementing a set of security features and their configurations.

(v) No application system-level approach currently exists that can indicate the level of security provided by a particular WLAN authentication and access control implementation. Additionally, no research has been reported on simulation model based approaches to WLAN authentication and access control implementation.

Based on related works discussed above, there are major gaps or potential improvement areas in the approaches for implementation of authentication and access control in a public WLAN. This research therefore dedicates its effort towards development of concepts, components and algorithms required for realization of a model based approach for implementing authentication and access control in a public WLAN.

2.10 Conceptual Architecture

Informed by related works on WLAN authentication and access control implementation, provisions of IEEE 802.11 standards and protocols, known attacks and vulnerabilities to WLAN security and attack tools as discussed in this chapter, the researcher developed conceptual architecture for this research. The model architecture is based on Trusted computing base(TCB) concept discussed in this chapter in section 2.7.6.Trusted computing base is a set of all hardware, firmware and software components of a computer system that are critical to its security such that any vulnerabilities occurring inside a TCB component negatively influences the security level of the entire system. Trusted computing base components in this model are; Client utility, Client driver, Access point utility, Authentication server, Authentication & access control Mechanism and User database system.

Secure trusted communication path between trusted computing base components is a functional requirement of TCB concept. Therefore, any vulnerabilities relating to a path between trusted computing base components similarly influences negatively the security level of the entire system. The most salient path between TCB components is the wireless path between the wireless client and access point. The components of wireless path in this model are; Cipher suite and Authentication credentials.

WLAN authentication and access control security [WAACS] which is a measure of the overall security strength provided by a WLAN implementation is therefore influenced by eight components/artifacts; Cipher suite, Authentication credentials, Client driver, Client utility, Access point utility, Authentication server, Authentication & access control Mechanism and User database system. The eight artifacts are the key sources of vulnerabilities which may lead to security attacks in a WLAN after or during authentication and access control. Client utility, Client driver and access point Utility constitute the client side of security artifacts(Front-End system software) while Authentication server, Authentication & access control Mechanism and User database system constitute the sever side of security artifacts during authentication and access control(Back-End authentication systems).

The wireless path between client device and access point is a key element because it is prone to major security threats. Cipher suite and authentication credentials selected and configured during authentication and access control determine its security.

While the trusted computing base concept was originally used in design of operating systems security (Rushby, 1981; Hohmuth et al, 2004; Klein et al, 2009), this research has adopted the concept for use in WLAN authentication and access control implementation. Figure 2.14 shows the WLAN authentication and access control security [WAACS] conceptual architecture. The model clearly separates the concepts and artifacts highlighting how the model artifacts are linked/related.

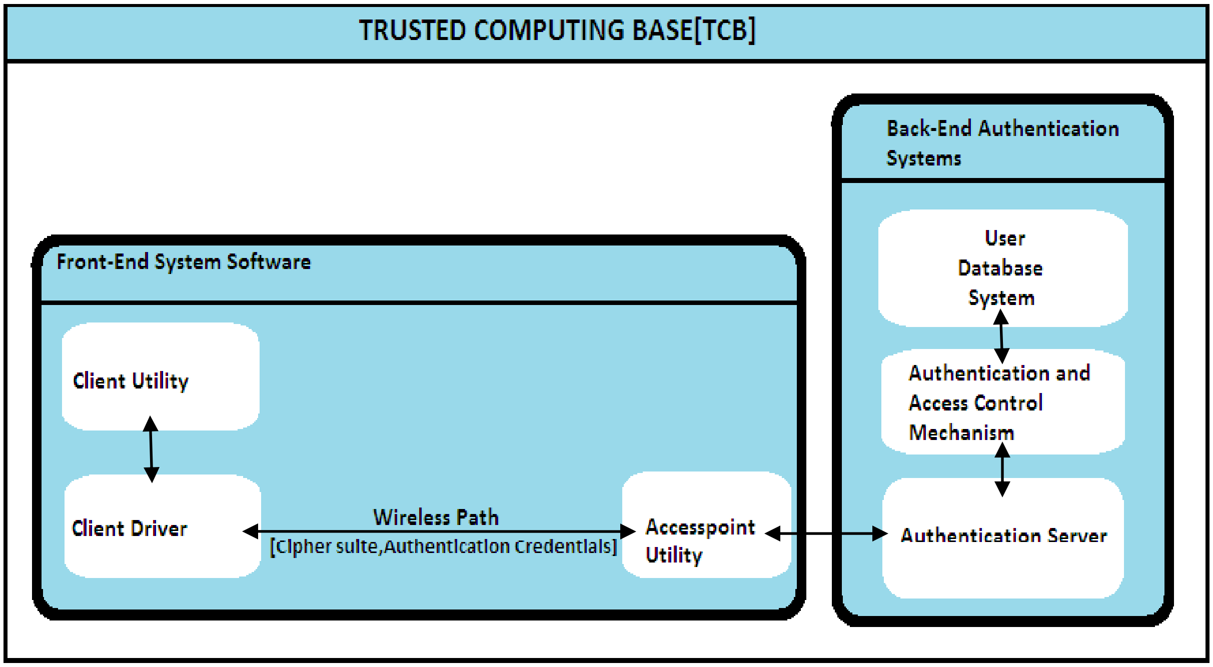

TRUSTED COMPUTING BASE[TCB]
Front-End System Software
Client Utility
Client Driver
Wireless Path
[Cipher suite,Authentication Credentials]
Accesspoint Utility
Back-End Authentication Systems
User Database System
Authentication and Access Control Mechanism
Authentication Server

Figure 2.14: WAACS Conceptual Architecture

The sections that follow provide a detailed description of the artifacts/components in the conceptual architecture.

2.10.1 Cipher Suite

Refers to cryptographic algorithms used to encrypt messages as well as perform integrity check for possible modification of messages between a wireless client device and access point. The strength of cryptographic algorithms implemented impacts on security of authentication traffic exchanged on the wireless path between a client device and access point.

2.10.2 Authentication Credentials

Refers to the messages delivered to the authentication server or provided by the authentication server and used to verify a claim by an entity (client or server) that it is authorized to act on behalf of a known identity. The nature and type of authentication credentials exchanged between a client device and access point impacts on the security of the wireless path.

2.10.3 Client Utility

Client utility refers to utility software (also called supplicant) running on the client machine and that communicates with access point firmware/utility. Whenever a client utility is misconfigured e.g. a client device configured not to support management frame protection or where support is optional, then connection by the client device to a WLAN without protection for management frames is possible. This has potential to cause security breaches such as disassociate and de-authentication attacks (Scott, 2011). Many WLAN users configure their client utility to ignore validation of authentication server certificate and the specific authentication server address (name) verification. Additionally the client utility is also configured in such a way that users can choose the server that is the source of the certificate (Mwathi et al, 2016).This has potential to cause RADIUS certificate attacks.

2.10.4 WLAN Client Driver

WLAN Client driver refers to the WLAN device driver implemented on the client Machine. Device drivers are key sources of security vulnerabilities in modern operating systems (Ken, Dawson & Engler, 2002).Although protected by security mechanisms such as personal firewalls, anti-virus and host intrusion prevention systems, the mechanisms are ineffective in handling WLAN driver attacks. This is because drivers run with kernel privileges and therefore the attacker targeting WLAN drivers is able to run code with kernel privileges (Laurent & Julien, 2008).

Compared with other kernel code, drivers experience higher error rates making them the most poor quality code in most kernels (Andy, Junfeng, Benjamin, Seth, & Dawson, 2001). The fact that the device driver code is developed by programmars who may not possess deep knowledge of the target operating system kernel is one factor that contributes to the high error rate (Tal, Ben, Jim, Mendel & Dan, 2003).Drivers for wireless interface cards, most of which conform to IEEE 802.11 standards are easy to interact with and potentially exploit if the attacker is within the radio range of the client device (Jason et al, 2006).The high availability of IEEE 802.11 devices, the ease of driver interaction and possibility of poor quality driver code creates potential for an attacker to fingerprint a device driver and consequently launch a driver-specific exploit (Laurent & Julien,2008).

IEEE 802.11i does not provide an explicit algorithm to be used by client device drivers to scan (probe) for access point. Therefore, developers of device drivers develop and implement their own probing mechanism. Since various WLAN drivers have their specific probing algorithm it is easy to identify a driver based on the unique scanning approach it employs. Once identified its vulnerabilities may then be exploited.

Security features and configurations of a WLAN driver implemented on wireless client Machines therefore impact on the authentication and access control security

2.10.5 Access Point Utility

Refers to the security features and configurations of system software running on the access point and/or WLAN controller. Access point is a device that authenticates client devices or may be configured to act as an authenticator passing authentication information to a separate authentication server. Access point broadcasts its security capabilities using two approaches (Sheila et al). The first approach is through beacon frames sent from access point’s specific channel and the other one is through a probe response frame. Security capabilities of beacon or probe response frames are contained in robust security network information element. Client devices configured to managed mode can therefore discover available access points and their corresponding security capabilities by actively probing every channel while those in monitor mode will passively monitor the beacon frames from the access point.

Many access point utility/firmware are configured not to support management frame protection such as authentication requests (Eian, 2009).An adversary can install his/her own access point with a spoofed MAC address, spoofed SSID, configured with appropriate freeware e.g. HostAP and with a strong signal to fool a client device into associating with it and leaking credentials or private data (Park & Dicoi, 2003).

2.10.6 Authentication Server

Refers to the protocol employed by the server application (IEEE 802.1x enabled or non-IEEE 802.1x) that processes authentication requests from the client utility (Rigney, Willens, Rubens & Simpson, 2000). While there are many authentication servers, different authentication servers support varying authentication and access control methods. The two main protocols standardized by IETF through RFC and used for WLAN authentication are RADIUS and DIAMETER. While DIAMETER provides end to end authentication, RADIUS authentication of the entity is hop by hop and not end to end. DIAMETER'S end-to-end security framework provides message origin authenticity even when there are relays or proxies present (pat et al, 2002).On the other hand, because of the RADIUS hop-per-hop shared secrets and changing identifiers, all proxies must be able to read and modify any message. Proxies also may or may not send proxy-state attributes from the client side to the remote server, and they may need to modify other attributes to enforce a local policy. Thus the messages may change when travelling through the proxies, which make the entire data authentication, integrity and confidentiality support difficult (Rigney et al, 2000).

While both protocols offer some protection against replay attacks ,DIAMETER is more secure than RADIUS because it uses some kind of transport layer security scheme, such as IP Security or TLS which guarantees replay protection(Pat et al,2002).On the other hand, IP security support for RADIUS is optional. Whereas DIAMETER server is allowed to initialize messages e.g server re-authentication, RADIUS server cannot initiate messages. Only its client can do so.In RADIUS, all user passwords are always sent encrypted. However, password is the only part of the packet that is encrypted and that neither the RADIUS specification nor the RADIUS extensions provide support for whole packet confidentiality (Rigney et al, 2000).

While RADIUS uses unreliable, best effort delivery UDP for transport, DIAMETER uses TCP or SCTP at transport layer which are reliable (Li-chuan et al, 2009).Use of a reliable transport protocol enables DIAMETER to have an error reporting mechanism such that its messages are only discarded when there is no other suitable way to solve the problem. This is unlike RADIUS which stops any further processing and discards/drops packets whenever any fault occurs causing denial of service.

Other AAA protocols that may be used for authentication include; Terminal access controller access control system (TACACS), Enhanced Terminal access controller access control system (TACACS+).However, these standards have not been standardized by IETF through RFC.

2.10.7 Authentication and Access Control Mechanism

Refers to the specific approaches used to verify the claim that an entity is allowed to act on behalf of a given known identity in order to access wireless LAN. The approaches also restrict the right of an entity to accessing a WLAN until the entity is verified and cryptographic keys established.

2.10.8 User Database Architecture

User database refers to the configuration and database architecture used to store information used to verify user identities during authentication. User Databases stores user names and password or MAC addresses (Charlie & Benjamin, 2011). Examples of user databases include: Microsoft’s active directory/LDAP, access point internal database, local flat text file, relational database file e.g. SQL or MySQL database.

The attacks targeting user database are mainly denial of service attacks. These attacks target situations where the database resides in the access point or when MAC address filtering is used for access control .In other cases, the database server may be on a dedicated server but due to centralized architecture, the server’s resources are consumed by malicious and sometimes distributed authentication requests.

When WLAN user database is implemented on an active directory, it will constantly be inundated with new queries from various applications which will make WLAN DOS attacks successful(Charlie & Benjamin,2011).Examples of known attacks on user database include database server denial of service(DOS), distributed flooding, authentication flooding and injection attacks(Bellardo & Savage,2003).

2.11 Conclusions from Review of Related Work

This chapter has brought into perspective the challenges that need to be addressed in order to solve the problem of selection, design and configuration of security features for WLAN.A generic conceptual model that can handle most of the challenges encountered in implementing WLAN authentication and access control has been arrived at.

There were two broad sources from which the researcher obtained theoretical underpinning and components for this study; related works, IEEE 802.11 standards, IEEE 802.11 based protocols, analysis of attacks made by experimental team based approaches and careful analysis of theoretical concepts on published research related to WLAN security implementation.

The researcher summarized, analyzed and integrated the findings from the literature review in order to articulate the gaps in knowledge and shortcomings or merits of previous approaches/methods and also to provide theoretical underpinnings for the new study that justify the conceptual model. In order to actualize the conceptual model into a concrete architecture and develop a prototype capable of giving indicative performance, some important data needed to be collected. Additionally procedures to collect this data were designed, developed and implemented. The determination of this data and procedures is detailed in the next chapter.

CHAPTER 3: METHODOLOGY

This chapter provides the details of various research strategies and specific research actions geared towards the design of a model that enables design or selection and configuration of security features for WLAN authentication and access control in a public WLAN. A comprehensive analysis of resources selected, methods, tools and techniques for data gathering, analysis, model development process and validation is provided.

3.1 Overview of Issues to be Tackled

The main objective of this research was to develop and prototype a model that facilitates implementation of WLAN authentication and access control security in the context of large public WLANs such as universities. A conceptual architecture was introduced and discussed in detail in section 2.10 .However, the conceptual architecture is a high level design that only identified key architectural artifacts/components that security in a WLAN depends on during authentication and access control. In order to actualize the conceptual model into a concrete architecture and develop a prototype capable of giving indicative performance, some important issues needed to be tackled. The issues are as follows:

i. Discovery of security features and configurations on each architectural component
ii. Analysis of attack susceptibility of security features and configurations
iii. Development of model value function tables and algorithms.
iv. Validation of the model for its intended purpose over the domain of its intended applicability.

The above issues formed the basis for this research. Each of these issues/tasks was tackled through a specific research procedure.

3.2 Research Design Synopsis

The following is a synopsis of the research design applied for each of the four tasks listed in section 3.1 above. A detailed description of each research activity is given in the respective sections that follow. Descriptive survey research design complemented with published sources was adopted for informing the security features and configurations discovery envisaged in item i of section 3.1.

Literature survey and analysis was adopted for analysis of attack susceptibility of security features/configurations (item ii of section 3.1).

Results of descriptive survey design as well as literature survey and analysis were used to develop model value function tables and algorithms envisaged in item iii of section 3.1.

Validation envisaged in item iv of section 3.1 was conducted through an evaluation survey where the model was validated through expert intuition/opinion and complemented with theoretical analysis.

3.3 Research Design of Security Features and Configurations Discovery

The study which generated both qualitative and quantitative data employed descriptive survey approach. This was necessary in order to collect data about what actually exists in real implementations. A survey was carried out on identified cases. Through the survey, the researchers wanted to discover security features and configurations implemented in various public WLANS. The security features were then analyzed against published sources to establish the implementation specific issues that may contribute to poor WLAN authentication and access control security performance in selected University WLANs in Kenya.

Descriptive survey is chosen in this research because descriptive designs enable data collection from a small, as well as large number of people (Swatzel & Jennings, 2007).The method helps in collecting information by interviewing or administering questionnaire to a sample of individuals (Orodho 2003).

Synthesis of literature in chapter 2 established that each of the known attacks on WLAN targeted one or more of the vulnerabilities in the following components; authentication credentials, cipher suite, client utility, client driver, accesspoint utility, authentication and access control mechanism ,authentication server and user database. The researchers therefore used the components as base parameters for the study. Important issues put into consideration while collecting data included; what data was collected, how it was collected, when and where the data was collected, why it was collected and who it was collected from.

3.3.1 Target Population and Sampling Strategy

The researcher carried out the survey in Universities and University colleges in Kenya. This is because the research was seeking to develop a model that facilitates implementation of security features for WLAN authentication and access control in public WLANS such as those in these Universities. When the survey was conducted, there were a total of 53 accredited universities and university colleges (Commission for University education, 2013). The survey was however to be conducted in universities and university colleges where WLANs had been implemented.

Before the survey was carried out, a pre-study was made to establish universities where WLANs were in place. One previous e-readiness study conducted by Kashorda and Waema (2013) had identified 30 universities and University colleges in Kenya that had implemented WLANs. The study had particularly found that on average 52.8% of students in those universities own a laptop while 53.3% own a smart phone. This was an indicator of a large pool of WLAN devices in use in those universities.

The researcher therefore identified all the 30 universities for inclusion in the target population (see the list in appendix 14).In addition the researcher investigated the other remaining universities and identified 10 more universities that had WLANs in place and also included them in the target population. This brought the target population to fourty. The target population was therefore small and so the researcher included the entire target population in the sample. For each university sampled, an ICT director or one senior network/system security administrator was selected for the survey.

3.3.2 Research Instruments

This survey used questionnaires and Observation checklists to obtain primary data from subjects. The questionnaires had been developed with due consideration of the published and current body of knowledge in WLAN security. They were closed type of questions to get specific or hard fact information and open ended questions to capture opinions of respondents. The subjects completed the questionnaires and thereafter were collected by the researcher. Observation checklists were used to record security configurations on the end user devices.

3.3.3 Pretesting the Instruments

Right from the first draft of the instrument to the final one, consultation and review by a number of experts in the area of computer and network security was sought. Once the questionnaire and checklist were finalized, a pilot test of the instruments was done whereby they were distributed (pre-tested) to 10 colleagues at work and professionals in the field of Computer and network security. They were requested to provide useful suggestions especially on appropriateness, structure and relevance of the questionnaires for the study. They were also requested to assess the clarity of the questions, duration it would take to have a respondent respond to all the questions. This provided an idea of the data collection process. Their suggestions were incorporated into the instrument to improve its reliability.

After adjustments, the instrument was tested again with 5 subjects and another iteration of improvement based on their comments followed. In this iteration, the emphasis was on improving the content validity and consistency. While content validity checks whether the instrument covers an acceptable content of applicable domain issue to be measured, consistency checks that there is correspondence between the instrument items and the concept.

3.3.4 Data Collection and Analysis Strategy

Questionnaires were delivered to respondents physically or through an email, were filled and either physically collected or emailed back. The researcher also visited the Universities and recorded observations on user device configurations on a checklist.

Completed responses from questionnaires were checked for completeness, consistency, viability and accuracy before processing them. Before processing results, the researcher examined the raw data carefully to gain insights into the findings of the survey.

Quantitative as well as qualitative data was collected and analyzed. Respondents were coded to hide their identities. Using statistical package for social scientists (SPSS), the numerical/quantitative results were aggregated and analyzed using descriptive statistics based on the conceptual model architectural components. The numerical results are then presented in tables and graphs and accompanied with written explanation and analytical discussions. The discussion provides insights on the results by adding knowledge that the researcher gained that is not in those results. What is learned from the research is clearly stated.

Qualitative data collected through open ended questions was analyzed by identifying various themes from the content of the responses. A coding system was used to identify content about different themes. The responses were then organized into themes and concepts and presented as summaries that represent the key points emerging from the data. The data collected via observation checklists complemented the questionnaire responses.

3.4 Attack Susceptibility Analysis of Security Features

This involved literature survey and analysis research design. Attacks and vulnerabilities exploited by the known attacks were identified from the literature. Articles from peer reviewed journals, white papers, conference papers, technical reports or part of the standards literature that is emerging in the area addressing known WLAN authentication and access control attacks on cipher suite, authentication credentials, end user and server system softwares that implement various security in WLANS were used. Exhaustive search was employed i.e articles were searched and picked from various sources and databases matching the inclusion criteria above. The scope of the literature analysis extended from most current to 2001 when the first serious paper on WEP insecurity was presented (Borisov et al, 2001) and the limiting factor was the natural limit to the effort the author spent on collection. Work that clearly diverged from operational WLAN security was not taken into account as well as papers that offered highly specific analysis not related to computing and information security in operational settings. Redundant articles were discarded e.g where the same or very similar attacks appear in more than one publication, often by the same (or common subsets of) authors that have gradually extended a concept.

3.4.1 Data Collection and Analysis Strategy

(a)From literature sources:

(i) Attacks targeting authentication and access control mechanisms, cipher suites negotiated during authentication and access control, credentials used for authentication, end user system software and server system software that implement authentication and access control in a WLAN were identified.

(ii) The security features and configurations that contribute to each of the identified attacks together with the vulnerabilities in them that lead to realization of the attack were established.

(iii) The set of tools used to launch each of the identified attacks were established.

(b)Model the attacks on an attack tree using attack tree methodology.

The attack tree methodology earlier presented and discussed in detail in section 2.7.3 was used to model the attacks targeting security offered by WLAN cipher suites, authentication & access control mechanisms, end user and server system software used in WLAN authentication and access control. The modeling was done as follows:

(i) Each of the eight artifacts/components in the conceptual architecture became a root forming a separate tree

(ii) All identified attacks against an artifact were added to the respective tree with the vulnerabilities for each attack becoming children of the respective attack. Each attack was mapped to a security feature(s) or configuration(s).

This process was repeated for all the eight artifacts/components consequently generating eight attack trees.

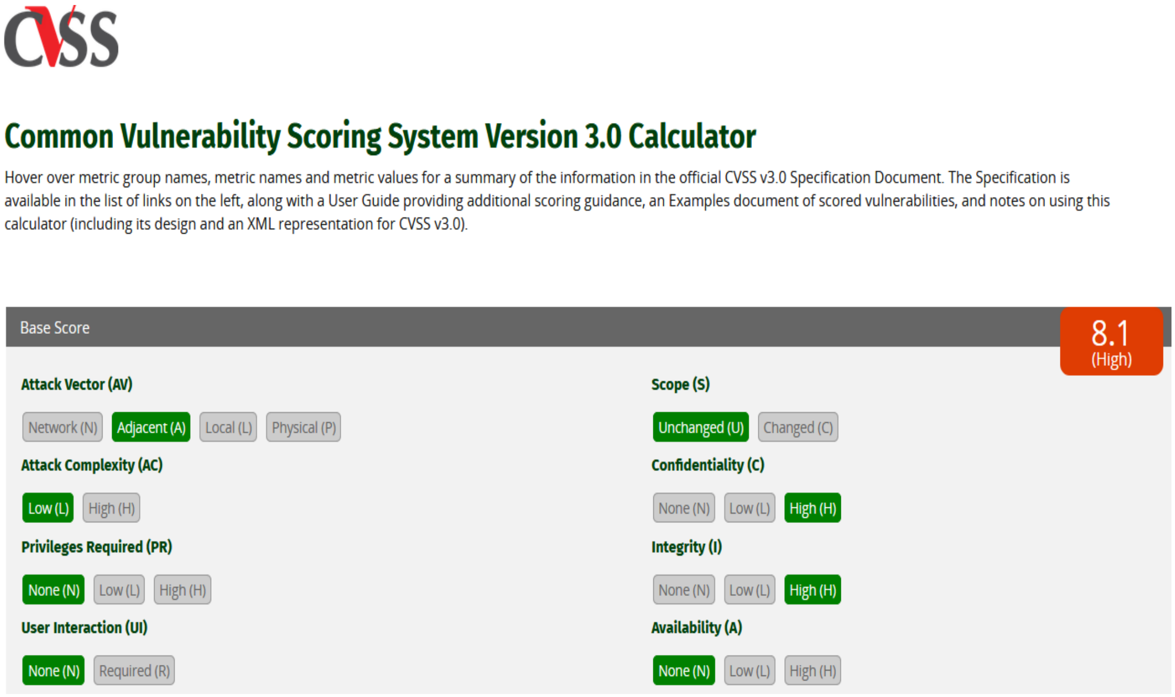
(c) Vulnerability Analysis/Attack Susceptibility of Security Features

From the literature sources, the vulnerability characteristics of each of the identified attacks on each attack tree/artifact in section 3.4.1b were studied and analyzed based on common vulnerability scoring system (CVSS) base metrics. The CVSS base metrics, earlier presented and discussed in detail in section 2.7.4, include; attack vector (AV)**,** attack complexity (AC)**,** privileges required (PR)**,** user interaction (UI)**,** scope(S), confidentiality impact (C), integrity impact (I) and availability impact (A) .The analysis was done as follows:

(i) For each attack, a value is picked for each of the eight CVSS metrics. Detailed tables that guide one to fully understand how to pick correct values for a given vulnerability or attack and how to interpret CVSS scores are presented in appendix 5.

(ii) The values picked for each attack were then entered into an online CVSS calculator whose interface is shown in figure 3.1.

For every attack, the online calculator developed by FIRST (2014) allows a user to enter a value for each of the eight metrics. Based on values entered for each metric by a user, the calculator then implements a CVSS algorithm that generates a score for each value and an overall CVSS score for the attack. Since the vulnerability characteristics of each attack are intrinsic to a security feature or configuration, the overall CVSS score represent attack susceptibility of the associated security feature or configuration. This process was repeated for all the attacks in each tree/artifact and the scores presented in form of tables.



Common Vulnerability Scoring System Version 3.0 Calculator

Hover over metric group names, metric names and metric values for a summary of the information in the official CVSS v3.0 Specification Document. The Specification is available in the list of links on the left, along with a User Guide providing additional scoring guidance, an Examples document of scored vulnerabilities, and notes on using this calculator (including its design and an XML representation for CVSS v3.0).

Base Score 8.1 (High)

Attack Vector (AV)

Network (N) [✓ Adjacent (A)] Local (L) Physical (P)

Attack Complexity (AC)

[✓ Low (L)] High (H)

Privileges Required (PR)

[✓ None (N)] Low (L) High (H)

User Interaction (UI)

[✓ None (N)] Required (R)

Scope (S)

[✓ Unchanged (U)] Changed (C)

Confidentiality (C)

None (N) Low (L) [✓ High (H)]

Integrity (I)

None (N) Low (L) [✓ High (H)]

Availability (A)

[✓ None (N)] Low (L) High (H)

Figure 3.1: Common Vulnerability Scoring System Calculator (FIRST, 2014).

3.5 Model Value Function Tables and Algorithms Development

The data collected from preliminary studies described in section 3.3 and 3.4 led to the following

(i) Discovery of security features and configurations on each architectural component

(ii) Analysis of attack susceptibility of security features and configurations

The preliminary study results together with conceptual architecture presented in section 2.10 and literature sources were used to tackle the following issues pertaining model development:

(i) Designing of value function tables that map security features to security levels

(ii) Designing an algorithm for combining and propagating model input values

(iii) Designing an algorithm for EAP method selection

3.5.1 Design of Value Function Tables that Map Security Features to Security Levels

The vulnerabilities exploited to realize the attacks were either associated with specific security features or a to a certain configuration issue in the component concerned. Using CVSS, the severity of the vulnerabilities was established and then mapped to the related security feature or a configuration issue. These CVSS scores informed the security strengths assigned to various security features and configuration issues in the model by the value function. The value function which assigns a security feature /configuration to an attack susceptibility level relies on rational justification informed by results envisaged from CVSS analysis in section 3.4.1 which established the severity scores of vulnerabilities and attacks targeting these security features and configurations.

3.5.2 Design of an Algorithm for Combining and Propagating Model Input Values

An algorithm to propagate (combine) the component severity values and consequently compute wireless authentication and access control security was established. Approaches that could be used to perform the same role are weighed average, bayesian network and fuzzy logic. Unlike Bayesian network and fuzzy logic approaches which would allow an attribute (in this case a security feature) to have multiple categories with varying degree in each e.g. a security feature WEP could have weak, strong and medium components each component varying in degree e.g. weak (60%), medium (30%), strong (10%), weighed average approach exhibits pragmatism in assigning attributes to values e.g. WEP can be directly mapped to very weak because it is actually very weak. This justified the selection of this approach by the researcher. Additionally, weighted average approach has been applied in other related studies including (Danielle, 2011; Brookes et al, 2010).

An appropriate weighted average approach was designed for combining and propagating model input values by the researcher.

3.5.3 Design of an algorithm for Selection of EAP Method

Based on analysis of characteristics of various EAP methods in section 2.8.4, 2.8.5 and 2.8.6 and subsequent identification of gaps, an algorithm for selection of EAP method was developed to fill the gaps identified.

3.6 Prototype of the Simulation Model

In order to facilitate validation of the model, the model specifications were prototyped. The prototype was carefully designed and implemented as a web based application in order to be accessible and convenient to experts irrespective of their location (Amosa et al, 2015). JavaScript, html, CSS, java and e2glite expert system were the five software tools used to implement the model prototype.

JavaScript was used to implement scripts associated with the method for propagating parameters in the model.HTML and CSS were used for display style and associated formatting. The prototype of the algorithm for selection of EAP method was constructed using e2gLite rule based expert system shell. E2gLite is a free development toolkit (a 'shell'), developed by eXpertise2GO and is downloadable from http://www.expertise2go.com/webesie/e2gdoc/e2gmod2.htm. It is implemented as a Java applet. Just like any other compiled java program, the applet is embedded into a web page via a special HTML tag and is invoked from the web page via the HTML applet tag when needed.

The components that make up a knowledge base using e2gLite consist of three files: the e2gLite.jar file, the .kb file and the .html file. The e2gLite.jar file is the executable file which is actually the expert system shell. It consists of a set of class files which have all been packaged together as a Java Archive file known as e2glite.jar. The .kb file is the knowledge base which includes the goal, the rules by which the goal will be reached, and the questions (prompts) which the user must answer. The knowledge is represented in .kb file in the form of IF-THEN rules and its reasoning is by forward chaining. The .html file is used to provide an appropriate interface for the prototype because to use the expert system, a web page that loads the applet and identifies the knowledge base is needed.

3.7 Design of Model Validation

There is no single modeling approach applicable to all systems. Therefore, scientists build models that abstract important components of a system and just approximate those components that have lesser (or no) impact to their intended study (Stacewicz and Włodarczyk, 2010). If a model eliminates important components or over-emphasizes components with lesser impact, then the model will produce misleading outcomes (Stacewicz and Włodarczyk, 2010) Therefore models need to be subjected to validation/evaluation to test their correctness.

Balci (1998) explains that for a model to be valid, it must be checked to ascertain whether its behavior is satisfactory and that it is consistent with study objectives. A valid model is that which is a representation of the problem domain (Sargent, 2011).In other words, validation checks the accuracy of the model's representation of the real system. The process of validation gives the model an empirical basis.

Figure 3.2 shows a summary of the validation process which comprised three steps derived from Sargent (2011); Conceptual model validity, computerized model verification and Operational validity. Conceptual model validation was done after completion of the model design.

Conceptual model validation employed face validation and theoretical analysis (degenerate tests and traces) as the primary validation techniques as pointed out by Sargent (2011) .It was done to determine the following:

(i) Whether the theories and assumptions underlying the conceptual model are correct

(ii)Whether the model's representation of the problem entity, its structure, logic and mathematical causal relationships are "reasonable' for the intended purpose of the model.

Verification of the prototype was done to ensure that the computer programming and implementation of the conceptual architectural model is correct and bug free. The research employed structured walkthroughs (static testing) and traces (dynamic testing) as the primary validation technique as pointed out by Sargent (2011).

Operational model validation was done by providing the computerized model/prototype to domain experts mainly practitioners who were required to explore the model by performing some experimental tests and thereafter provide the model's accuracy for its intended purpose over the domain of its intended applicability on the questionnaires.

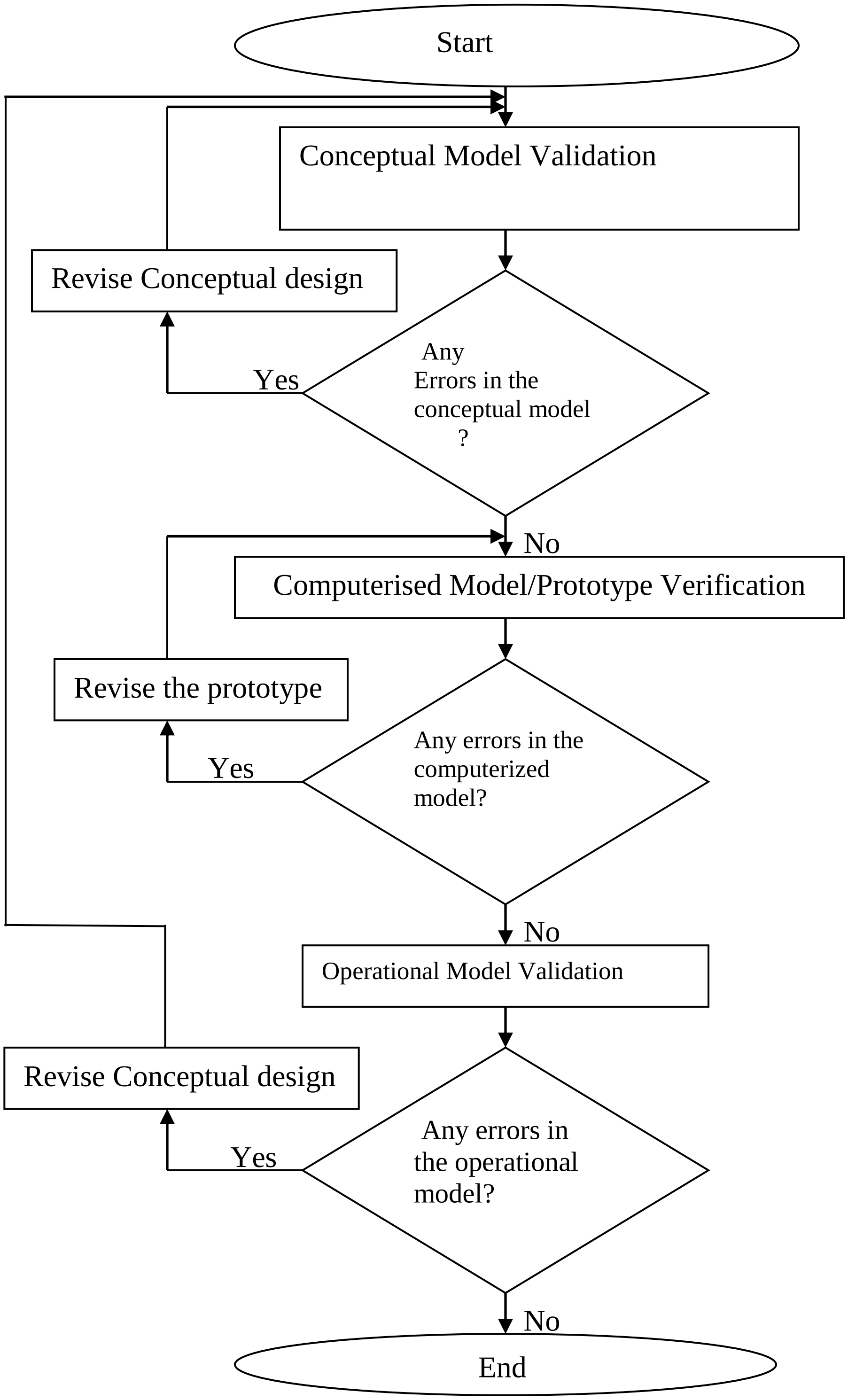


Figure 3.2: Summary of Validation process

3.7.1 Conceptual Model Validation Using Experts/Face Validation

Face validation involved checking whether experts belief that the model is correct for its intended purpose within the domain of its applicability. This provided a measure of suitability of the conceptual model in doing what it is meant to. In choosing the experts, the researcher was guided by knowledge of the expert in the key problem areas and experience both general IT and in the area of WLAN security (SANS, 2011)

3.7.1.1 Sampling strategy (Sampling Frame, Method and Size)

Experts (researchers and consultants) in the area of network security with high level of competence in WLAN security were used to evaluate the correctness of the model for its intended purpose within the domain of its intended applicability. These experts were mainly drawn from universities and industry. The experts drawn from the industry were linked with universities as external service providers. The choice of the experts was primarily based on the practicality of accessing experts with relevant expertise.

Chain sampling (snowball method or snowball referral) which is a form of purposive sampling was used to identify individual experts to validate the model. Chain sampling is used to identify cases of interest from the people who can identify others that are familiar with population cases that are information rich (Mugenda & Mugenda, 2003) where a referral network system is used to identify other sample units until an adequate sample size is achieved.

Chain sampling being a non-probabilistic sampling technique was suitable in this case because the referral aspect itself led to building confidence in the respondents who were required to possess certain characteristics such as all being involved in WLAN security research or have practiced in the area for a long period. Such population is hard to reach or hidden hence the need to apply this sampling method. In selecting the sample to use in the study, the researcher was guided by adequacy of the sample size, reliability and homogeneity of sample units. Through chain sampling, a sample of thirty (30) experts was identified for face validation of the model. Several studies including (Ashton, 1986; Batchelor & Dua, 1995; Briand, 1998; Danielle et al, 2011; Yaniv, 2004; Shirazi, 2009) argue on the number of experts needed. Whereas there is consensus that there is improvement in accuracy when many experts are used, the same is lacking on what expert limit is optimal. However, there is consensus that a natural limit exists where further increase in experts does not improve accuracy of the results. Chain referral being a type of purposive sampling method, the sample size was determined on the basis of “theoretical saturation” that is the point in data collection when new data no longer brings additional insights to the research questions**.** Theoretical saturation was however difficult to determine empirically and was rather subjective and therefore limited by practical reasons. The sample size was also bound by geographical reachability of the experts because there was need to physically get to where they were.

3.7.1.2 Research instruments and Data Collection Procedure/ Strategy

The researcher used guided questionnaires to collect data from the experts. The questionnaires had closed type of questions to get specific or hard fact information or open ended to capture opinions of the experts. Once the questionnaire was finalized, a pilot test (pre-testing) of the instrument was done by distributing them to 5 colleagues at work and professionals in the field of Computer and Network security. This helped provide useful suggestions especially on appropriateness, structure and relevance of the questionnaires for the study. It also helped to assess the clarity of the questions, duration it would take to have a respondent respond to all the questions which gave an idea of the data collection process. Their suggestions were incorporated into the final instrument which improved its reliability. After adjustments, the instrument was tested again with 5 subjects and another iteration of improvement followed. In this iteration, the emphasis was on improving the content validity and consistency.

Before giving out questionnaires, potential respondents would be investigated. For all the respondents, the researcher had one on one discussion to explain and demonstrate the details of the model and what was expected of the respondent. Thereafter, the respondents filled the questionnaires which were collected by the researcher. Some respondents filled the questionnaire and sent it via email.

3.7.1.3 Data Analysis

According to (FHI, 2012), purposive sampling is most successful when data review and analysis are done in conjunction with data collection. In this research, analysis was performed after every five questionnaires. Completed questionnaire responses would be edited for completeness, consistency, viability and accuracy before processing them.

Qualitative as well as quantitative analysis was used to analyze the data. Before presenting results, the researcher examined the raw data carefully to gain further insight into the results of the survey. Analysis of the validation results was expert by expert so as not to lose the insights from each expert that would happen if results are aggregated. Experts were coded to hide their identities. Then, the numerical results were aggregated. While various expert opinion aggregation approaches exist e.g. Bayesian(Morris ,1974, 1977), linear opinion pools (Stone,1961) , axiomatic (Morris ,1983, 1986) and simple averaging of individual opinions, many studies have suggested simple averaging of individual opinions as a method for improving the accuracy of predictions (Armstrong, 1985; Ashton, 1986; Hill,1982; Hogarth, 1978; Zajonc, 1962).

Therefore, this research employed simple averaging of individual opinions. The numerical results are presented in tables and graphs and are accompanied with a carefully written explanations and analytical discussion. The discussion provides insights on the results, adding knowledge that the researcher gained that is not in those results. What is learnt from the research is clearly stated.

Qualitative data collected through open ended questions was analyzed by identifying various themes from the content of the responses. A coding system was used to identify content about different themes. The responses were then organized into themes and concepts and presented as summaries that represent the key points emerging from the data.

3.7.2 Conceptual Model Validation Using Theoretical Analysis

Degenerate and traces validation was used to perform theoretical validation of the conceptual model. These tests were done to complement face validation tests on logic and mathematical causal relationships relating to propagation of security strengths in the model. Degenerate validation involved analysis of input values to test the corresponding changes in the internal components e.g. does the attack susceptibility go down when more secure configurations and security features are selected and vice versa? Does the security level/strength go down when highly susceptible configurations and security features are selected and vice versa?

Validation using traces on the other hand was done to determine whether the mathematical logic of the technique for propagation of values in the model maintains necessary accuracy and consistency. To achieve this, the researcher tracked entities' strength and type of influence through each sub-model and the overall model and analyzed the results using Ms-Excel spreadsheet.

3.7.3 Computerized Model/Prototype Verification

Structured walkthrough, traces (dynamic testing), degenerate tests and extreme condition tests were performed on the computerized model. The prototype was presented to other researchers in the team (Supervisors) who provided feedback on whether the prototype had been programmed and implemented correctly. The results/outputs of different types of specific entities in each sub-model were traced (followed) through the model to determine if the implementation of model's logic is correct and consistent.

Extreme condition tests for any extreme or unlikely combination of factors in the system were made by the researcher specifically to check whether the model provides useful results when extreme conditions are used. Degenerate tests were also carried out by analyzing input values to test the corresponding changes in the internal parameters e.g does the attack susceptibility go down when more secure configurations and security features are selected and vice versa? Does the security level/strength go down when highly susceptible configurations and security features are selected and vice versa?

3.7.4 Operational Model Validation Using Parameter Variability- Sensitivity Analysis

It is expected that individuals who are knowledgeable and experienced about the system being modeled (experts on the system) can estimate the directions and possibly "general values" of the magnitudes of the outputs/results from the system model(Sargent, 2011).The experts were therefore asked to perform parameter variability-sensitivity analysis and provide feedback on the accuracy of the model's output. Their feedback provided insights on the accuracy of the model in relation to that required for the model's intended purpose over the domain of the model's intended applicability.

3.7.4.1 Sampling strategy (Sampling Frame, Method and Size)

The knowledgeable practitioners who had participated in phase1 (preliminary survey) together with the researchers that had participated in conceptual validation were sampled. This was because of their involvement in the model development from early stages. They were complemented with other practitioners established through a chain referral system. This translated to a sample size of 50. For each one of them it had been established that they interacted with WLANs and its security administration and the networks they run are actively used. These conditions had been established via a pre-study survey and confirmed through a preliminary survey.

This being purposive sampling method, the sample size was determined on the basis of "theoretical saturation". However, theoretical saturation was difficult to determine empirically and was rather subjective and therefore, sample size was limited by practical reasons.

3.7.4.2 Research instruments and Data Collection Procedure/Strategy

The researcher used questionnaires to collect data from the experts after having given them time to explore the prototype features. The questionnaires had been developed with due consideration of the published literature on the area of study and validation studies. They had closed type of questions to get specific or hard fact information or open ended to capture opinions of the expert practitioners.

Once the questionnaire design was finalized, a pilot test (pre-testing) of the instrument was done by distributing them to 5 colleagues at work and professionals in the field of Computer science and computer security. This helped provide useful suggestions especially on appropriateness, structure and relevance of the questionnaires for the study. It also helped to assess the clarity of the questions, duration it would take to have a respondent respond to all the questions which gave an idea of the data collection process. Their suggestions were incorporated into the instrument which improved its reliability. After adjustments, the instrument was tested again with 5 subjects and another iteration of improvement followed. In this iteration, the emphasis was on improving the content validity and consistency.

The prototype was hosted on a website (http://csict.chuka.ac.ke/Web/) from where all participating practitioners accessed it. The practitioners were required to explore the model by performing some experimental tests and thereafter provide the model's accuracy for its intended purpose over the domain of its intended applicability on the questionnaires.

The practitioners were clearly instructed to do the following:

i. Collect data on security features and configurations from either an operational or hypothetical WLAN environment.
ii. Feed the data collected into the prototype
iii. Process results using computer model /prototype
iv. Assess accuracy of results (Magnitude and direction of output behaviour)
v. Repeat steps i-iv until you have sufficient data to enable you evaluate the model
vi. Provide feedback on the questionnaire.

The questionnaires were either collected by the researcher or practitioners sent them back via email.

3.7.4.3 Data Analysis

Analysis was performed after every five questionnaires. Completed questionnaire responses would be edited for completeness, consistency, viability and accuracy before processing them. Qualitative as well as quantitative analysis was used to analyze the data. Before presenting results, the researcher examined the raw data carefully to gain further insight into the results of the survey. Analysis of the validation results was expert by expert so as not to lose the insights from each expert that would happen if results are aggregated. Experts were coded to hide their identities. Then, the numerical results were aggregated.

While various expert opinion aggregation approaches exist e.g. Bayesian(Morris ,1974, 1977),linear opinion pools(Stone,1961) , axiomatic (Morris ,1983, 1986) and simple averaging of individual opinions, many studies have suggested simple averaging of individual opinions as a method for improving the accuracy of predictions (Armstrong, 1985; Ashton, 1986; Hill,1982; Hogarth, 1978; Zajonc, 1962).This therefore explains why simple averaging of individual opinions was employed in the analysis. The numerical results of parameter variability-sensitivity analysis are presented in tables and graphs and are accompanied with written explanations and analytical discussion. The discussion provides insight on the results adding knowledge that the researcher gained that is not in those results. What is learnt from the research is clearly stated.

Qualitative data collected through open ended questions was analyzed by identifying various themes from the content of the responses. A coding system was used to identify content about different themes. The responses were then organized into themes and concepts and presented as summaries that represent the key points emerging from the data.

3.7.5 Partial Operational Model Validation Using data

To illustrate practical applicability of the model, security data collected from preliminary survey for various components was fed into the operational/computerized model (prototype) by the researchers and results generated from the model were analyzed using a spreadsheet application.

3.8 Chapter Summary

This chapter has presented the details of various research strategies and specific research actions/activities geared towards the design of a model that enables design or selection and configuration of security features for WLAN authentication and access control in a public WLAN.

In particular it has detailed the activities of descriptive survey aiming at informing the security features and configurations discovery. It also detailed the activities of literature survey with CVSS based analysis aimed at analysing the attack susceptibility of security features and configurations on WLANs. The application of results from descriptive and literature survey and analysis in informing the development of model value function tables and algorithms has also been discussed.

Finally, the chapter detailed the activities of model validation aimed at giving the developed model an empirical basis. Table 3.1 shows a summary of the research objectives, how each objective was addressed and the main deliverables that informed the resulting model and its validity.

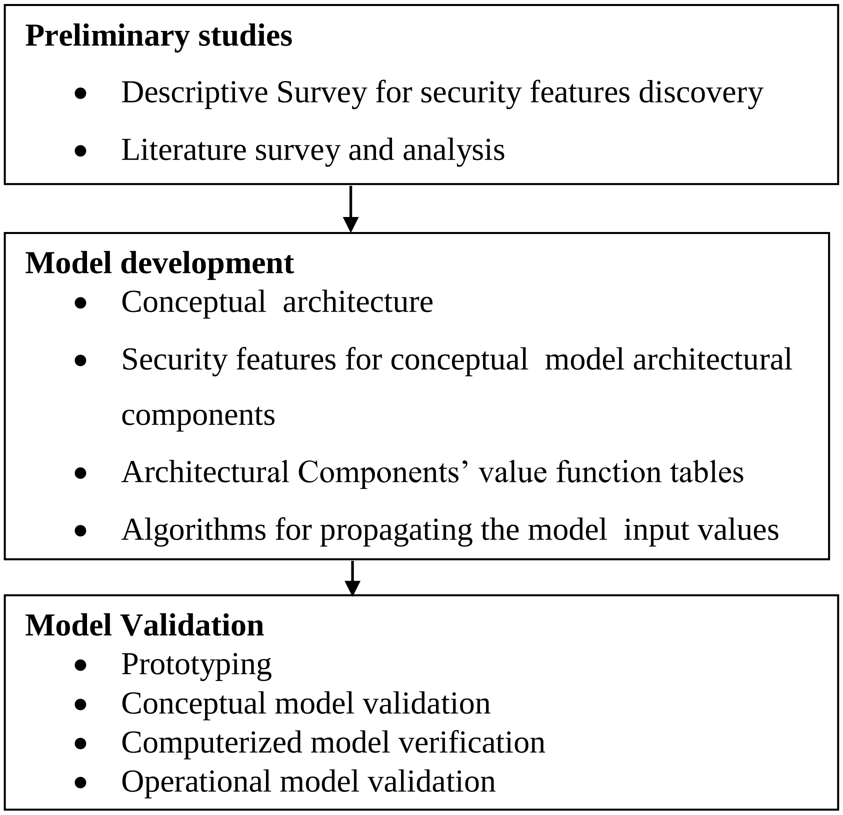
Table 3.1: Summary of objectives, methods and main deliverables

Research Objective	**How addressed (methods)**	**Main Deliverables**
Investigate IEEE 802.11 implementation specific vulnerabilities that may contribute to poor WLAN authentication and access control security performance in WLANs in Kenyan Universities.	-Descriptive survey on selected WLANs in Kenyan Universities.	-Security features implemented in a typical public WLAN. -Implementation specific vulnerabilities in a typical public WLAN.
Analyze security offered by WLAN cipher suites, authentication and access control mechanisms, end user and server system software used in WLAN authentication and access control.	Literature survey	Vulnerabilities exploited to attack cipher suite, authentication and access control mechanisms, end-user and server system software security features and configurations.
	Analysis using attack tree methodology and CVSS.	-Attack susceptibility of various security features implemented in public WLAN authentication and access control.
Establish relevant architectural components and use them to develop and prototype a simulation model that enables appropriate design or selection of security features and their configuration for WLAN authentication and access control	Literature survey	Conceptual model architectural components
	Discovery of security features and configurations implemented on a typical public WLAN via descriptive survey.	Security features for model architectural components

in public WLANs.	Analysis of attack susceptibility of various security features and configurations based on attack tree and CVSS analysis.	Architectural Components' value function tables
	Literature survey	Algorithms for propagating the model input values
		Algorithms for selection of EAP method
Validate the model for its intended purpose over the domain of its intended applicability.	Development of a prototype	Prototype [Test bed]
	Face Validation through expert intuition	Validated Conceptual model
	Theoretical analysis via degenerate and trace tests.	
	Structured Walkthrough	Verified Computerized model
	Trace Tests	
	Extreme Condition tests.	
	Parameter variability-sensitivity Analysis.	Validated Operational Model
	Partial model validation using data	

In summary, the model design research process involved three phases as shown in the figure 3.3. The Three Phases in this research are roughly consistent with the scientific method categories of observe, formulate and evaluate (Glass, 1995).

Preliminary studies were carried out to strengthen the background theory for the research. The findings from preliminary studies informed the design of the model. The model was prototyped to produce a computerized model. Validation process was done in three stages; conceptual model validation, computerized model verification and operational validation.



Preliminary studies

- Descriptive Survey for security features discovery
- Literature survey and analysis

Model development

- Conceptual architecture
- Security features for conceptual model architectural components
- Architectural Components' value function tables
- Algorithms for propagating the model input values

Model Validation

- Prototyping
- Conceptual model validation
- Computerized model verification
- Operational model validation

Figure 3.3: Research Approach Summary

CHAPTER 4: RESULTS, MODEL DESIGN DESCRIPTION AND EVALUATION

This chapter presents findings of discovery of security features and configurations related to architectural components, analysis of attack susceptibility of security features & configurations, model design description, model validation, discussion of the results and research contribution.

4.1 Findings from Discovery of Security Features and Configurations Survey

The respondents of this survey were network administrators (58 %) and heads of ICT (42%).Observation checklists were used on each university to collect data on security features and configurations on the following; client utility, client driver and access point utility. Observation checklists were also used to verify some questionnaire responses on cipher suite, authentication and access control mechanism, authentication credentials, user database and authentication server.

Fourty (40) practitioners (network administrators and heads of ICT) from chartered Universities and University colleges in Kenya were sampled, out of which 31 responded representing 77.5 % response rate. According to Mugenda & Mugenda (2003) a response rate of 77.5 is very good.

All Universities sampled had a WLAN infrastructure in place .All respondents reported that they were aware of security features employed on their University WLAN. Most of the respondents (93.5 %) had the opinion, that the University placed high value for its information resources. Additionally 71 % had at least one staff working specifically in IT security (25.8% had one, 22.6 % had two, 12.9% had three, 9.7 % had four) while 29% of the Universities had no IT staff working specifically in IT security. This therefore affirms that many universities placed value for its information resources. 58.1% indicated that sensitive and confidential documents are sent via university WLAN which justifies the need to ensure their security.

The most common systems in the Universities that are accessed via WLAN include:

i. Staff portal that includes Lecturers marks entry form and leave application.
ii. ELearning system
iii. Student management system; students registration, student results and students finance

iv. Financial management system

v. Mail servers, emails and institutional websites

Others are: survey system, e-library resources, QMS, online help system, Biokit, User account management tool (self-care), human resource information system, DSpace repository and centralized printing.

Based on the analysis of the practitioner responses, the following are the key IEEE 802.11 implementation specific issues that may contribute to poor WLAN authentication and access control security performance.

4.1.1 Cipher Suite

Figure 4.1 shows that 77.4 % of the University WLANs use confidentiality and integrity protocols that have well known vulnerabilities. It was established that 35.5% have implemented WEP only while 41.9 % have implemented TKIP only. Special concern is on 35.5 % who have implemented WEP that is very trivial to crack and with many tools targeting it readily available. No organization should be using WEP at all. Additionally 16.1% of university WLANS use combination of cipher suite; CCMP and TKIP (3.2 %), WEP and TKIP (3.2 %), WEP, TKIP and CCMP (6.5), WEP and TKIP (3.2 %).Only 6.5% of the networks (i.e. those implementing CCMP only) have ability to support RSN association (RSNA). This therefore means that many WLANs are vulnerable to pre-RSN related attacks.

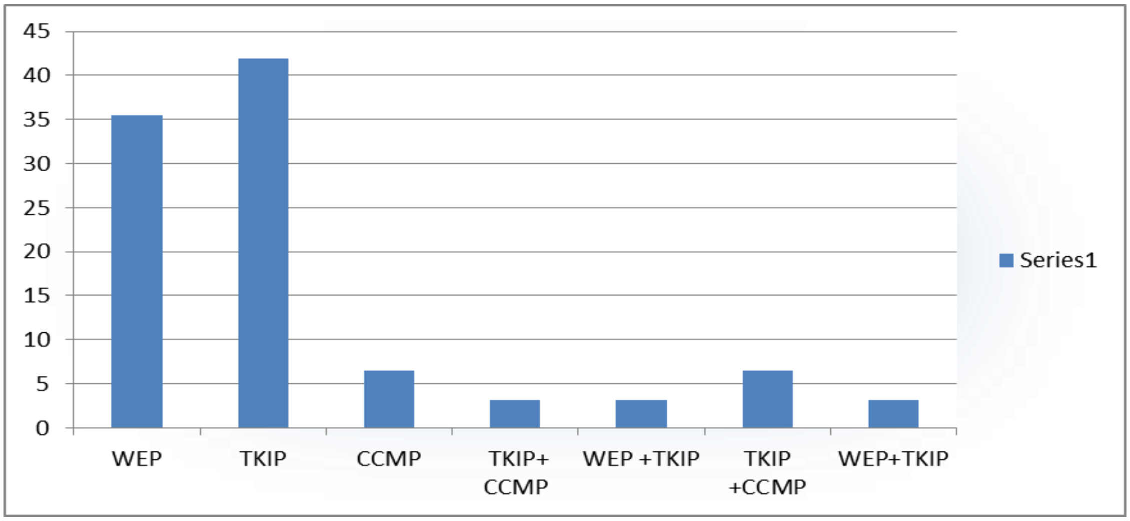


Figure 4.1: Cipher suites implemented in University WLANs

4.1.2 Authentication and access Control Mechanism

Figure 4.2 shows the primary methods of authentication used by University WLANs which are; Pre-shared key only authentication (32.3 %) and IEEE 802.1x with EAP method (32.3 %).35.4 % of the University WLANs use combined methods as follows; Pre-shared key and IEEE 802.1x with EAP method (19.35%), Pre-shared key and captive portal (6.45%), Captive portal and IEEE 802.1x with EAP method (6.45 %), MAC address and Pre-shared key (3.23%).Similarly MAC address authentications though rarely in use (3.23%) is prone to MAC address spoofing.

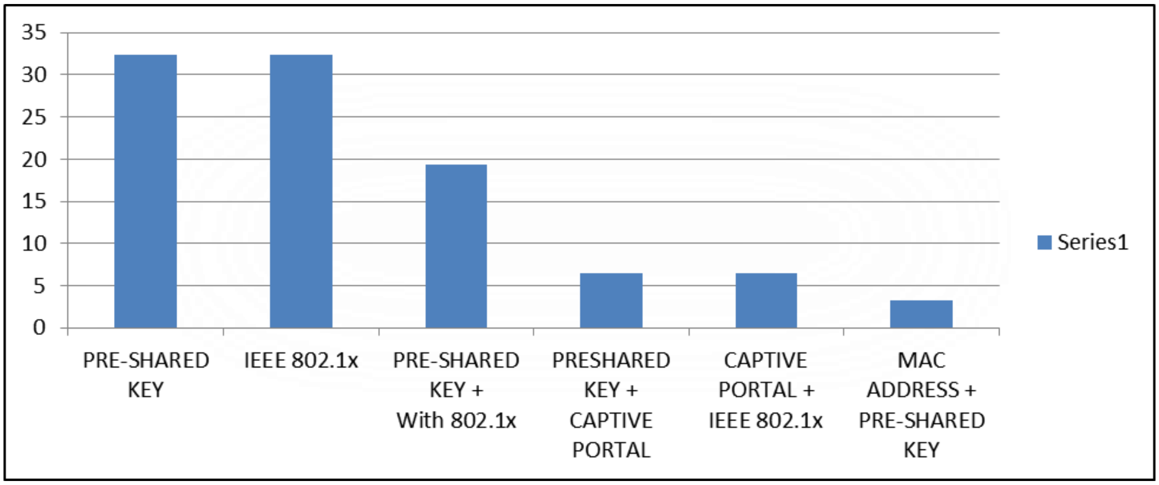
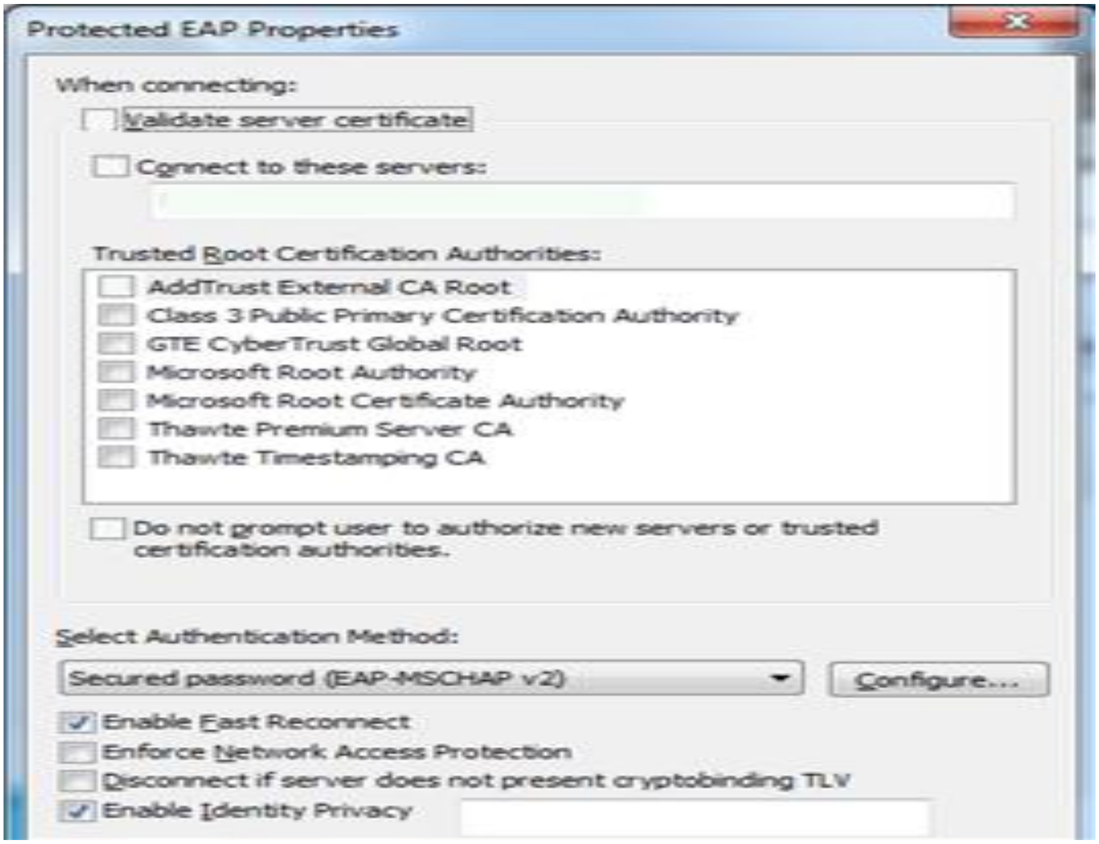


Figure 4.2: Authentication and access control mechanisms implemented

4.1.3 WLAN Client Utility

The EAP method used by majority of the University WLANS implementing IEEE 802.1x is PEAP and EAP TTLS (61 % PEAP, 28 % EAP TTLS .However many users configure their end devices to ignore validation of authentication server certificate and the specific authentication server address (name) verification is ignored. Additionally the devices are also configured in such a way that users can choose the server that is the source of the certificate. Specifically 54.8% of the WLANs have implemented WLAN security such that WLAN devices do not validate certificates provided by the authentication server of University WLAN whenever it connects to it. Observations made from user devices sampled show most devices having client utility configurations similar to what is shown in Figure 4.3.



Protected EAP Properties

When connecting:

□ Validate server certificate

□ Connect to these servers:

Trusted Root Certification Authorities:

□ AddTrust External CA Root
□ Class 3 Public Primary Certification Authority
□ GTE CyberTrust Global Root
□ Microsoft Root Authority
□ Microsoft Root Certificate Authority
□ Thawte Premium Server CA
□ Thawte Timestamping CA

□ Do not prompt user to authorize new servers or trusted certification authorities.

Select Authentication Method:

Secured password (EAP-MSCHAP v2)

☑ Enable Fast Reconnect
□ Enforce Network Access Protection
□ Disconnect if server does not present cryptobinding TLV
☑ Enable Identity Privacy

Figure 4.3 Client utility (Supplicant) misconfiguration

4.1.4 Access point Utility

Most WLAN (58%) were not configured to use IEEE 802.11w (i.e. management frame protection). These networks are therefore prone to many attacks that exploit lack of protection of management frames.

4.1.5 Authentication Server

58.1 % of WLANs corresponding to 18 Universities use RADIUS server for authentication while 41.9% do not. RADIUS servers have been known to be weak and easy to compromise e.g. RADIUS WPE. None of the Universities implement DIAMETER which is considered security wise superior to RADIUS.

4.1.6 Authentication credentials

Figure 4.4 shows that among the 18 University WLANs using RADIUS server for authentication, 11 % of the universities use password based EAP methods(LEAP and MD5) while 89 % use client side certificate based EAP methods (61 % PEAP,28 % EAP TTLS).LEAP and MD5 has known vulnerabilities with readily available attack tools.

PEAP and TTLS are secure. However they are prone to known man in the middle (MITM) attacks when poorly configured. No University WLAN among those sampled has implemented both client and server side certificate (TLS) .TLS is the most secure EAP method. However, it is complex to implement because of complexities associated with Public key infrastructure (PKI).

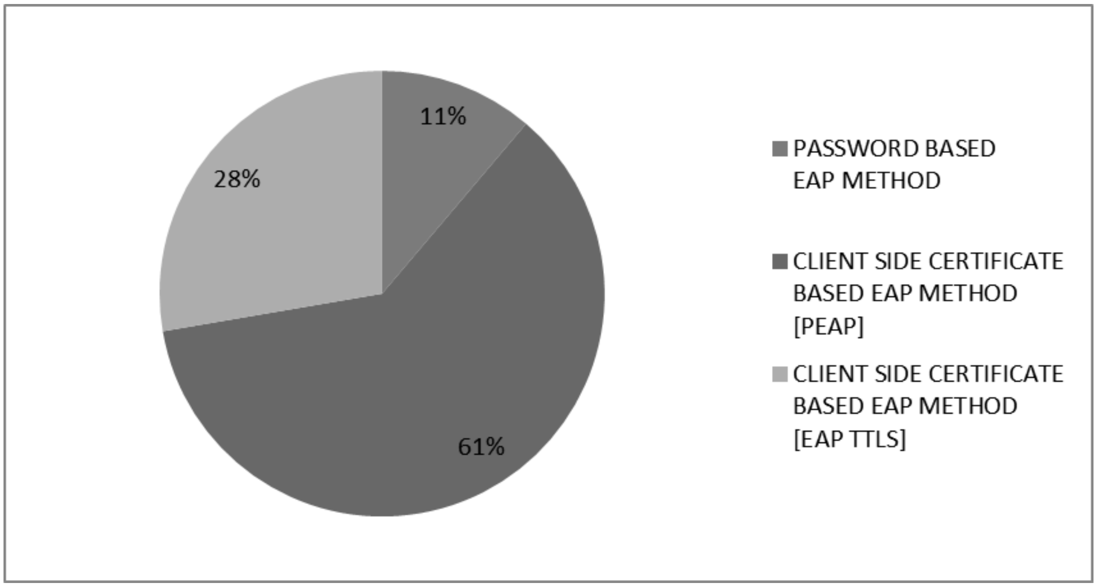


Figure 4.4: Authentication credentials used in WLAN implementations

The survey established that 38.7% of the university WLAN administrators never change the pre-shared key while 9.7% change them yearly.

4.1.7 User Database

It was observed that all the Universities sampled have implemented centralized user database for user names and passwords and in some cases MAC addresses that are associated to user names. None of the university WLANs implements a distributed database system. Additionally, none of the universities has implemented an intrusion detection system to monitor abnormal database access with an aim of detecting attacks.

4.1.8 Unchanged RADIUS server-Access point passphrase

45% of the University WLAN administrators implementing IEEE 802.1x with EAP do not change RADIUS server-access point passphrase. Another 22% change it yearly. This indicates that these WLAN suffer the risk of attacks on the RADIUS server-access point passphrase which can lead to man in the middle attacks.

4.1.9 Lack of digital certificate infrastructure

Only 6.4 % of Universities have a system where students can register for digital certificates. This indicates that very few WLANs are ready to deploy the most secure authentication methods such as TLS.

4.1.10 Known Attacks on University WLANs

Figure 4.5 shows that Majority of universities (61%) reported not having experienced a WLAN related security attack while a significant percentage (39 %) reported having experienced the attacks. The most common attack at 75% was denial of service while man in the middle (integrity) attack was at 8%. One University WLAN was reported having experienced both denial of service and man in the middle attack.

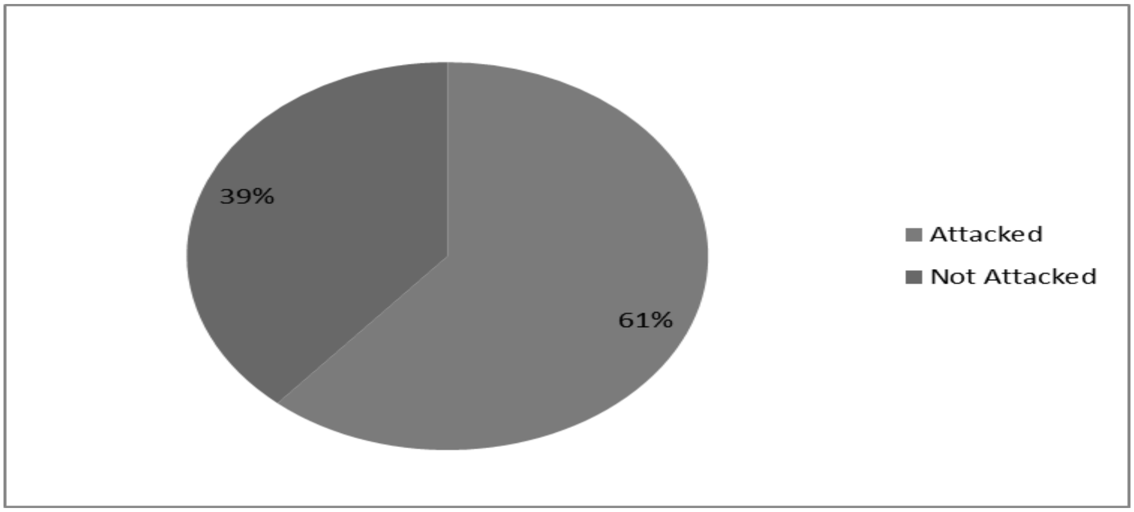


Figure 4.5: Attack Status of University WLANs

Practitioners provided the following as either causes of attack or vulnerabilities exploited:

(i) Lack of proper setup/configuration of authentication scheme in use

(i) Cracking the authentication credentials (pre-shared key) and consequently broadcasting packets

(ii) Network device failure due to old age

(iii) Students setting their own access points on their laptops. 45.2% indicated that their WLAN supports configuration of Virtual WiFi Soft Access points by WLAN devices

(iv) Weak pre-shared key

(v) Lack of network segmentation to separate WLAN traffic from wired traffic.

(vi) Weak/poor authentication methods

(vii) Vulnerable student devices e.g Lack of configuration of server name and other security details on user devices.

(viii) Overwhelming the RADIUS server.

(ix) Unauthenticated server

(x) Lack of updating the Operating system

(xi) Configuration weaknesses/errors

(xii) Deployment of vulnerable security features.

4.1.11 Model Justification

The practitioners appreciated the need for a model to explain and visualize the security of a WLAN authentication and access control. There was also concurrence among practitioners that an implementation model for authentication and access control can be used to increase the security of WLAN authentication in their environments. Some reasons provided by practitioners on why the proposed model is important are; The model will enhance security of WLANs, it will increase implementer and user awareness, it will enable regular auditing of the existing security on current implementations, it will act as a guideline or baseline for secure WIFI implementation in universities and will assist in security policy formulation and implementation. These responses are consistent with the researchers' justifications for the study. The results of the empirical survey shed light on operational security of many public WLANs. The survey also established many IEEE 802.11 configuration specific issues that may contribute to poor WLAN authentication and access control security performance and therefore justified the need for a model that facilitates selection or design and configuration of WLAN authentication and access control security features.

4.2 Analysis of Attack susceptibility of Security Features & Configurations

This section presents the results of attack susceptibility analysis of various attacks and vulnerabilities related to security features and configurations on a WLAN .authentication and access control implementation. The identified attacks were modeled in form of an attack tree and the vulnerability characteristics for the attacks were then analyzed based on CVSS model. A sample attack tree is shown in appendix 15 while raw scores/values of CVSS analysis can be found in appendix 16. Vulnerability scores (CVSS scores) of various attacks and vulnerabilities related to security features and configurations on a WLAN .authentication and access control implementation are presented and discussed in sections that follow.

4.2.1 Authentication and Access Control Mechanisms

Based on the CVSS scores, captive portal has highly vulnerable attacks when used as an authentication mechanism especially if not SSL encrypted and if it is not combined with link layer security. Captive portals provide no link layer encryption for wireless users; instead they rely on the MAC and IP address of the client as a unique identifier which can be spoofed easily. They therefore do not provide protection against eavesdropping and so are vulnerable to session hijacking (man in the middle attack) or captive portal evil twin.

Pre-shared key authentication exposes a WLAN to access point impersonation attacks as well as Pre-shared key recovery attacks both with high attack susceptibility. Lack of mutual authentication (access point not being authenticated to a client station) in some authentication and access control mechanisms is a major contributor to impersonation/rogue access points. The difficulty of managing security of manually distributed pre-shared keys (PSKs) on numerous devices makes it not suitable for use in large enterprise public WLAN deployments such as universities. The challenge handshake protocol (CHAP) used in this scheme has vulnerabilities that are easily broken**.** This indicates that pre-shared key is a weak authentication mechanism. Combining pre-shared key and captive portal authentication provides improved security.MAC address filtering access control mechanism leads to highly vulnerable impersonation attacks and so needs to be avoided. Though 802.1x authentication and access control has many attacks, attack susceptibility of these attacks is on average low. This makes it stronger than both captive portal and pre-shared key. Table 4.1a, 4.1b and 4.1c shows vulnerability scores of attacks on authentication and access control mechanisms.

Table 4.1a: Vulnerability Scores for Authentication and Access Control Mechanisms

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	STA Impersonation attacks	-Use of MAC address filtering access control mechanism -MAC address spoofing -Open/Null Authentication -No Mutual Authentication	8.1 [Very High]
2	Captive Portal circumvention (Evil Twin)	-Use of captive portal authentication that is not SSL encrypted.	8.3 [Very High]
		-Allowing SSL Self signed certificates from the captive portal -Lack of Validation of SSL server certificate -Lack of validation of captive portal server name.	7.1 [High]
3	Pre-shared key recovery attacks	-Use of Pre-shared key authentication mechanism -Use of Weak Pre-shared key -Use of challenge handshake authentication protocol.	7.1 [High]
4	802.1x Identity theft	-Use of 802.1x with EAP TLS -Cleartext 802.1x identity .	3.1 [Low]
5	802.1x password guessing	-Cleartext 802.1x identity -Weak session key/password	6.8 [Medium]

Table 4.1b: Vulnerability Scores for Authentication and Access Control Mechanisms

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
6	AP impersonation attack	-Lack of support for mutual authentication(Access point not authenticated) -SSID Unencrypted	7.1 [High]
		-802.1x with EAP based authentication -Weak AP-AS passphrase -Not regularly changing AP-AS passphrase	3.1 [Low]
7	802.1x LEAP cracking	-Use of light weight EAP method.	5.3 [Medium]
8	802.1x EAP downgrade attack	-Use of an EAP method that does not provide replay attack resistance	3.1 [Low]
9	802.1x EAP length attacks	-lack of EAP message authentication	3.1 [Low]
10	802.1x EAP of death	-lack of EAP message authentication.	3.1[Low]

Table 4.1c:Vulnerability Scores for Authentication and Access Control Mechanisms

	Attack	**Configuration issue/Vulnerable feature**	**CVSS Score**
11	802.1x EAP Start Flood	Low resources(memory and processing speed) on an access point	3.1 [Low]
12	802.1x EAP Replay	- Use of an EAP method that does not provide replay attack resistance[nonce, timestamp/sequence No]	4.2 [Medium]
13	802.1x EAP failure	- Use of an EAP method that does not provide replay attack resistance[nonce, timestamp/sequence No]	4.2 [Medium]
14	Brute force attacks	-Use of PIN based WIFI protected setup for authentication -Use of pre-shared key authentication	8.1 [Very High]
15	WPA-PSK Dictionary/ PSK Cracking	Use of pre-shared key authentication	6.8 [Medium]

4.2.2 Authentication Credentials

Various credentials used to authenticate an identity in a WLAN include; passwords/secret key, SSID, PIN, MAC address, session key and certificates. These credentials are attributed to attacks as shown in the tables 4.2a and 4.2b. The attacks exploit vulnerabilities that are intrinsic to the credentials or those that are as a result of the way the authentication credentials are implemented e.g use of MAC address is easily spoofable, wireless protected setup (WPS)-PIN is weak credential, weak passwords, dictionary based passphrases, not regularly changing authentication server–access point passphrase, use of certificates signed by public CAs, self- signed certificates, allowing a client to choose the CA, etc. Password recovery, cracker and sniffer tools such as Cain and Abel, which are freely available, can easily recover weak pre-shared keys These attacks can be avoided by using strong passwords, use of certificate signed by an internal trusted CA, not allowing self-signed certificates. Implementers should also avoid use of

MAC address only for authentication as well as wireless protected setup (WPS) that uses PIN for authentication.

Table 4.2a: CVSS Vulnerability Scores for Authentication Credentials Based Attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	EAP Dictionary Attacks	Use of weak Ms-CHAP-password	8.1 [Very High]
2	WPA-PSK Dictionary/ PSK Cracking	-Weak pre-shared key - Use of dictionary based passphrases.	6.8 [Medium]
3	Password based MITM attack	Use of Password/secret key as authentication credentials for an EAP method	6.8 [Medium]
4	STA Impersonation attacks	Use of MAC address as only authentication credential.	8.1 [Very High]
5	802.1x password guessing	-Cleartext 802.1x identity -Weak session key/password	6.8 [Medium]

Table 4.2b:Vulnerability Scores for Authentication Credentials Based Attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
6	Brute force attacks	-Use of PIN as authentication credential -Weak pre-shared key - Use of dictionary based passphrases.	8.1 [Very High]
7	802.1x RADIUS Cracking	Weak AP-AS passphrase AS-AP passphrase that is never changed.	4.2 [Medium]
8	RADIUS certificate MITM attacks	Self-signed certificates.	8.1 [Very High]
		Certificate signed by a public CA	8.1 [Very High]

4.2.3 Cipher Suite Attacks

.Cipher suite attacks comprise those attacks emanating from vulnerabilities of various cipher suites used for encrypting frames between client device and access point. These cipher suites (confidentiality and integrity cryptographic algorithms) are negotiated during authentication and access control. Table 4.3a, 4.3b and 4.3c shows vulnerability scores of attacks on confidentiality and integrity cryptographic algorithms (cipher suite). From the scores, wired equivalent privacy (WEP) is highly susceptible/ vulnerable because of weak confidentiality (RC4) and integrity (CRC-32) algorithms. The researcher therefore recommends that this cipher suite should not be used at all in any implementation because it will expose the WLAN to highly vulnerable attacks. While TKIP/WPA is also prone to attacks due to weak encryption algorithm (RC4), the vulnerability susceptibility is moderate because the integrity algorithm is moderately strong. CCMP using AES as encryption algorithm is the strongest cipher suite with susceptibility of known attacks being on average low.

Table 4.3a:Vulnerability Scores for Attacks on Cipher Suite

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	FMS	-WEP with Weak encryption algorithm (RC4) -Use of static encryption key.	8.1 [Very High]
2	KoreK	WEP with Weak encryption algorithm(RC4)	8.1 [Very High]
3	PTW	WEP with Weak encryption algorithm(RC4)	8.1 [Very High]
4	ChopChop	WEP with Weak encryption algorithm(RC4)	8.1 [Very High]
5	Bit flipping attacks	-WEP with Weak integrity protection CRC-32 - WEP with Weak encryption algorithm(RC4)	8.1 [Very High]

Table 4.3b: Vulnerability Scores for Attacks on Cipher Suite

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
6	Iterative key guessing attacks	-WEP with static encryption key - WEP with Weak encryption algorithm(RC4)	8.1 [Very High]
7	STA Impersonation attacks	-WEP with Weak integrity algorithm -WEP with Weak confidentiality protection algorithm(RC4)	8.1 [Very High]
8	WPA/TKIP Decryption attack.	-WPA with Weak encryption algorithm (RC4).	6.8 [Medium]
9	WPA-PSK Dictionary/ PSK Cracking	-WPA with Weak confidentiality algorithm.	6.8 [Medium]

Table 4.3c: Vulnerability Scores for Attacks on Cipher Suite

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
10	TKIP Countermeasures	Implementing WPA/TKIP	7.1 [High]
11	WPA Hole 196 Denial of service	Implementing both WPA and WPA2 cipher suites in a WLAN -Virtual WLANs	3.7 [Low]
12	802.11 Management frame Replay attacks	-WEP with Weak integrity protection CRC-32 -Lack of support for MFP	8.1 [Very High]
13	Brute force attacks	-WEP with Weak integrity and confidentiality protection algorithm	8.1 [Very High]
		-WPA with Weak confidentiality algorithm	6.8 [Medium]
14	ARP Poisoning	Implementing both WPA and WPA2 cipher suites in a WLAN	3.7 [Low]

4.2.4 Client Utility

Results show that many of the attacks are as a result of the way client utility is configured e.g client utility's support or lack of support for management frame protection and validation. These issues can be resolved in the following ways. Whenever client utility is configured to support both client and server side Certificate based mutual Authentication, implementers should enforce Validation of authentication server certificates and server name, client utility should be manually configured to allow a certificate signed by an internal certificate authority (CA) that is trusted, self-signed certificates should not be allowed. Tools like active directory wireless group policies can be used to centrally achieve this. Additionally client utility should support management frame protection and validation. Some of the available tools to execute the attacks are; Void11 and Deauth tool that executes deauthentication attacks, File2air and AirJack for 802.11 Management frame Replay attacks. Table 4.4a, 4.4b and 4.4c shows CVSS vulnerability scores for Client utility attacks

Table 4.4a: Vulnerability Scores for Client Utility Attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	STA Impersonation attacks	Client utility configured for MAC address authentication	8.1 [Very High]
		Client utility lack of support for MFP	8.1 [Very High]
2	RADIUS certificate MITM attack	Validation of server certificate and server name not enforced.	8.1 [Very High]
		Configured to allow self-signed certificates.	8.1 [Very High]
		Configured to allow certificate signed by a public CA	8.1 [Very High]
		Prompting user to authorize new servers and new trusted certification authorities.	7.3 [Very High]

Table 4.4b: Vulnerability Scores for Client Utility Attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
3	Disassociate flooding	Client Utility Lacks support for MFP	7.1 [High]
4	De-Authentication flooding	Client Utility Lacks support for MFP	7.1 [High]
5	802.11 Management frame Replay attacks	Client Utility lacks Support for MFP	8.1 [Very High]
		MFP set to optional	8.1 [Very High]
6	Security level rollback attack(TSN)	Client utility Supports both Pre-RSNA and RSNA.	7.5 [High]

Table 4.4c: Vulnerability Scores for Client Utility Attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
7	RSN IE poisoning/spoofing	-Lack of support for MFP -Unnecessary message exchanges between the RSN IE negotiation and confirmation.	7.5 [High]
8	AP impersonation attack	Validation of server certificate and server name not enforced	8.1 [Very High]
		Configured to allow self-signed certificates.	8.1 [Very High]
		Configured to allow certificate signed by a public CA.	8.1 [Very High]
		Prompting user to authorize new servers and new trusted certification authorities	7.3 [Very High]

4.2.5 Client Driver

Table 4.5 shows CVSS vulnerability scores for client driver attacks. As can be seen from the table, lack of or optional driver support for MFP, driver being set to a specific static scanning approach and use of pre-RSN devices are the most common source of vulnerabilities in client drivers. Use of specific scanning approach makes it easier for finger printing tools to launch driver specific attacks while lack of management frame support makes it easier for de-authentication attacks, disassociate flooding and STA impersonation attacks. Security level rollback attack is as a result of implementing combined RSNA and pre-RSNA wireless network cards.

Table 4.5: CVSS vulnerability scores for Client driver attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	STA Impersonation attacks	Lacks of driver support or optional driver support for MFP	8.1 [Very High]
2	Disassociate flooding	Lack of or optional support for MFP	7.1 [High]
3	De-Authentication flooding	Lack of or optional support for MFP	7.1 [High]
4	Driver finger printing attacks	Driver not set to a configurable scanning approach and instead set to a specific scanning approach.	5.3 [Medium]
5	Security level rollback attack(TSN)	-Client driver Supports both Pre-RSNA and RSNA. -Lack of or optional support for MFP	7.5 [High]

4.2.6 Access point Utility

Table 4.6a and 4.6b shows CVSS vulnerability scores for access point utility. Many of the attacks targeting access point utility are highly vulnerable/susceptible and are as a result of the configurations on the access point firmware e.g. support for MAC address filtering, access point firmware configured not to enforce management frame protection and validation, enabling pre-RSN association and use of firmware that is outdated e.g that which lacks support for IEEE 802.11i. Other vulnerabilities are intrinsic to access point e.g. low memory and processing capacity, These issues can be resolved by upgrading the firmware to support IEEE 802.11i and IEEE 802.11w and properly configuring the access point firmware e.g. Firmware configured to support management frame protection (MFP /IEEE 802.11w) and is set to required, firmware configured to support only RSNA connections(RSNA enabled).Firmware configured to adopt a separate identifier counter for each association and avoiding MAC address filtering on an access point. Other remedies include transferring the authentication function to an authentication server.

Table 4.6a: Vulnerability Scores for Access point utility

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	STA Impersonation attacks	Accesspoint firmware Configured to support MAC address filtering	8.1 [Very High]
		Access point firmware is configured not to enforce MFP.	8.1 [Very High]
		Pre-RSN enabled on the accesspoint firmware.	8.1 [Very High]
2	Disassociate flooding	Access point firmware is configured not to enforce MFP.	7.1 [High]
		Accesspoint firmware MFP set to optional	7.1 [High]
3	Authentication flooding	Low memory & processor capability of Accesspoints	8.1 [Very High]
		-Broadcasting SSID	8.1 [Very High]
4	De-Authentication flooding	Access point firmware is configured not to enforce MFP.	7.1 [High]
		Accesspoint firmware MFP set to optional	7.1 [High]

Table 4.6b: Vulnerability Scores for Access point utility

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
5	Association Flooding	Low memory & processor capability of Access points Memory and processor resources exhausted	7.1 [High]
		AP configured not to adopt a separate identifier counter for each association causing Counter space exhaustion.	8.3 [High]
6	Distributed flooding	Low memory & processor capability of Access points	8.3 [High]
		-Broadcasting SSID -AP configured not to adopt a separate identifier counter for each association	8.3 [High]
7	Probe request flooding	SSID Unencrypted	8.3 [High]
8	802.11 Management frame Replay attacks	Access point firmware is configured not to enforce MFP.	8.1 [Very High]
		-Access point firmware MFP set to optional	8.1 [Very High]
9	Security level rollback attack(TSN)	-Client utility Supports both Pre-RSNA and RSNA. -Management frame unencrypted.	7.5 [High]

4.2.7 Authentication server

Table 4.7 shows CVSS scores for Authentication server based attacks. Attacks associated with authentication server mainly target vulnerabilities in the configuration of the RADIUS based authentication server and situations where the authentication server is embedded in the access point. These attacks can be avoided by deploying DIAMETER based authentication server or deploying RADIUS server and sealing the loop holes that make it vulnerable such as use of strong passphrase that is changed regularly, configuring mutual authentication, configuring it not to accept self-signed certificates or certificates signed by public Certificate authorities(CAs).Implementers should avoid use of authentication servers embedded on an access point.

Table 4.7: Vulnerability Scores for Authentication Server Based Attacks

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	Authentication flooding	Authentication server integrated in access point	8.1 [Very High]
2	802.1x RADIUS Cracking	-Weak access point-authentication server passphrase -Not regularly changing Passphrase	4.2 [Medium]
3	RADIUS certificate MITM attacks	Mutual authentication not supported on RADIUS server.	8.1 [Very High]
		Using RADIUS Certificate signed by public CA	8.1 [Very High]
		Server configured to use self-signed certificates when authenticating to client	8.1 [Very High]
4	802.1x EAP length attacks	-lack of EAP message authentication	3.1 [Low]
5	802.1x EAP of death	-lack of EAP message authentication	3.1 [Low]

4.2.8 User Database System

Table 4.8 shows CVSS vulnerability scores for attacks on user database system. The attacks targeting user database are mainly denial of service attacks. These attacks target situations where the database resides in the access point. In other cases, the database server may be on a dedicated server but due to centralized architecture, the server’s resources are consumed by malicious and sometimes distributed authentication requests.

One tool that can be used to facilitate these attacks is void11.Although database attacks are few and with medium attack susceptibilities, they are critical because they are mainly denial of service attacks which are very difficult to control. Database intrusion detection systems (IDSs) that act as intelligent, real-time monitors and that inspect data streams to detect inappropriate activity is the most appropriate remedy for these type of attacks. Implementing distributed database server would also serve to mitigate the effects of these attacks.

Table 4.8: Vulnerability Scores for Attacks on User Database System.

S/N	Attack	Configuration issue/Vulnerable feature	CVSS Score
1	Database server DOS	-Centralized user database.	8.1 [Very High]
		-User Database integrated in access point	8.1 [Very High]
2	Distributed flooding	User Database integrated in access point	8.1 [Very High]
3	Authentication flooding	Unmonitored automated authentication requests	8.1 [Very High]
4	Injection attacks	Unmonitored automated authentication requests	8.1 [Very High]

4.2.9 Summary of Attacks

Table 4.9 shows a summary of 41 attacks analyzed in section 4.2 and the artifact/ components they target. From the table, it is evident that all the eight artifacts identified in the conceptual architecture are targets of WLAN security attacks. It is also clear that some attacks target more than one component.

Table 4.9: Summary of attacks and the components they target

	Attack	Security Component targeted
1	FMS	Cipher Suite
2	KoreK	Cipher Suite
3	PTW	Cipher Suite
4	ChopChop	Cipher Suite
5	WPA-PSK Dictionary/ PSK Cracking	Cipher Suite
		Cipher Suite
6	WPA/TKIP Decryption attack.	Cipher Suite
		Authentication and access control mechanism.
7	Bit flipping attacks	Cipher Suite
8	Iterative key guessing attacks	Cipher Suite
9	STA Impersonation attacks	Cipher Suite

		Authentication and access control mechanism.
		Client Utility
		Client Driver
		Accesspoint utility
		Authentication credentials
10	Captive Portal circumvention (Evil Twin)	Authentication and access control mechanism
		Authentication Credentials
11	ARP Poisoning	Cipher Suite
12	RADIUS certificate MITM attacks	Client Utility
		Authentication Credentials
		Authentication Server
13	Disassociate flooding	Client Driver
		Client utility
		Access point utility
14	De-Authentication flooding	Client utility
		Access point utility
		Client Driver
15	Authentication flooding	Access point utility
		Authentication server
		User Database
16	Association Flooding	Access point utility
17	Database server DOS	User database
18	TKIP Countermeasure	Cipher suite
19	WPA Hole 196 Denial of service	Cipher suite
20	Distributed flooding	Access point firmware
		User database
21	Probe request flooding	Access point utility
22	EAP Dictionary Attacks	Authentication Credentials
23	Password based MITM attack	Authentication credentials
24	802.1X Identity theft	Authentication Mechanism
25	802.11 Management frame Replay attacks	Client Utility
		Access point utility
		Cipher suite
26	Brute force attacks	Cipher suite

		Authentication credentials
		Authentication and access control mechanism
27	Driver finger printing attacks	Client driver
28	Security level rollback attack(TSN)	Client utility
		Client driver
		Accesspoint utility
29	RSN IE poisoning/spoofing	Client Utility
30	AP impersonation attack	Authentication and access control mechanism
		Client utility
		Authentication credentials
31	802.1X RADIUS Cracking	Authentication server
		Authentication credentials
32	802.1x EAP Replay	Authentication server
33	802.1x password guessing	Authentication server
		Authentication credentials
34	802.1x EAP downgrade	Authentication Server
35.	802.1x EAP of death	Authentication and access control mechanism
		Authentication Server
36.	802.1x EAP length attack	Authentication and access control mechanism
		Authentication Server
37.	Pre-shared key recovery attacks	Authentication and access control mechanism
38.	802.1x LEAP cracking	Authentication and access control mechanism
39	802.1x EAP start flood attack	Authentication and access control mechanism
40	802.1x EAP failure	Authentication and access control mechanism
41	Injection attack	User Database

The research established that there was at least one vulnerability exploit tool available targeting each of the eight artifacts/components that influence attack susceptibility as shown in table 4.10. Most of these tools are found in backtrack security auditor collection which is an open source toolkit intended for use during penetration testing and vulnerability assessment.

Table 4.10: Summary of attack tools and the components they target.

Component/Parameter	**Attack Tool**
Cipher suite	Wireshark,ettercap,dsniff Aircrack-ng,airsnort
Authentication and access control mechanism	Cain and Abel coWPAtty,genpmk,KisMAC,wpa_crack Asleap
Authentication Credentials	Cain and Abel, Aircrack-ng
Client Utility	Wireshark,ettercap,dsniff Aircrack-ng,airsnort
Client Driver	WIFIDenum(WIFI Driver Enumerator)
Accesspoint Utility	Void11,FakeAP
Authentication Server	RADIUS WPE QACafe,file2air,libradiate
User Database	Void11,FakeAP

4.3 Architecture and Key Algorithms of the Simulation Model

This section presents the architecture and key algorithms that make up a simulation model developed. These include value function tables that map security features and configurations to security levels, algorithm for combining and propagating model input values and algorithm for EAP method selection.

The preliminary study results presented in section 4.1 and 4.2 together with conceptual architecture presented in section 2.10 and literature sources were used to tackle the following issues pertaining model development:

(i) Design of value function tables that map security features and configurations to security levels.

(ii) Design of an algorithm for combining and propagating model input values

(iii) Design of an algorithm for EAP method selection

4.3.1 Simulation Model Operation Algorithm

The model has four steps that define its operation:

(i) Selection of security features or configurations available to the security implementer.

(ii) Mapping security features/configurations to attack susceptibility/vulnerability Strengths.

(iii) Combining and propagating the attack susceptibility values of the security features and configurations selected.

(iv) Generation of results

Subsequent sub-sections detail the activities of each step.

4.3.1.1 Selection of Security Features or Configurations

This is the set of security features/configurations available to the security implementer for each of the eight artifacts in the conceptual architecture. The artifacts previously discussed in section 2.10 are: client utility, client driver, access point utility, authentication server, authentication & access control mechanism, user database, cipher suite and authentication credentials.

It was established in section 4.2.9 that there was at least one vulnerability exploit tool available for each of these eight artifacts as illustrated in foregoing section in Table 4.10. For that reason, all the eight artifacts have been considered equivalent in relative importance in relation to their influence on attack susceptibility meaning that none of them can be considered superior to the other. However, their actual influence values/strength will be determined by the security features selected or configurations on each of the components.

4.3.1.2 Mapping Security Features/Configurations to Vulnerability Strengths

The model maps the security features/configurations selected to “Very High”, “High”, “Moderate” or “Low” vulnerability strength based on already predetermined values. Each security feature/configuration is associated with certain characteristics which determine its strength of vulnerability. The decision on which strength a security feature/configuration is mapped to is based on a value function.

The design of value functions which map security feature/configuration to an attack susceptibility level was informed by CVSS results in section 4.2 which established the severity scores of vulnerabilities and attacks targeting these security features and configurations.

Table 4.11 to Table 4.18 show value function tables for the eight model artifacts. For each of the function table, whenever attack susceptibility of a security feature/configuration is mapped to level low, moderate or high, it is denoted 1, 2 and 3 respectively. Security strength for the same is however denoted as 3, 2 and 1 respectively because attack susceptibility and security strength have an inverse relationship/negative type influence between them. Whenever attack susceptibility of a security feature/configuration is mapped to level very high, it is denoted as *.The corresponding security level is denoted as 0.

This means that if this security feature/configuration is selected and implemented, the implementation of authentication and access control security is highly susceptible to attacks and therefore such security feature/configuration is not recommended for use in a public WLAN implementation of authentication and access control.

Table 4.11: Value Function Table for Authentication Credentials

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of Security Feature/ Configuration**
Low [1]	**3**	Both Client and Server Certificates
Moderate [2]	**2**	PAC, One time password OR Server Side certificate only(Tunneled)
High [3]	**1**	Secret Key/password(Mutual or Unilateral)
Very High [*]	**0**	SSID
Very High [*]	**0**	MAC address
Very High [*]	**0**	PIN

Table 4.12: Value Function Table for Cipher Suite

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of the Security feature/Configuration**
Low [1]	3	CCMP (WPA2 +AES)
Moderate [2]	2	TKIP(WPA +AES)
High [3]	1	TKIP(WPA +RC4)
High [3]	1	TKIP(WPA2 +RC4)
Very High [*]	0	WEP

Table 4.13: Value Function Table for WLAN Client Driver

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of Security Feature/ Configuration**
Low [1]	3	• Supports management frame protection (MFP/IEEE 802.11w) and validation. • Supports configurable active scanning approach.
Moderate [2]	2	• Supports management frame protection(MFP/IEEE 802.11w) and validation • Lacks Support for Configurable active scanning approach
Moderate [2]	2	• Lacks support for management frame protection (IEEE 802.11w) and validation • Supports IEEE 802.11i. • Supports configurable active scanning approach.
High [3]	1	• Lacks support for management frame protection (MFP/IEEE 802.11w) and validation • Lacks support for Configurable active scanning approach. • Supports IEEE 802.11i.
Very High [*]	0	Lacks support for IEEE 802.11i.

Table 4.14: Value Function Table for WLAN Client Utility

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of Security Feature/ Configuration**
Low [1]	3	• Configured to support both client and server side Certificate based mutual Authentication. • Supports Management frame protection. • Configured to enforce validation of server certificates and server name. • Configured not to allow Self signed certificates.
Moderate [2]	2	• Configured to support server side only Certificate based mutual Authentication. • Supports Management frame protection (IEEE 802.11w). • Configured to enforce validation of server certificates and server name. • Configured not to allow Self signed certificates.
High [3]	1	• Configured to support Password, pre-shared key or MAC address based mutual Authentication mechanism. • Supports Management frame protection (IEEE 802.11w)
High [3]	1	• Configured to support server side only or both client and server side Certificate based mutual Authentication • Lacks Support for Management frame protection (IEEE 802.11w) and validation. • Supports IEEE 802.11i.
High [3]	1	• Configured to support Password, pre-shared key or MAC address based mutual Authentication mechanism. • Lacks Support for Management frame protection (IEEE 802.11w) and validation. • Supports IEEE 802.11i.
Very High [*]	0	Lacks support for IEEE 802.11i.
Very High [*]	0	Configured to support server side only or both client and server side certificate but Validation of server certificates and/or server name not enforced.
Very High [*]	0	Configured to support server side only or both client and server side certificate but allows Self signed certificates.
Very High [*]	0	Mutual authentication not supported.

Table 4.15: Value Function Table for Access point Utility

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of Security Feature/ Configuration**
Low [1]	**3**	• Firmware configured to support management frame protection (MFP/IEEE 802.11w) and validation and is set to required. • Firmware configured to Support only RSNA connections(RSNA enabled)
Moderate [2]	**2**	• Firmware configured to support optional management frame protection (MFP/IEEE 802.11w) and validation. • Firmware configured to Support only RSNA connections(RSNA enabled)
High [3]	**1**	• Firmware does not support MFP/IEEE 802.11w and validation • Firmware configured to Support only RSNA connections(RSNA enabled)
Very High [*]	**0**	Firmware not configured to Support only RSNA connections(Pre-RSNA enabled)

Table 4.16: Value Function Table for Authentication and Access control mechanism

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of Security Feature/ Configuration**
Low [1]	3	IEEE 802.1x With EAP method
Low [1]	3	Captive portal and IEEE 802.1x With EAP Method
Moderate [2]	2	Captive Portal and Pre-shared Key
High [3]	1	Captive Portal Only
High [3]	1	Pre-shared Key Only
Very High [*]	0	MAC address filtering
Very High [*]	0	Open SSID
Very High [*]	0	PIN based authentication(WPS)
Very High [*]	0	Button press based authentication(WPS)

Table 4.17: Value Function Table for Authentication Server

Attack Susceptibility **[**Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of Security Feature/ Configuration**
Low [1]	**3**	DIAMETER. Configured to Support mutual authentication
Moderate [2]	**2**	RADIUS. Configured to Support mutual authentication
High [3]	**1**	DIAMETER. Not Configured to Support mutual authentication
High [3]	**1**	RADIUS. Not Configured to Support mutual authentication
High [3]	**1**	KERBEROS
***Very High [*]**	**0**	None/Independent on each Access point

Table 4.18: Value Function Table for User Database System

Attack Susceptibility [Strength/ Weight of influence]	**Security** [Strength/ Weight of influence]	**Description of Security Feature/Configuration**
Low [1]	**3**	Distributed Database Servers with an Intrusion Detection System(IDS)
Moderate [2]	**2**	Distributed Database Servers without an Intrusion Detection System(IDS)
Moderate [2]	**2**	Centralized Database Server with an Intrusion Detection System(IDS)
High [3]	**1**	Centralized Database Server without an Intrusion Detection System(IDS)
Very High [*]	**0**	None/Independent on each Access point

4.3.1.3 Combining and Propagating the Attack Susceptibility Values of the Security Features/Configurations in the Model

The model determines the overall security level of an implementation by aggregating attack susceptibilities of individual artifacts based on security features and configurations set in them.

The artifacts whose attack susceptibilities are aggregated are: client utility, client driver, access point utility, authentication server, authentication & access control mechanism, user database, cipher suite and authentication credentials. Figure 4.7 shows the structure of hierarchy and direction of propagation of attack susceptibilities. The aggregation of attack susceptibility is hierarchical and is done bottom up as follows:

(i) Attack susceptibilities of **client utility**, **client driver** and **access point utility** are aggregated to derive a composite attack susceptibility level for front-end system software

(ii) Attack susceptibility of **authentication server**, **authentication & access control mechanism** and **user database** are aggregated to derive a composite attack susceptibility level for back-end authentication systems.

(iii) The derived attack susceptibility level for **front-end system software** is aggregated with that of **back-end authentication systems** to derive a composite attack susceptibility level for trusted computing base (TCB).

(iv) Attack susceptibility of **cipher suite** and **authentication credentials** are aggregated to derive a composite attack susceptibility level for wireless path.

(v) Finally, the attack susceptibility level of **trusted computing base (TCB**) and that of **wireless path** are aggregated to form an **overall attack susceptibility** of the implementation.

(vi) If overall attack susceptibility is **“Low”, “Moderate”** ,**”High”** or **“Very High”** then the wireless authentication and access control security (WAACS) level is “**Strong”**, “**Moderate” ,** ”**Weak” or “Very Weak”** respectively. This is because attack susceptibility has a negative type of influence on security strength/level.

The model therefore provides a what-if simulation of the security expected from a combination of the influences of the selected security features and/or configurations.

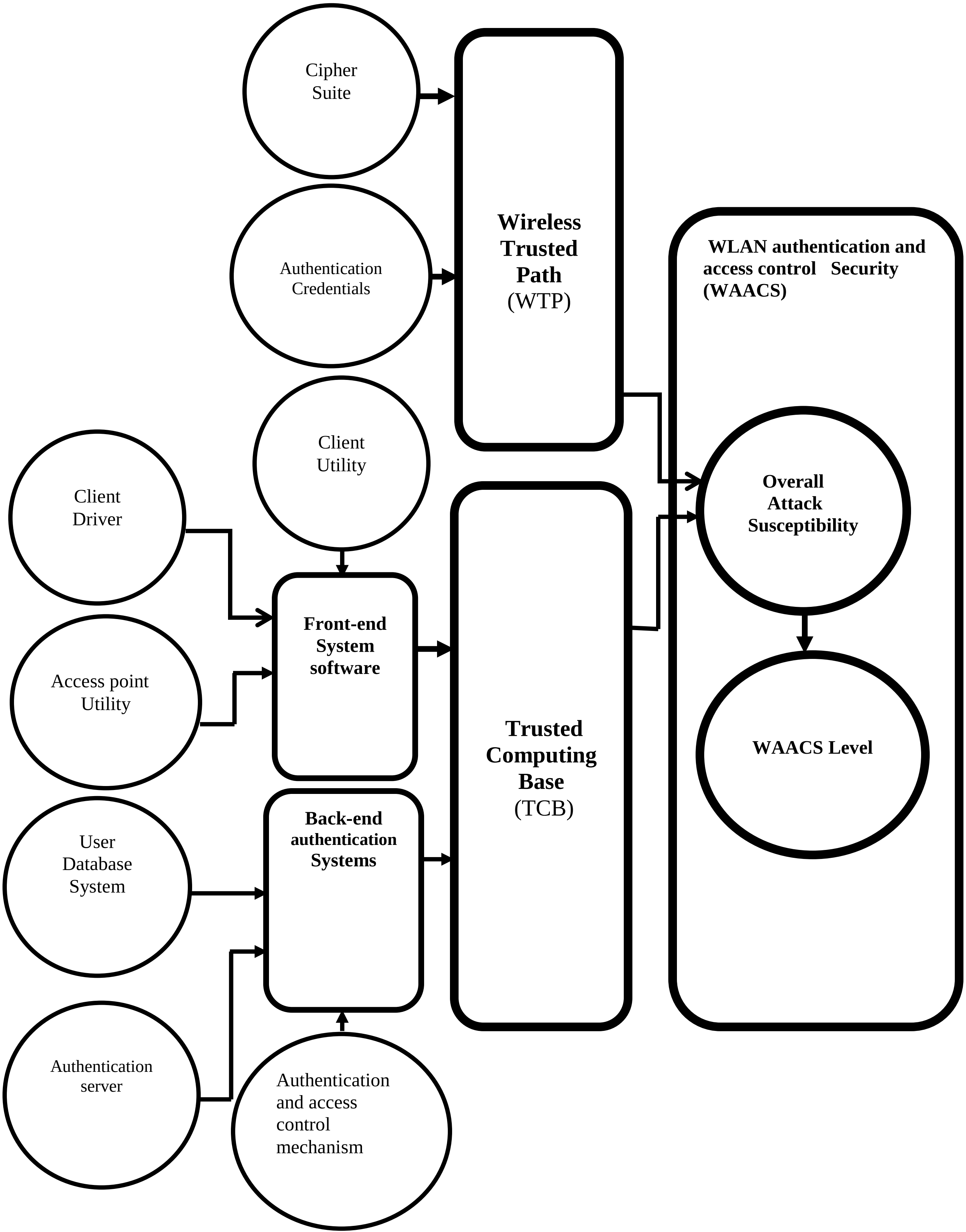

Cipher Suite
Authentication Credentials
Wireless Trusted Path (WTP)
WLAN authentication and access control Security (WAACS)
Client Utility
Client Driver
Overall Attack Susceptibility
Front-end System software
Access point Utility
WAACS Level
Trusted Computing Base (TCB)
Back-end authentication Systems
User Database System
Authentication server
Authentication and access control mechanism

Figure 4.7: Structure of Hierarchy and Direction of Propagation of Attack Susceptibilities.

The combination and propagation mechanism used to aggregate attack susceptibilities is illustrated below:

(a) Starting with terminal nodes, every subtree has a parent node **R** and a set of child nodes **C**. The child nodes may have a negative or positive type of influence on **R.** A positive influence of child **C$_i$** on **R** means that when attack susceptibility of **C$_i$** is high, that of **R** is influenced to move upwards too. On the other hand, a negative influence of child **C$_i$** on **R** means that when attack susceptibility of **C$_i$** is high, that of **R** is influenced to move downwards.

(b) If a parent node **R** has at least one child with **very high** attack susceptibility strength, the model gives a notification that the security feature or configuration is not recommended for use in a public WLAN implementation of authentication and access control. This is because this feature renders the security of the entire WLAN very weak.

(c) If a parent node **R** has ***k*** child nodes with combination of positive and negative influences and of strength S$_i$ (High, Moderate, Low) and values of attack susceptibility for all child nodes are known, the value **V$_R$** of the parent node is computed based on the following weighted average.

$$V_R = \frac{\sum^{k}{}_{i=1}\ (Si * Vi)}{\sum^{k}{}_{i=1}\ (\ Si\ )}$$

Where:

S$_i$ refers to the strength of the influence of a child C $_{\boldsymbol{i}}$ on parent **R** which is equal to 1, 2, or 3 if the influence of the child is low, moderate, and high respectively.

V$_i$ refers to the value of child **C$_{\boldsymbol{i}}$** and is dependent on S$_i$ and type of influence of child C$_{\boldsymbol{i}}$ on parent node **R**. If the child node C$_{\boldsymbol{i}}$ has a positive influence on Parent node **R** and the strength of influence (S$_i$) of node C$_{\boldsymbol{i}}$ is low, moderate, or high then V$_i$ is equal to 1, 2, and 3 respectively. On the other hand, if the child node C$_{\boldsymbol{i}}$ has a negative influence on parent node **R** and strength of influence (S$_{i)}$ of node C$_{\boldsymbol{i}}$ is low, moderate or high then V$_i$ is equal to 3,2 or 1 respectively.

Figure 4.8 shows a parent node**(R)** with **k** child nodes each child C$_i$ having an influence of type **t$_i$** and of strength S$_i$ on Parent node R.

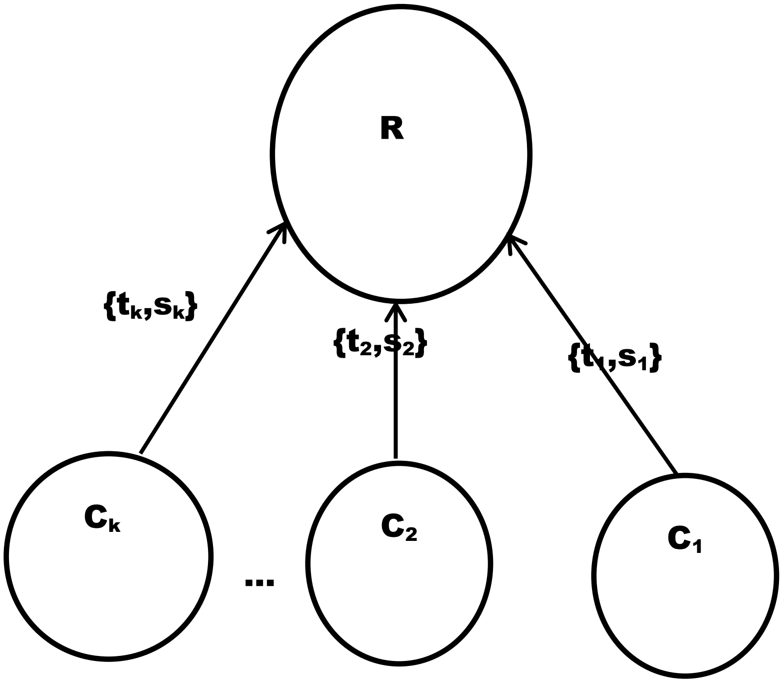


Figure 4.8: Relationship between child nodes and parent nodes in the model

(d)Once a value V_R is determined, thresholds have been set to decide the values of V_R as follows;

(i)If $1<=V_R<1.5$, then the value of R is low

(ii)If $1.5 <= V_R <= 2.5$, then the value of R is moderate

(iii)If $2.5 < V_R<=3$, then the value of R is High.

(e)The process is repeated recursively up the hierarchy until a value for the root node is established.

This technique is based on weighted average approach as described by (Brookes et al, 2010). The process involves transformation from attribute (security feature/configuration) to value (could be a score e.g 3 or a category e.g "High") which is done by a value function as shown in Table 4.11 to Table 4.18. The second step is to combine multiple values into a single value using a combination function. However, before the values can be combined they must be normalized to a single scale to avoid implicit weighting. Because the approach can be weighted this method/approach is known as weighted average (Brookes et al, 2010).

4.3.1.4 Generation of Results

The model generates the following results:

(a)A qualitative output (Very Weak, Weak, Moderate, Strong) of Level/strength of WLAN security associated with selected security features/configurations.

(b)Notification of any highly vulnerable security features/configuration that may have been input/selected with recommendation(s) that it should not be used in the WLAN security implementation.

4.3.2 Algorithm for Selection of a Secure EAP Authentication Method

Figure 4.9 shows an algorithm for selection of a secure EAP authentication method based on implementation environment parameters. The implementation environment parameters applied in the algorithm include: infrastructure support for IEEE 802.1x, CCMP or TKIP, need to protect identity of communicating parties, need to use legacy authentication methods, whether the organizational network is currently using digital certificates for other applications and whether the organization is facing any difficulties in enforcing password security by users.

The EAP methods involved in the selection algorithm include: Transport layer security(TLS),Tunneled transport layer security(TTLS), Light weight extensible authentication protocol(LEAP), Protected Extensible authentication protocol(PEAP) and Flexible authentication via secure tunneling(EAP-FAST).

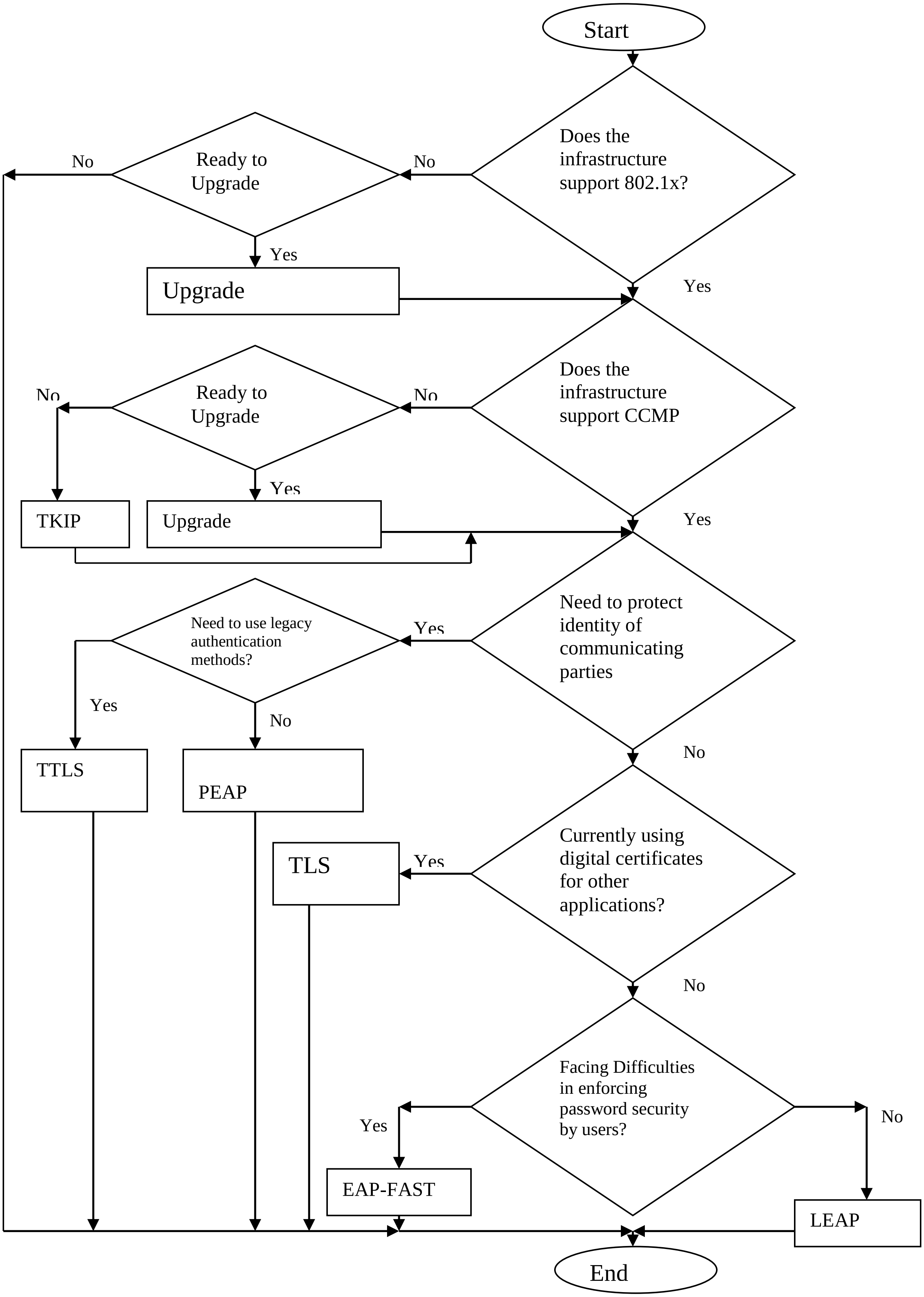
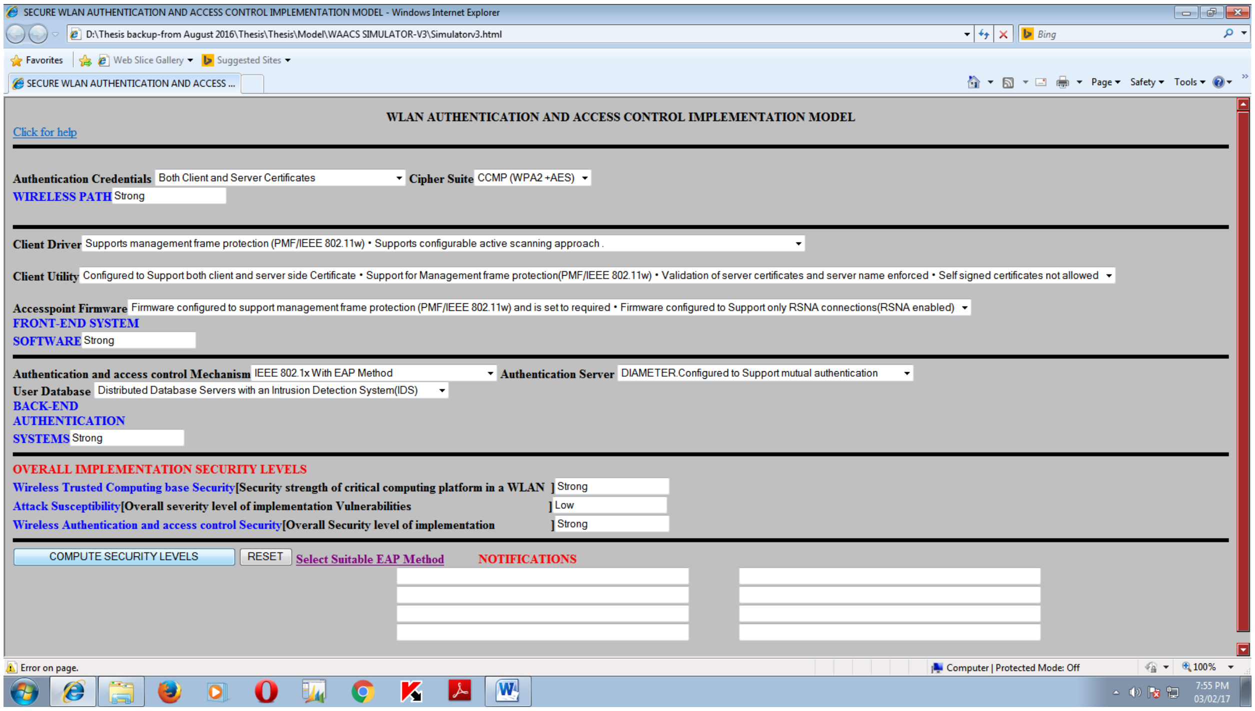

Start
Does the infrastructure support 802.1x?
No
Ready to Upgrade
No
Yes
Upgrade
Yes
Does the infrastructure support CCMP
No
Ready to Upgrade
No
Yes
TKIP
Upgrade
Yes
Need to protect identity of communicating parties
Yes
Need to use legacy authentication methods?
Yes
No
TTLS
PEAP
No
Currently using digital certificates for other applications?
Yes
TLS
No
Facing Difficulties in enforcing password security by users?
Yes
No
EAP-FAST
LEAP
End

Figure 4.9: Algorithm for Selection of a Secure EAP authentication Method

4.4 Model Prototype

Figure 4.10 shows an interface of the model where an implementer is required to select features from each of the eight components of the model and on pressing the **Compute Security** level button, the model propagates the values of the selected features, computes and displays the values for Wireless Path security, Front end systems software Security, back-end systems software Security ,Wireless trusted computing base security, attack susceptibility and finally overall WLAN authentication and access control security(WAACS).The implementer can try different combinations of security component parameters while observing the equivalent security for each and then choose the parameters that are appropriate for configuration.


SECURE WLAN AUTHENTICATION AND ACCESS CONTROL IMPLEMENTATION MODEL - Windows Internet Explorer
D:\Thesis backup-from August 2016\Thesis\Thesis\Model\WAACS SIMULATOR-V3\Simulatorv3.html
Bing
Favorites
Web Slice Gallery
Suggested Sites
SECURE WLAN AUTHENTICATION AND ACCESS ...
Page
Safety
Tools
Error on page.
Computer | Protected Mode: Off
100%
7:55 PM
03/02/17

WLAN AUTHENTICATION AND ACCESS CONTROL IMPLEMENTATION MODEL

Click for help

Authentication Credentials: Both Client and Server Certificates
Cipher Suite: CCMP (WPA2 +AES)
WIRELESS PATH: Strong

Client Driver: Supports management frame protection (PMF/IEEE 802.11w) • Supports configurable active scanning approach .

Client Utility: Configured to Support both client and server side Certificate • Support for Management frame protection(PMF/IEEE 802.11w) • Validation of server certificates and server name enforced • Self signed certificates not allowed

Accesspoint Firmware: Firmware configured to support management frame protection (PMF/IEEE 802.11w) and is set to required • Firmware configured to Support only RSNA connections(RSNA enabled)
FRONT-END SYSTEM SOFTWARE: Strong

Authentication and access control Mechanism: IEEE 802.1x With EAP Method
Authentication Server: DIAMETER.Configured to Support mutual authentication
User Database: Distributed Database Servers with an Intrusion Detection System(IDS)
BACK-END AUTHENTICATION SYSTEMS: Strong

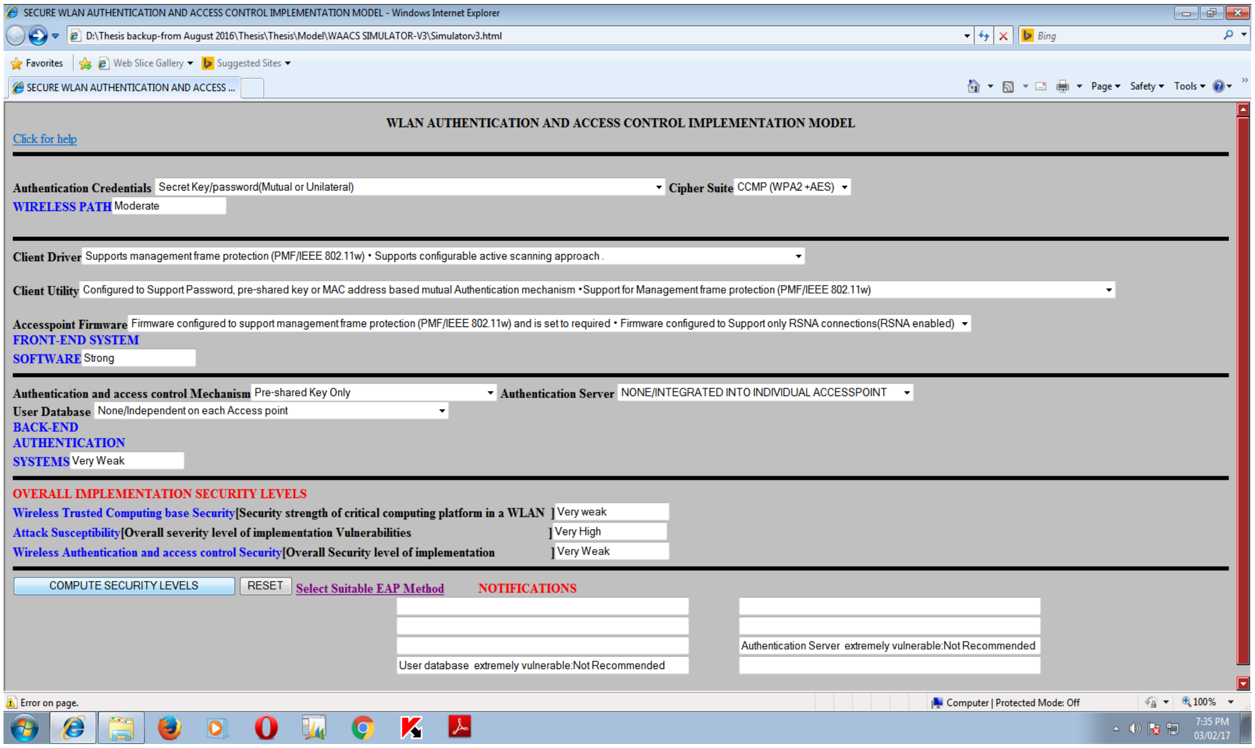
OVERALL IMPLEMENTATION SECURITY LEVELS
Wireless Trusted Computing base Security[Security strength of critical computing platform in a WLAN] Strong
Attack Susceptibility[Overall severity level of implementation Vulnerabilities] Low
Wireless Authentication and access control Security[Overall Security level of implementation] Strong

COMPUTE SECURITY LEVELS | RESET | Select Suitable EAP Method | NOTIFICATIONS

Figure 4.10: Interface for WLAN Security Features Selection and Analysis

The prototype does not need intensive training to be used. It has a simple and attractive interface.

It can be accessed from http://csict.chuka.ac.ke/Web/ .The source code for the script is shown in appendix 6.Where highly vulnerable security parameters have been selected, the model provides notifications as indicated in figure 4.11.


SECURE WLAN AUTHENTICATION AND ACCESS CONTROL IMPLEMENTATION MODEL - Windows Internet Explorer
D:\Thesis backup-from August 2016\Thesis\Thesis\Model\WAACS SIMULATOR-V3\Simulatorv3.html
Bing
Favorites
Web Slice Gallery
Suggested Sites
SECURE WLAN AUTHENTICATION AND ACCESS ...
Page
Safety
Tools
COMPUTE SECURITY LEVELS
RESET
Error on page.
Computer | Protected Mode: Off
100%
7:35 PM
03/02/17

WLAN AUTHENTICATION AND ACCESS CONTROL IMPLEMENTATION MODEL

Click for help

Authentication Credentials: Secret Key/password(Mutual or Unilateral)
Cipher Suite: CCMP (WPA2 +AES)
WIRELESS PATH: Moderate

Client Driver: Supports management frame protection (PMF/IEEE 802.11w) • Supports configurable active scanning approach .

Client Utility: Configured to Support Password, pre-shared key or MAC address based mutual Authentication mechanism •Support for Management frame protection (PMF/IEEE 802.11w)

Accesspoint Firmware: Firmware configured to support management frame protection (PMF/IEEE 802.11w) and is set to required • Firmware configured to Support only RSNA connections(RSNA enabled)
FRONT-END SYSTEM SOFTWARE: Strong

Authentication and access control Mechanism: Pre-shared Key Only
Authentication Server: NONE/INTEGRATED INTO INDIVIDUAL ACCESSPOINT
User Database: None/Independent on each Access point
BACK-END AUTHENTICATION SYSTEMS: Very Weak

OVERALL IMPLEMENTATION SECURITY LEVELS
Wireless Trusted Computing base Security[Security strength of critical computing platform in a WLAN] Very weak
Attack Susceptibility[Overall severity level of implementation Vulnerabilities] Very High
Wireless Authentication and access control Security[Overall Security level of implementation] Very Weak

Select Suitable EAP Method

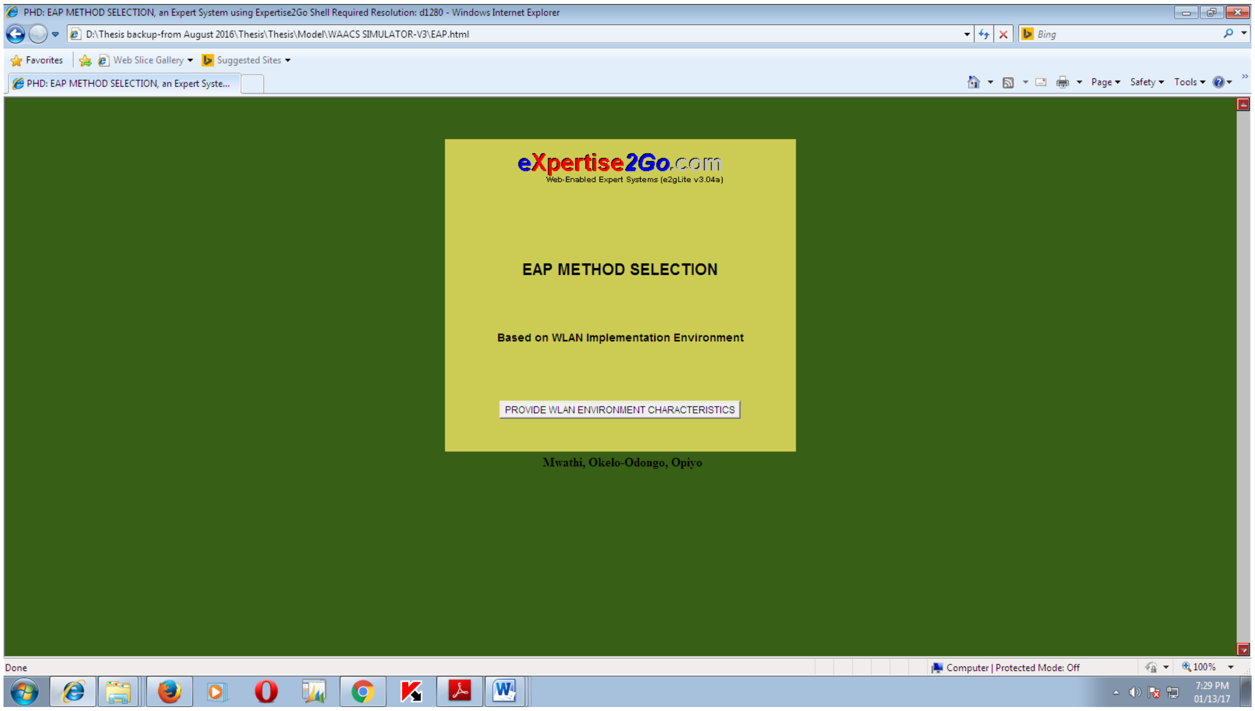
NOTIFICATIONS

User database extremely vulnerable:Not Recommended
Authentication Server extremely vulnerable:Not Recommended

Figure 4.11: Notifications when highly Vulnerable Security Features are Selected.

Figure 4.12 shows the expert system interface used to enable selection of a secure EAP authentication method while figure 4.13 shows sample output from the expert system based prototype. The webpage that runs this prototype is called EAP.html. The EAP .html file is used to provide an appropriate interface for the prototype because to use the expert system, a web page that loads the applet and identifies the knowledge base is needed.

The e2glite expert system shell which contains the knowledge engine is implemented as a Java applet. Just like any other compiled java program, the applet is embedded into a web page via a special HTML tag and is invoked from the web page via the HTML applet tag when needed.


PHD: EAP METHOD SELECTION, an Expert System using Expertise2Go Shell Required Resolution: d1280 - Windows Internet Explorer
D:\Thesis backup-from August 2016\Thesis\Thesis\Model\WAACS SIMULATOR-V3\EAP.html
Bing
Favorites
Web Slice Gallery
Suggested Sites
PHD: EAP METHOD SELECTION, an Expert Syste...
Page
Safety
Tools
eXpertise2Go.com
Web-Enabled Expert Systems (e2gLite v3.04a)
Done
Computer | Protected Mode: Off
100%
7:29 PM
01/13/17

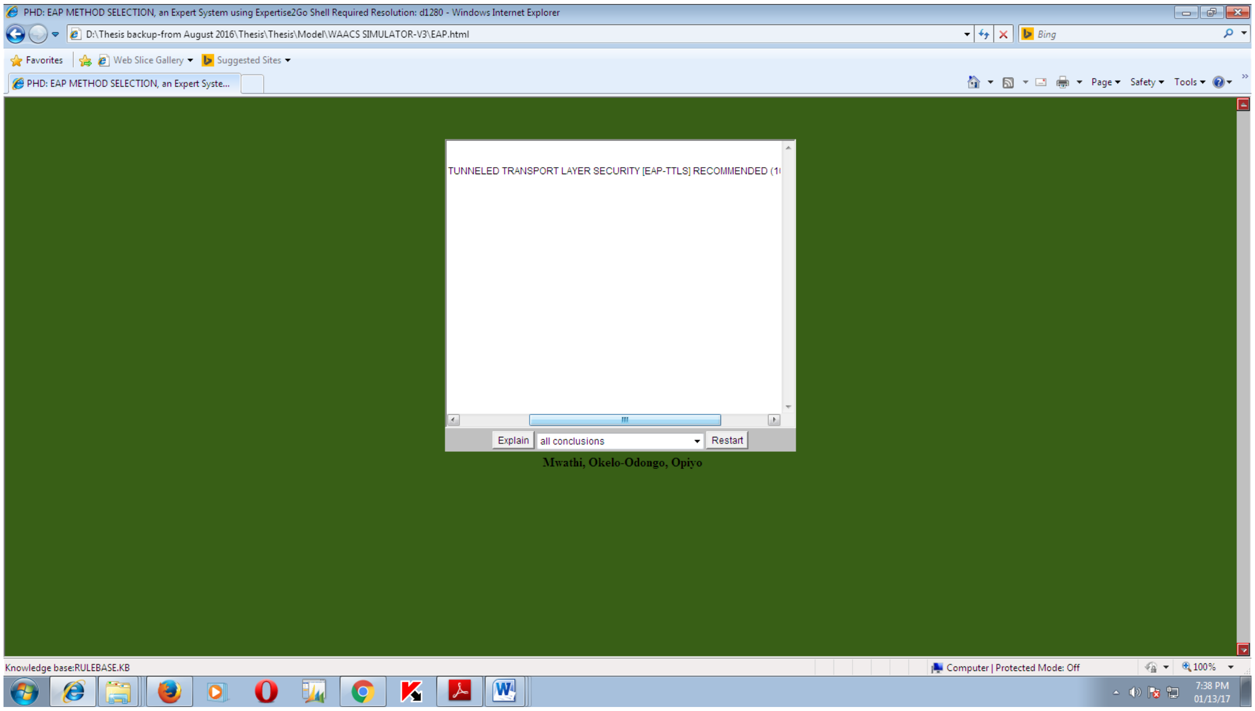
EAP METHOD SELECTION

Based on WLAN Implementation Environment

PROVIDE WLAN ENVIRONMENT CHARACTERISTICS

Mwathi, Okelo-Odongo, Opiyo

Figure 4.12: Start Screen of EAP Method Selection Prototype


PHD: EAP METHOD SELECTION, an Expert System using Expertise2Go Shell Required Resolution: d1280 - Windows Internet Explorer
D:\Thesis backup-from August 2016\Thesis\Thesis\Model\WAACS SIMULATOR-V3\EAP.html
Bing
Favorites
Web Slice Gallery
Suggested Sites
PHD: EAP METHOD SELECTION, an Expert Syste...
Page
Safety
Tools
Explain
all conclusions
Restart
Knowledge base:RULEBASE.KB
Computer | Protected Mode: Off
100%
7:38 PM
01/13/17

TUNNELED TRANSPORT LAYER SECURITY [EAP-TTLS] RECOMMENDED (1

Mwathi, Okelo-Odongo, Opiyo

Figure 4.13: Output Screen of EAP Method Selection Prototype

4.5 Results of Conceptual Model Face Validation through Experts

Validation using experts sought to establish whether, to a large extent, the model includes components and algorithms that meaningfully and accurately reflect a model that facilitates selection or design and implementation of security features for WLAN authentication and access control.

Thirty (30) experts were identified, out of which 20 responded representing 66.7 % response rate. According to Mugenda & Mugenda (2003) a response rate of 66.7 % is good enough. All respondents were experienced researchers/consultants because they had been in their jobs for more than three years. Additionally the level of competence of all the respondents ranged from moderate to highly competent with the majority (90 %) being highly competent in WLAN security as shown in figure 4.14.

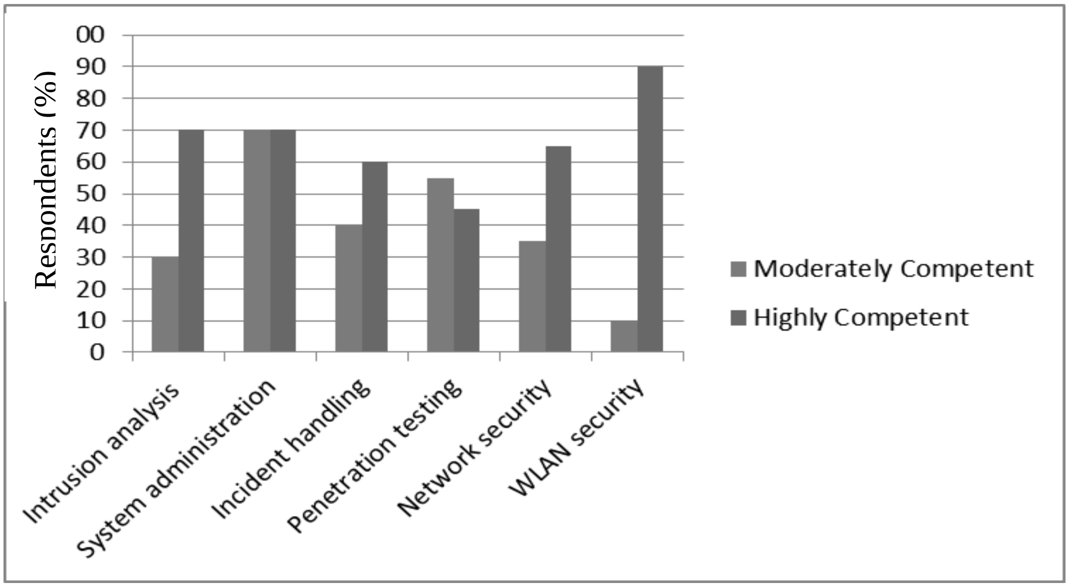


Figure 4.14: Competence Level of Experts

4.5.1 Model Structure

The model structure consists of architectural components each with its characteristics that influence the attack susceptibility and consequently security level of a WLAN authentication and access control implementation. The components fall in two main dimensions based on trusted computing base concept; Wireless path and Trusted Computing base.

The researchers evaluated the model structure on a scale of 1-5 interpreted as follows;

1. I don’t agree with the categorization
2. Somewhat confident with the categorization
3. Neither Confident Nor Not confident with categorization
4. Confident with categorization
5. Very confident with categorization

Architectural Components

The model identified eight architectural components whose features and configurations(characteristics) influence attack susceptibility; authentication credentials, cipher suite, WLAN client driver, WLAN client utility, access point utility, authentication and access control mechanism ,authentication server and user database system. Based on the aggregated findings, majorities (96.25 %) of the respondents were confident with these components (53.75 % very confident and 42.5 % confident).3.125 % were not decided while 0.625 % disagreed with the components but without giving reasons. These aggregated percentages indicate that the components that influence attack susceptibility and consequently security level were well thought and were consistent with the understanding of experts. Table 4.19 shows specific percentages of experts’ confidence levels for each parameter.

Table 4.19: Confidence Levels on Architectural Conceptual Model components

Parameters	**Very Confident (%)**	**Confident (%)**	**Neither confident nor not confident (%)**	**Somewhat confident (%)**
Cipher Suite	95.0	5.0		
Authentication Credentials	60.0	35.0	5.0	
WLAN Client Driver	35.0	55.0	5.0	5.0
WLAN Client Utility	35.0	55.0	10.0	
Access point Utility	35.0	65.0		
Authentication and access control Mechanism	75.0	25.0		
Authentication Server	60.0	40.0		
User Database	35.0	60.0	5.0	
Percentage Average	**53.75**	**42.5**	**3.125**	**0.625**

Dimensions

Trusted computing base (TCB) is a small amount of software, firmware, hardware and procedural components that security depends on and that we distinguish from a much larger amount that can misbehave without affecting security. A secure path between trusted computing base elements is a mandatory requirement. Based on this concept the eight components were categorized into two main dimensions; **Wireless Path Security (WPS**) which refers to the wireless MAC layer security between end devices and access point and **WLAN Trusted Computing base Security (WTCBS)** which refers to security critical computing platform in a WLAN and consist of end user devices, access points, authentication systems and their configurations.

From the findings all the respondents were confident with this categorization (45 % very confident and 55 % confident).These aggregated percentages indicate that this categorization was well thought and was consistent with the understanding of the experts.

Table 4.20 shows specific percentage confidence levels for each Dimension-component combination.

Table 4.20: Confidence Levels on Categorization of Architectural Components

Dimension	**Component**	**Very Confident (%)**	**Confident (%)**
Wireless Path Security (WPS)	Authentication Credentials	25.0	75.0
	Cipher Suite	65.0	35.0
Wireless Trusted Computing Base Security(WTCBS)	WLAN Client Driver	50.0	50.0
	WLAN Client Utility	60.0	40.0
	Access point Firmware	35.0	65.0
	Authentication Server	35.0	65.0
	User Database	25.0	75.0
	Authentication and access control Mechanism	65.0	35.0
Percentage Average		**45**	**55**

Components of Trusted Computing Base.

Based on client server architecture associated with WLAN authentication, WLAN trusted computing base (WTCB) security components were further categorized into two intermediate components (i) Front-end system software which refers to security features and configurations on utility and driver softwares associated with both end user devices and access point and (ii) Back-end authentication systems which refers to the security features and configurations on Server and access point software components associated with authentication of users to the WLAN. Researchers evaluated them on a scale of 1-5.From the findings majority (97.5 %) of the respondents were confident with this categorization (80 % very confident and 17.5 % confident) while 2.5 % were not decided. None of the respondents disagreed with the categorization. These percentage averages indicate that the categorization of trusted computing base was well thought and was consistent with the understanding of experts. Table 4.21 shows specific percentage confidence levels for Wireless trusted computing base Security components categorization.

Table 4.21: Confidence Levels on Categorization of WTCB Security Components

Component	**Parameters**	**Very Confident (%)**	**Confident (%)**	**Neither confident nor not confident (%)**
Front-end System Software	WLAN Client driver	75.0	20.0	5.0
	WLAN Client utility	85.0	10.0	5.0
	Access point utility	75.0	20.0	5.0
Back-end Authenticati on Systems	Authentication Server	90.0	10.0	
	User Database	80.0	20.0	
	Authentication and access control mechanism	75.0	25.0	
Percentage Average		**17.5**	**80**	**2.5**

4.5.2 Assumptions

An attacker driven by motive, opportunity and capability launches one or many attacks to achieve a specific objective. Attacker capability refers to availability of resources such as attack tools, knowledge, experience and funding necessary for launching attacks. Attacker motivation refers to perceived benefit to the attacker after a successful attack. Opportunity refers to a favourable situation that the attacker exploits to achieve the intended goal. The model design assumes that there exists attackers who have motivation and capability and therefore ready to compromise any WLAN implementation whenever there is an opportunity. The results that are presented in figure 4.15 indicate that majority (95 %) of the experts belief in this assumption while 5 % of the experts were undecided.

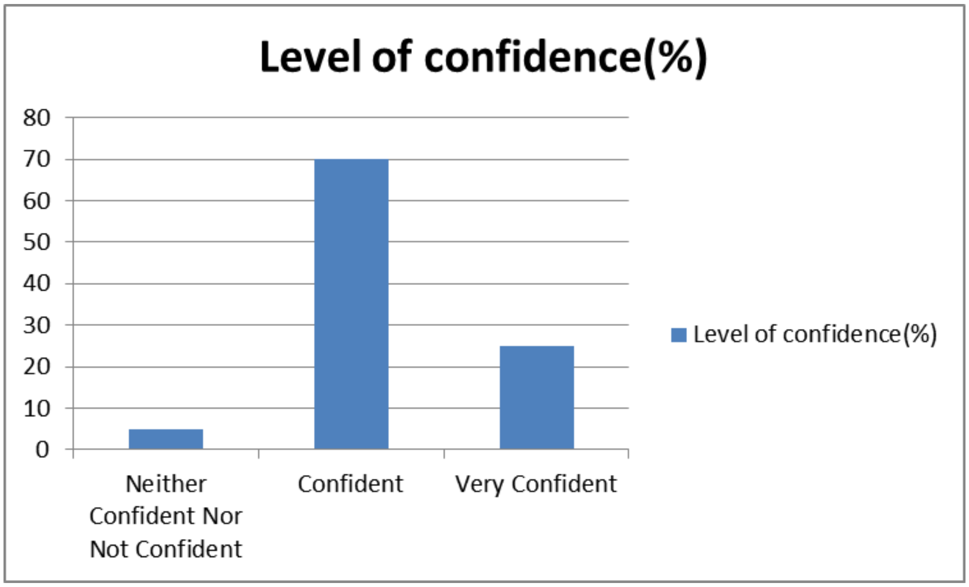


Figure 4.15: Confidence in Existence of Motivated and Capable Attackers

Preliminary research established that the exploit code targeting each of the eight components is mature (i.e there is at least a functional exploit code available for each component or sufficient technical details to exploit the component vulnerabilities exist) For that reason, the model assumes that all the eight components have equal potential of vulnerability exploitation and therefore have equal relative importance in the model.

The results indicate that 75 % of the experts (55% confident and 20% very confident) belief in this assumption while 10% were somewhat confident and 15% were undecided as shown in figure 4.16.

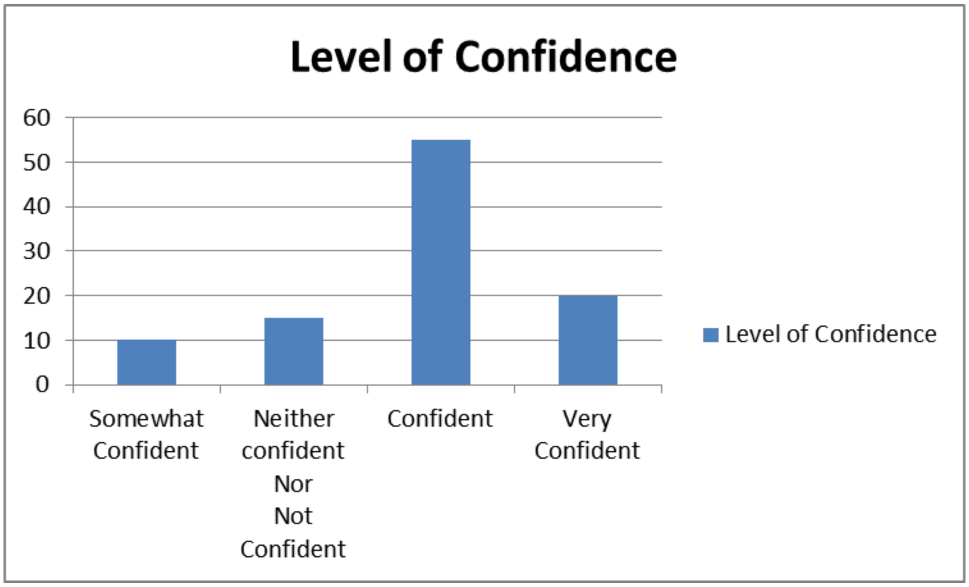


Figure 4.16: All Components have Equal Relative Importance in the Model.

4.5.3 Model's Representation of the Problem Entity, Logic and Mathematical Causal Relationships

The experts were asked how confident they are in the correctness of the security weights/strengths assigned next to the security features/configurations of each of the components. This question was aimed at obtaining the level of expert's confidence in the security weights/strengths assigned to various component features and configurations (characteristics) when implemented to provide security in a public WLAN authentication and access control. From the findings majority (87.5 %) of the experts were confident with the security weights (43.75 % very confident and 43.75 % confident).10.625 % were not decided while 1.875 % disagreed with the security weights. These percentage averages indicate that the assignment of weights was well thought and was consistent with the understanding of experts. Table 4.22 shows specific percentage confidence levels for each component's weights.

Table 4.22: Experts' Percentage Confidence Levels for Each Component's Weights

Parameter	**Very Confident (%)**	**Confident (%)**	**Neither confident nor not confident(%)**	**Somewhat confident (%)**
Authentication Credentials	25.0	60.0	15.0	
Cipher Suite	80.0	5.0	10.0	5.0
WLAN Client Driver	15.0	75.0	10.0	
WLAN Client Utility	25.0	60.0	10.0	5.0
Access point Utility	35.0	50.0	15.0	
Authentication Server	40.0	40.0	15.0	5.0
Authentication and access control Mechanism	85.0	15.0		
User Database	45.0	45.0	10.0	
Percentage Average	**43.75**	**43.75**	**10.625**	**1.875**

Experts were also asked how confident they are in the mathematical logic of the technique for propagation of values in the model. The results indicate that 95 % of them (45% confident and 50% very confident) belief in the mathematical logic of the technique for propagation of values in the model while 5 % of the experts were undecided as shown in figure 4.17.

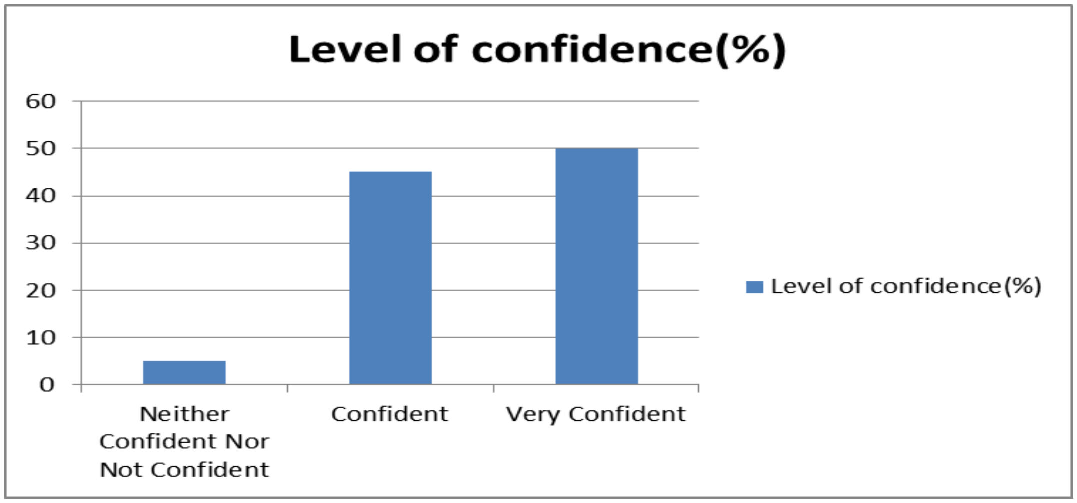


Figure 4.17: Mathematical Logic of the Technique for Propagation of Values

When experts were asked how confident they are in the correctness of the algorithm for selection of a secure Extensible Authentication protocol (EAP) method, their response is as shown in figure 4.18**.**The responses indicate that 95 % of the experts (80% confident, 15% very confident) belief in the correctness of the algorithm for selection of a secure Extensible Authentication protocol (EAP) method while 5 % of the experts were undecided.

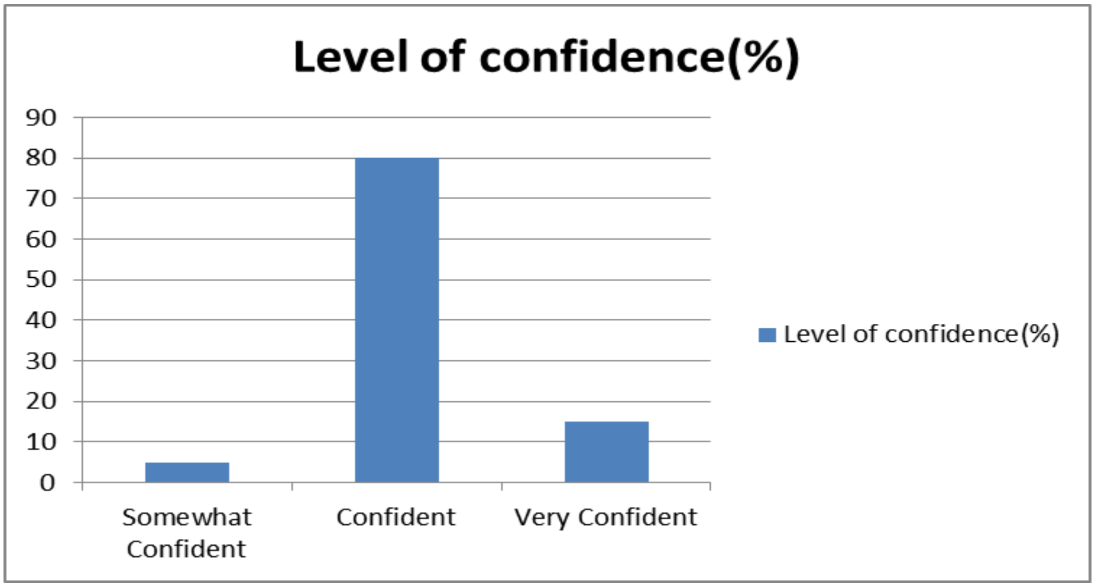


Figure 4.18: Correctness of the Algorithm for Selection of a Secure EAP method.

Similarly, when they (Experts) were asked how confident they are in the effectiveness of the algorithm for selection of a secure Extensible Authentication protocol (EAP) method, the results indicate that 70 % of the experts (65% confident and 5% very confident) belief in the effectiveness of the algorithm for selection of a secure Extensible Authentication protocol (EAP) method while 30 % of the experts were undecided. These results are shown in figure 4.19.

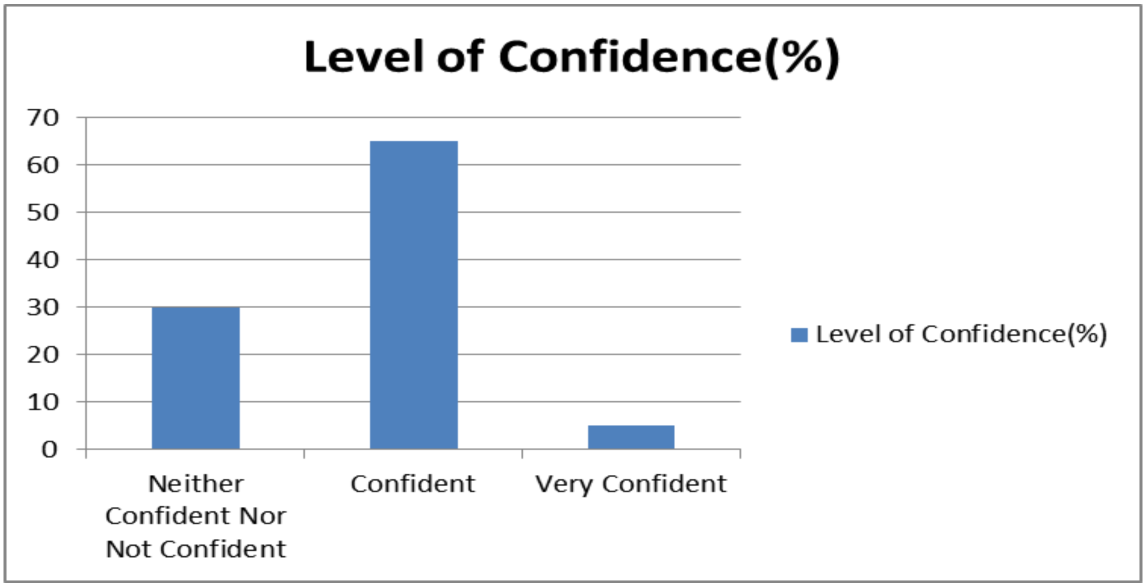


Figure 4.19: Effectiveness of the Algorithm for Selection of a Secure EAP Method.

Based on face validation results from experts, the researchers concluded that the model design was well thought and was consistent with the understanding of the experts.

4.6 Theoretical Analysis of the Model Concept Using Degenerate and Trace Tests

Table 4.23 shows results for a one component sub-model when type of influence is positive and a similar scenario when type of influence is negative**.** The following can be deduced from the table.

i. When attack susceptibility of the child component is low, medium or high, the attack susceptibility of the root/parent component is low, medium and high respectively when the type of influence is positive (+ve).

ii. When attack susceptibility of the child component is low, medium or high, the attack susceptibility of the root/parent component is high, medium and low respectively when the type of influence is negative (-ve).

Table 4.23: One Component Sub-model for both Positive and Negative Influence

Strength of component	**Strength of sub-model Root(P) When Relationship is +ve**	**Strength of sub-model Root(P) When Relationship is -ve**
Low [1]	Low [1]	High [3]
Moderate [2]	Moderate [2]	Moderate [2]
High [3]	High [3]	Low [1]

Table 4.24 shows a summary of results for a two component sub-model when type of influence is positive and a similar scenario when type of influence is negative**.**

The following can be deduced from the table.

i. When all the two child components have a low attack susceptibility the root/overall attack susceptibility is also low. This means the root/overall security is strong since relationship between attack susceptibility and security is of type negative.
ii. When one of the components has a high susceptibility than the other, the root/overall attack susceptibility leans towards the one with high attack susceptibility. This is consistent with Schneier's view that security of a system is as good as the weakest link (Schneier, 2000).
iii. When both components have moderate attack susceptibilities, the root/overall attack susceptibility is also moderate.
iv. Where one of the components has high attack susceptibility, and the other low attack susceptibility, the root/overall attack susceptibility is moderate.
v. When the relationship changes to type negative, the results are inverted.

Table 4.24: Two Component Sub-model for both Positive and Negative Influence.

Strength of component 1 (S1)	**Strength of component 2 (S2)**	**Strength of sub-model Root(P) when Relationship type +ve**	**Strength of Sub-model Root(P) when Relationship type -ve**
Low **[1]**	Low **[1]**	Low **[1.00]**	High **[3.00]**
Low **[1]**	Moderate **[2]**	Moderate **[1.67]**	Moderate **[2.33]**
Low **[1]**	High **[3]**	Moderate **[2.50]**	Moderate **[1.50]**
Moderate **[2]**	Low **[1]**	Moderate **[1.67]**	Moderate **[2.33]**
Moderate **[2]**	Moderate **[2]**	Moderate **[2.00]**	Moderate **[2.00]**
Moderate **[2]**	High **[3]**	High **[2.60]**	Low **[1.40]**
High **[3]**	Low **[1]**	Moderate **[2.50]**	Moderate **[1.50]**
High **[3]**	Moderate **[2]**	High **[2.60]**	Low **[1.40]**
High **[3]**	High **[3]**	High **[3.00]**	Low **[1.00]**

Table 4.25 shows a summary of results for a three component sub-model when type of influence is positive and a similar scenario when type of influence is negative**.**

The following can be deduced from the table.

i. When all the three components have high attack susceptibility, the root/overall attack susceptibility is high. Similarly, when all the three parameters have low attack susceptibility, the root/overall attack susceptibility is also low. Also where all the three components have moderate attack susceptibility, the root/overall attack susceptibility is moderate.

ii. When one of the three components have high attack susceptibility, the root/overall attack susceptibility leans towards that of the component having high attack susceptibility which is consistent with Schneier's view that security of a system is as good as the weakest link(Schneier,2000).

iii. For any given set of component input values, the results of situations where the relationship is of type positive(+ve) are the inversion of the results under the same component values if relationship is of type negative(-ve)

Table 4.25: Three Component Sub-model for both Positive and Negative Influence

Strength of Component 1 (S1)	**Strength of Component 2(S2)**	**Strength of Component 3(S3)**	**Strength of sub model Root(P) when Relationship type +ve**	**Strength of sub model Root(P) when Relationship type –ve**
Low **[1]**	Low **[1]**	Low **[1]**	Low **[1.00]**	High **[3.00]**
Low **[1]**	Low **[1]**	Moderate**[2]**	Moderate **[1.50]**	Moderate **[2.50]**
Low **[1]**	Low **[1]**	High **[3]**	Moderate **[2.20]**	Moderate **[1.80]**
Low **[1]**	Moderate**[2]**	Low **[1]**	Moderate **[1.50]**	Moderate **[2.50]**
Low **[1]**	Moderate**[2]**	Moderate**[2]**	Moderate **[1.80]**	Moderate **[2.20]**
Low **[1]**	Moderate**[2]**	High **[3]**	Moderate **[2.33]**	Moderate **[1.67]**
Low **[1]**	High **[3]**	Low **[1]**	Moderate **[2.20]**	Moderate **[1.80]**
Low **[1]**	High **[3]**	Moderate**[2]**	Moderate **[2.33]**	Moderate **[1.67]**
Low **[1]**	High **[3]**	High **[3]**	High **[2.71]**	Low **[1.29]**
Moderate **[2]**	Low **[1]**	Low **[1]**	Moderate **[1.50]**	Moderate **[2.50]**
Moderate **[2]**	Low **[1]**	Moderate**[2]**	Moderate **[1.80]**	Moderate **[2.20]**
Moderate **[2]**	Low **[1]**	High **[3]**	Moderate **[2.33]**	Moderate **[1.67]**
Moderate **[2]**	Moderate**[2]**	Low **[1]**	Moderate **[1.80]**	Moderate **[2.20]**
Moderate **[2]**	Moderate**[2]**	Moderate**[2]**	Moderate **[2.00]**	Moderate **[2.00]**
Moderate **[2]**	Moderate**[2]**	High **[3]**	Moderate **[2.43]**	Moderate **[1.57]**
Moderate **[2]**	High **[3]**	Low **[1]**	Moderate **[2.33]**	Moderate **[1.67]**
Moderate **[2]**	High **[3]**	Moderate**[2]**	Moderate **[2.43]**	Moderate **[1.57]**
Moderate **[2]**	High **[3]**	High **[3]**	High **[2.75]**	Low **[1.25]**
High **[3]**	Low **[1]**	Low **[1]**	Moderate **[2.20]**	Moderate **[1.80]**
High **[3]**	Low **[1]**	Moderate**[2]**	Moderate **[2.33]**	Moderate **[1.67]**
High **[3]**	Low **[1]**	High **[3]**	High **[2.71]**	Low **[1.29]**
High **[3]**	Moderate**[2]**	Low **[1]**	Moderate **[2.33]**	Moderate **[1.67]**
High **[3]**	Moderate**[2]**	Moderate**[2]**	Moderate **[2.43]**	Moderate **[1.57]**

High **[3]**	Moderate**[2]**	High **[3]**	High **[2.75]**	Low **[1.25]**
High **[3]**	High **[3]**	Low **[1]**	High **[2.71]**	Low **[1.29]**
High **[3]**	High **[3]**	Moderate**[2]**	High **[2.75]**	Low **[1.25]**
High **[3]**	High **[3]**	High **[3]**	High **[3.00]**	Low **[1.00]**

It was also observed that where all the eight components have low attack susceptibility the overall attack susceptibility is also low and overall security is high/strong. Similarly where all the eight components have high attack susceptibility the overall attack susceptibility is high and overall security is low/weak.

These observations indicate that the logic of the technique for propagation of component values maintains accuracy and consistency as required and that the model results are consistent with the design principles.

4.7 Results of Computerised Model Verification

The following are the observations made from the results obtained during the verification of the computerized model.

i. Where there are two components with all having a low attack susceptibility, the root/ overall security is strong.

ii. Where there are two components with one having a high attack susceptibility than the other, the root/ overall security leans towards the weaker one (the one with high attack susceptibility).This is consistent with schneier's view that security of a system is as good as the weakest link(Schneier,2000).

iii. Where there are two components with their attack susceptibilities both being moderate the root/ overall security is also moderate.

iv. Where there are two components with one having high attack susceptibility, and the other low attack susceptibility, the root/overall security is moderate.

v. Where there are two components with all having high attack susceptibility the root/overall security is weak.

vi. Where there are three components with all having high attack susceptibility, the root/overall security is weak.

vii. Where there are three components with all having low attack susceptibility, the root/overall security is strong.

viii. Where there are three components with all having moderate attack susceptibility, the root/overall security is also moderate.

ix. Where there are three components with one having high attack susceptibility, the root/overall security leans towards the weaker one i.e the one having high attack susceptibility.

x. Where there are three components with all having low attack susceptibility, the root/overall security is high.

xi. Where all the eight components have a low attack susceptibility the overall attack susceptibility is also low and overall security is high/strong.

xii. Where all the eight components have a moderate attack susceptibility the overall attack susceptibility is also moderate and overall security is also moderate

xiii. Where all the eight components have high attack susceptibility the overall attack susceptibility is also high and overall security is low/weak.

These observations are consistent with those of the dry run tests carried out on the conceptual model. Therefore, implementation of the model's logic for propagation of component values is correct and maintains consistency.

4.8 Analysis of Operational Validation Using Parameter Variability Sensitivity

Fifty (50) experts were identified, out of which 33 responded representing 66 % response rate. According to Mugenda & Mugenda (2003) a response rate of 66% is good enough. All respondents had experience in the area of WLAN security with experience of above 3 years. They were all competent in network security areas with 97% being highly competent in WLAN security as shown in table 4.26.

Table 4.26: Level of Practitioners Competence in Various IT security Areas

IT Security Area	Moderately Competent	Highly Competent
Intrusion analysis	39.4	60.6
System administration	12.1	87.9
Incident handling	24.2	75.8
Penetration testing	36.4	63.6
Network security	9.1	90.9
WLAN security	3.0	97.0

4.8.1 Practitioners Belief in Accuracy of the Prototype Results/outputs

Practitioners were asked to indicate the extent they agree with the accuracy of the results/outputs from the prototype**.** This question attempted to elicit practioners' belief in the accuracy of the model results. Table 4.27 shows the specific responses for each result/output from the prototype. The responses indicate experts' high degree of belief on the accuracy of the model results.

Table 4.27: Practitioners' Level of Belief in the Accuracy of the Model Results

Result/output	**Strongly Agree**	**Agree**	**Neither Agree Nor Disagree**
Strength of Wireless Path security for various component inputs(Cipher suite, Authentication and access control mechanism)	51.5	48.5	
Strength of Front-end System software for various component inputs(Client Driver, Client Utility, Access point firmware)	57.6	39.4	3.0
Strength of Back-end Authentication Systems for various component inputs (Authentication Server, User database, Authentication Credentials).	27.3	66.7	6.1
Strength of Wireless Trusted Computing Base Security for various component inputs	48.5	48.5	3.0
Strength of Attack Susceptibility for various component inputs	27.3	72.7	
Strength of Wireless Authentication and access control Security for various component inputs	42.4	57.6	
Remarks/Recommendations provided for various component inputs	60.6	30.3	9.1
Extensible Authentication Protocol (EAP) method recommended for various parameter inputs	45.5	42.4	12.1

4.8.2 Practitioners Belief in Usefulness of the Model's Results

Practitioners were asked to indicate the extent they agree with specific statements about the model. The question was attempting to elicit experts' belief on the usefulness of the model's results for the intended purpose within its domain of applicability. As shown from table 4.28 the responses indicate that the experts believe the model results are useful for the intended purpose within its domain of applicability.

Table 4.28:Practitioners' level of belief in the usefulness of the model results

	Strongly Agree	Agree	Neither Agree nor Disagree
The model correctly provides results useful for design of security features for WLAN Authentication and access control	63.6	30.3	6.1
The model correctly provides results useful for selection of security features for WLAN Authentication and access control	39.4	51.5	9.1
The model correctly provides results useful for configuration of security features for WLAN Authentication and access control	45.5	42.4	12.1

4.8.3 Areas of Model Application

The researchers also wanted to elicit responses on areas where practitioners could apply the model and so when they (practitioners) were asked how the model would help them in their work, they gave the following suggestions;

i. Helpful when setting wireless LAN security configurations

ii. Will help security administrators and network engineers to decide on the most secure cipher suite and control mechanisms to employ and also the client driver, client utility and access point firmware to map to give their WLANs the best protection.

iii. Will help assess the security of University's network for the purpose of continuous improvement

iv. Useful for security analysis and design of wireless networks

v. Can be used as an audit tool for WLAN security and then recommend an appropriate security for an organization's security

vi. Can use it to control attack susceptibility

vii. Can be used to establish a suitable EAP method based on organisation's resources.

viii. Can be used to carry out research on WLAN security/Data collection by researchers.

ix. Can be used in designing a secure WLAN that authenticates users and devices securely.

x. Useful guide for Selection of WLAN features that would give the best security.

xi. Measure and monitor security level of a WLAN

xii. Establish highly vulnerable security features and configurations

xiii. Can be used as a measurement tool for WLAN security by network administrators

xiv. Can help visualize the security implications of selecting certain security features and configurations

xv. To advice WLAN users on their configurations for their devices

4.8.4 General Thoughts from the Practitioners

The researchers wanted to elicit general thoughts concerning the model from the experts and therefore asked them to provide general thoughts on the model. Some of the general comments provided were;

i. Model is helpful for configuring security for WLANs

ii. Based on test results, the model managed to offer correct security regarding WLAN.

iii. The model's output behavior is relatively accurate for the intended purpose

iv. The model can help inexperienced network administrators differentiate between secure and insecure features and configurations in a WLAN

v. Model's output behavior is realistic

vi. The model can be used to improve security of WLANs

vii. The model combines the different authentication mechanisms with a corresponding cipher suite to provide a secure combination.

viii. Model results are reasonable.

ix. Model represents reality.

x. This model will be used by practitioners across several public WLANs to explain implementation problems and inform implementation interventions.

4.9 Partial Validation Using Data (Model Application)

Figure 4.20 shows a graphical representation of operational wireless path security levels for each of the 31 Universities that participated in the preliminary survey. The results indicate that most Universities have implemented highly vulnerable wireless path security features and configurations. Only two Universities have high security levels for this parameter.

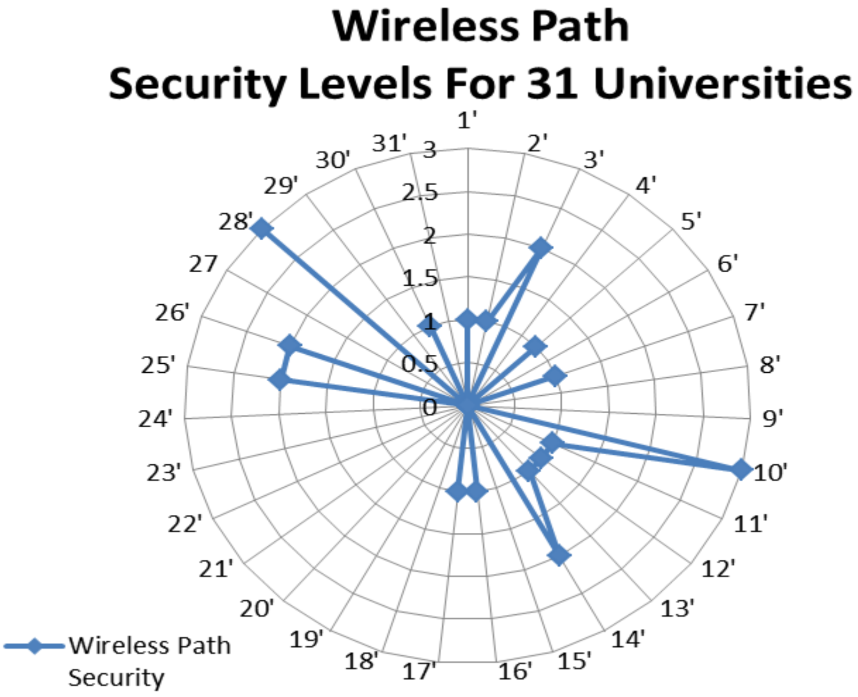


Figure 4.20: Operational wireless path security levels for 31 Universities

Figure 4.21 also shows a graphical representation of operational backend authentication systems security levels for each of the 31 Universities that participated in the preliminary survey. The results indicate that most Universities have implemented highly vulnerable backend authentication systems security features and configurations. Few Universities have moderate (level 2) security level and none has high (level 3) level of security for this parameter.

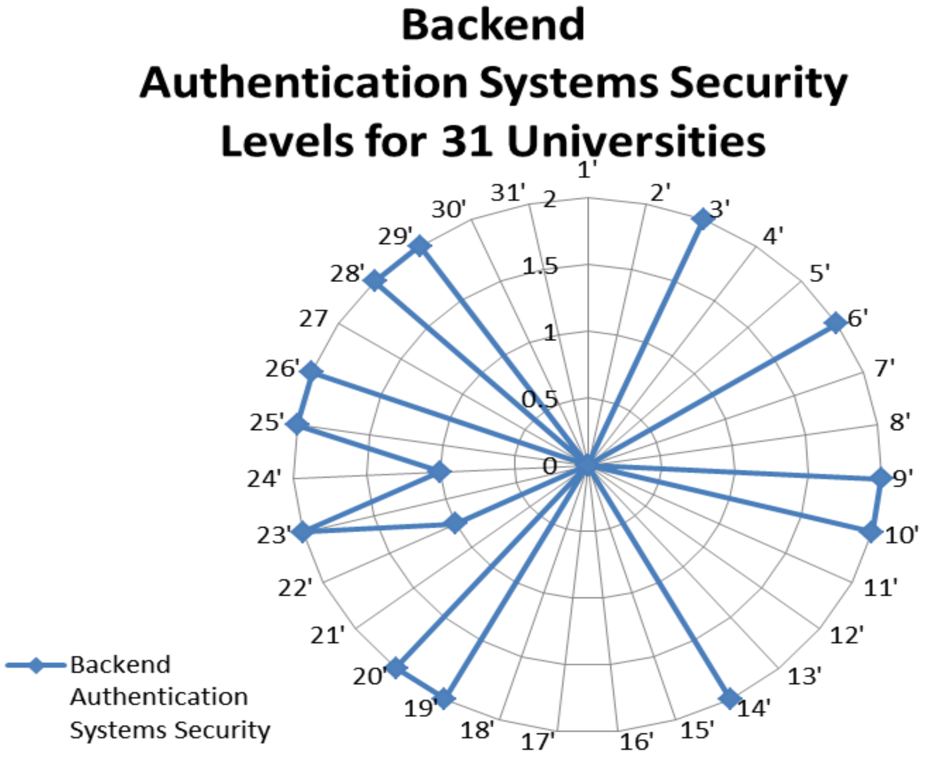


Figure 4.21: Operational Backend Authentication Systems Security Levels for 31 Universities

Though the data available was not sufficient to enable researchers apply full functionality of the model, it was used to provide insights in regard to application/usability of the model.

4.10 Discussion of Results

This section provides a discussion of the results presented in section 4.1 to 4.9. The discussion focuses on four research questions as per section 1.4, that the thesis sought to answer.

RQ1: What are the implementation specific vulnerabilities that may contribute to poor WLAN authentication and access control security performance in selected university WLANs in Kenya?

While answering this question, the researcher had to first establish the security features and configurations implemented on selected university WLANs and then benchmark with the literature reported vulnerabilities on the security features and configurations identified.

Based on results presented in section 4.1 and analyzed via the developed model as presented in Figure 4.20 and 4.21, most Universities have implemented highly vulnerable wireless path security and back-end authentication systems features and configurations. Only two Universities have high security levels for wireless path. Few Universities have moderate security level and none has high level of security for back-end authentication systems. This means that many of these implementations are susceptible to unauthorized access/connection, sniffing of confidential data such as authentication traffic and WLAN spoofing/cloning as described by (Hoffman,2006;Alikira,2012;Mwathi et al,2016) in their prior studies.

RQ2: What is the attack susceptibility of the vulnerabilities exploited by known attacks on WLAN cipher suite, authentication and access control mechanisms, end-user and server system software that implement authentication and access control in a WLAN?

Several vulnerabilities exploited to launch attacks on WLAN cipher suite, authentication and access control mechanisms, end-user and server system software that implement authentication and access control in a WLAN were discussed in section 4.2. The following can be deduced from the findings:

- The exploitable scope of WLAN attacks is bound to network stack and the attackers path to the vulnerable component is at the data link layer.
- Most of the attacks to WLAN do not require user interaction.
- Most attacks do not require attacker to be authenticated or have any privileges.
- In all the attacks, the vulnerable component is the same as impacted component
- Attack susceptibility of WLAN attacks are mainly influenced by attack complexity (AC), confidentiality(C), integrity (I) and availability (A) impacts.

These deductions imply that security features and configurations selected for implementing authentication and access control are key to establishing a trusted network consistent with the argument of (Li-Chuan et al, 2009).

RQ3: What are the relevant architectural components of consideration for developing a simulation model for selection or design as well as configuration of security features for public WLAN authentication and access control?

Relevant architectural components for developing a simulation model for selection or design as well as configuration of security features for public WLAN authentication and access control were established through literature analysis. The related security features and configurations were identified through descriptive survey. The artifacts discussed in section 2.10 and related features or configurations discussed in table 4.11 to 4.18 are key components of a simulation model for WLAN authentication and access control implementation. Many approaches to design and evaluation of security on WLANs e.g white-hat attacks on implementations and analysis of protocols (David et al, 2004) have established that it is impossible in practice to build a perfectly secure system. There is therefore much to be gained from employing a model-based approach in establishing an approximate security level one can expect from a particular implementation of WLAN authentication and access control. By employing a model that identifies the strength of security influence a component feature or configuration has over another, an implementer can analyze the effect of implementing one security feature/configuration versus another. When alternatives are possible e.g. WEP or CCMP, pre-shared key or IEEE 802.1x, one of the security features is implemented because the implementer will have established it as providing better security than the other.

RQ4: Is the developed model valid for its intended purpose over the domain of its intended applicability?

In responding to RQ4 which sought to determine the validity of the developed model for its intended purpose over the domain of its intended applicability, the researcher relied on results from various validation approaches. The model concept was validated based on expert intuition and theoretical analysis while its operation was validated by practitioners after using and experimenting with the model prototype.

Results from validation using expert intuition presented in section 4.5 show expert confidence in the model as high on average. This indicates that the theories and assumptions underlying the model are correct and that the model's representation of the problem entity, its structure, logic and mathematical causal relationships are “reasonable’ for the intended purpose of the model .This implies that the developed model is an accurate representation of the problem domain as envisaged by (Sargent, 2011).

Results presented in section 4.6 on theoretical analysis show that the combination and propagation mechanism used to aggregate attack susceptibilities in the model obeys key operational laws. For example, whenever a child node’s influence is positive on a parent node, and its attack susceptibility is high, then the parent node will have high susceptibility. Similarly whenever a child node’s influence on the parent node is positive, and its attack susceptibility is low, then the attack susceptibility of parent node will be low. In contrast, whenever a child node’s influence is negative on parent node and its attack susceptibility is high, the susceptibility of the parent node will be low. On the same note, whenever a child node’s influence is negative on the parent node and its attack susceptibility is low, the susceptibility of the parent node will be high. This indicates that the model behavior is satisfactory in relation to study objectives as envisaged by Balci (1998).

Results presented in section 4.8 on operational model validation using parameter variability-sensibility analysis show practitioner confidence in the accuracy, usefulness and applicability of the model as high on average. This indicates that the model behavior is valid for its intended purpose as visualized by (Kleijnen, 1995; Balci, 1998 & Sargent, 2011).

The results from all validation approaches in general indicate that the model developed is valid for its intended purpose over the domain of its intended applicability. Particularly, it enables design, selection and configuration of security features for WLAN authentication and access control. The validation process therefore created enough model confidence necessary for its results to be accepted as envisioned by (Kleijnen, 1995; Stewart, 1997; Balci, 1998 & Sargent, 2011).

Results presented in section 4.8 on model application indicate poor implementation of authentication and access control security in public WLANs particularly universities in Kenya. This is consistent with results from ealier works by (Mwathi et al, 2016).

To eliminate extremely vulnerable security features from their implementation, there is need for administators in organisations implementing public WLANs to develop a policy that prohibits selection and configuration of highly vulnerable security features especially those captured by the model. This is in order to avert possible unauthorized access to their WLANs, sniffing of confidential data such as authentication traffic and WLAN spoofing/cloning.

4.11 Research Contribution to Enhancement of Knowledge

This section provides details of the main contributions and achievements that were realized in this research. The contributions and achievements which add to the body of knowledge are either theoretical or technical/practical in nature.

4.11.1 Theoretical Contributions

Petre and Rugg (2010) argue that for one to characterize a theoretical contribution as either significant or not, one needs to show the significance of the findings or the contributions. In other words, do the findings or contribution matter to anyone? Additionally, one should provide the implications of the contribution to the body of knowledge in general and provide any limitation to generalization. Theoretical contributions are either methodological or non-methodological in nature and are discussed next starting with non-methodological contributions;

4.11.1.1 Simulation Model for Implementing WLAN Authentication and Access Control

One of the main deliverables of this work is a simulation model that enables appropriate design or selection of security features and their configuration for WLAN authentication and access control in public WLANs. This is a major contribution because no previous studies have been done with a view of developing a simulation model that can enable an implementer to visualize the security level expected from implementing a set of security features and their configurations. The model developed, whose researcher and practitioner confidence was on average high provides a basis for understanding determinants of WLAN authentication and access control security.

The key contributions relating to the model include:

(a)Conceptual architecture and value function tables that map security features to security levels

As established from literature sources, there is a gap in relation to comprehensiveness of available approaches to WLAN authentication and access control implementation. The model addresses the breadth and depth of this gap by identifying eight artifacts and developing a value function tables that map various security features and configurations to a security level for each artifact. This enables an implementer to visualize the security level expected from implementing a certain security feature in relation to another. The relationship between the model components has a significant theoretical power.

Value function tables manage complexity of security configurations in WLANs via reduction of state space which involves limiting one's choices of security features during configuration. With a set of **n** components each with ***x*** states, one is theoretically faced with an infinite number of possible configurations. In this case however, the value function tables provide ***8*** components each with **4** possible states leading to $\mathbf{4^8}$ possible states. Limiting the components and their states simplifies the configuration process and makes it tractable.

(b)An Algorithm for combining and propagating model input values

The algorithm for combining and propagating model input values aggregates security values of various security features and configurations selected to provide an overall security of an implementation. This simulation effect provided by the algorithm is a significant contribution because it enables an implementer to visualize the security level expected from implementing a set of security features and their configurations. This model therefore fills the simulation gap missing in related works.

The simulation effect is particularly crucial because it enables the model addresses the flexible nature of the provisions of IEEE 802.11i (2004) and IEEE 802.11w (2009) security standards by enabling an implementer to analyze the effect of implementing one security feature or configuration versus another. When alternatives are possible e.g. WEP or CCMP, pre-shared key or IEEE 802.1x, one of the security features is implemented because the implementer will have established it as providing better security than the other. This work therefore expands previous research efforts to make wireless networks more robust against attacks associated with authentication and access control.

(c)An algorithm for EAP method selection

The flexible nature of the provisions of IEEE 802.11 standards and supporting technologies create potential for selection of vulnerable EAP authentication method for use with IEEE 802.1x.The research addresses this gap by developing an algorithm that enable implementers to choose from five secure EAP methods based on implementation environment based considerations. These considerations are infrastructure support for IEEE 802.1x,CCMP, TKIP and digital signatures, need to protect identity of communicating parties, difficulty in enforcing password security by users and need to use legacy authentication methods.

4.11.1.2 Methodological Contribution

One major methodological contribution of this work is in the use of attack tree modeling combined with CVSS in analyzing severity of vulnerabilities in a system. Knowledge of severity of an attack is particularly necessary because it helps determine priority of response through selection and configuration of security features that are consistent with the priority.

This approach was particularly important in this research considering that one of the gaps emanating from the literature indicated that besides having several attacks discovered through various experimental team based approaches that try to compromise a WLAN, severity of these attacks had not been studied.

This methodology provides some important guidelines for researchers interested in WLAN security, network security in general and related areas. Specifically researchers interested in attack tree analysis model, and/or CVSS model will find the methodology used in this research useful.

4.11.2 Technical and Practical Contributions

The results of this study have significant technical and practical contributions:

4.11.2.1 Implementation of Theoretical Principles

Petre and Rugg (2010) explain that the implementation of theoretical principles is an important contribution to the body of knowledge. In this work several theoretical principles were pooled together and formed important practical contributions which were demonstrated through the implementation of a prototype that enables one to predict security levels on WLAN authentication and access control implementation and implementation of an algorithm for selection of EAP method. Examples of these theoretical principles include the use of attack tree analysis, common vulnerability scoring system, security metrics model, client-server architectures, trusted computing base and production model. These theoretical principles were applied in one coherent practical implementation which received on average a high rating from experts. The implementation fills a technical gap since no application system-level approach currently exists that can indicate the level of security provided by a particular WLAN authentication and access control implementation.

Use of an expert system shell to implement some key aspects of the model provides a re-usable approach to knowledge representation. Many implementations of expert systems exist. These systems have several known benefits such as their ability to represent knowledge naturally, their ability to deal with incomplete and uncertain knowledge , self-documentation, separation of knowledge from processing which makes it possible to develop different applications using the same expert system shell. Besides these benefits, network security area has not utilized them in solving problems related to security implementations especially where incomplete and uncertain knowledge is used for security decision making. This approach can therefore be embraced by researchers interested in this area especially when solving security implementation decision making problems.

The implementation code for the function for propagating values in the model which was implemented in javascript is shown in appendix 6 while the rule base/knowledge base code behind the algorithm for selection of EAP method is shown in appendix 7.

4.11.2.2 Addressing Practitioners Concerns

When practitioners were asked how the model can help them in their work, they gave the following applications which indicate the practical significance of the model;

i. Helpful when setting wireless LAN security configurations
ii. Will help security administrators and network engineers to decide on the most secure cipher suite and control mechanisms to employ and also the client driver, client utility and accesspoint firmware to map to give their WLANs the best protection.
iii. Will help assess the security of University's network for the purpose of continuous improvement
iv. Useful for security analysis and design of wireless networks
v. Can be used as an audit tool for WLAN security and then recommend an appropriate security for an organization's security
vi. Can use it to control attack susceptibility
vii. Can be used to establish a suitable EAP method based on organisation's resources.
viii. Can be used to carry out research on WLAN security/Data collection by researchers.
ix. Can be used in designing a secure WLAN that authenticates users and devices securely.
x. Useful guide for Selection of WLAN features that would give the best security.
xi. Measure and monitor security level of a WLAN
xii. Establish highly vulnerable security features and configurations
xiii. Can be used as a measurement tool for WLAN security by network administrators
xiv. Can help visualize the security implications of selecting certain security features and configurations
xv. To advice WLAN users on their configurations for their devices

4.12 Achievement on WLAN Authentication and Access Control Implementation Advancement.

This research has made several achievements in relation to WLAN security implementation advancement.

4.12.1 A Tool for Implementing WLAN Authentication and Access Control

Validation results from practitioners established that the model developed is suitable for its intended purpose over the domain of its intended applicability. This means that practitioners can use the model to design or select appropriate security features and their configuration for WLAN authentication and access control in the context of large public WLANs such as Universities. In addition practitioners identified many more model applications such as evaluation of WLAN authentication and access control security and others which were highlighted in the previous section

4.12.2 Abstraction of Complex WLAN Security

Abstraction in this context means to represent complex relationships using simple but representative mechanisms to hide complexities so that WLAN security implementers can have a simple model of the security system of a WLAN. Dijkstra (1969) defines computer science as ‘study and management of complexity’ (Quoted by Peter Wegner, 1976). Security configuration management of any system is generally intractable because a complete understanding of the system components and its complex relationships is intractable. The WAACS model helps manage complexity of deploying WLAN security because it makes it easy for technical people with little skills deploy fairly secure WLAN authentication. The WAACS model applies three different ways to reduce complexity in selection of security features: **reduction of state space** (4^8 possible states), **using simple operations** (simple algorithm for propagation of values**)** and **forming hierarchies and relationships among components.** These approaches make the model an effective communication tool among network administrators in selection, design and implementation of security features for WLAN authentication.

4.12.3 Complementation of Current Approaches to WLAN Security Configuration

The model complements experience and documentation which is commonly employed by network administrators in the course of their day to day work to reduce the complexity of configuration management. According to Yizhan (2006), many network security administrators use their experience of past solutions and documentation to configure security of network equipment. Once they establish that it is proper to use past experience or documentation in the environment at hand, they repeat those routine actions or follow instructions of the documentation (documented procedure or a wizard for installation) without doing dependency analysis. Selection and configuration of security features is mainly guided in most WLAN implementations by following a documented procedure or a wizard for installation which enables network administrators bypass the "hardness" of dependency analysis. For example, suppose a network administrator needs to configure a new access point's security settings. The installation guide may instruct one to select the cipher suite first, then authentication method. The network administrator may just follow these instructions without bothering to analyze the cumulative effect of the cipher suite-authentication method security features selected on overall security.

Use of documentation and experience approaches alone is not sufficient because:

(i) Documentation is not always 100% accurate due to errors in the software, human error, time and cost of developing detailed installation/configuration wizards by equipment manufacturers.

(ii) Documentation does not address all possible platforms because WLANs may comprise equipment/components from various developers and vendors. Even where the equipment have been tested and verified fully by their developers for any platform, it is possible that they can fail to function as specified in a particular platform.

(iii) Experience may also not always be 100% accurate and in a very dynamic environment, it is possible to misconfigure the system by simply following instructions from documentation or experience that do not apply to the system's current state.

(iv) WAACS, being a simulation model, complements documentation and experience by providing implementers a platform that enables them evaluate the overall effect of a set of security features and configurations on security before embarking on actual configuration.

CHAPTER 5: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

This chapter provides a summary of the research carried out. In particular it revisits the focus of the problem, main objectives, approaches followed and the main results, contributions, achievements, study limitations ,recommendations for furtherance of this work and research conclusions. Emphasis is laid on WLAN authentication and access control security focusing on the theoretical and practical implications.

5.1 Overview of the Research

Poor implementation of authentication and access control security in large public WLANs such as those in Universities was the main problem addressed in this research.

The problem has two sub-components which are listed here below;

- Lack of appropriate model that enables appropriate design or selection of security features and their configuration for WLAN authentication and access control in a public WLAN.
- Implementation (selection and configuration) of vulnerable cipher suite, authentication and access control mechanisms, end-user and server system features.

The two sub-components formed the basis of the objectives namely; investigating IEEE 802.11 implementation specific vulnerabilities that may contribute to poor WLAN authentication and access control security performance in WLANs in Kenyan Universities, analysis of security offered by various WLAN cipher suites, authentication and access control mechanisms, end user and server system software used in WLAN authentication and access control , establishing relevant architectural components and using them to specify and prototype a simulation model that enables appropriate design or selection of security features and their configuration for WLAN authentication and access control in the context of large public WLANs such as Universities, and finally validating the model for the intended purpose over the domain of intended applicability.

The study conducted a rigorous literature review with a view of understanding the main ideas within this problem area. This culminated in identification of theoretical gaps and formulation of conceptual architecture.

Issues to be tackled were identified .This led the focus of the research to descriptive and literature survey and analysis .An attack susceptibility analysis mechanism called CVSS was used to analyze attack susceptibilities of security features and configurations that can be implemented in a public WLAN.

Results of descriptive survey and attack susceptibility analysis led to the development of model function tables and algorithms. A prototype was developed for the purpose of validation. A large portion of the research was dedicated to validation of the wireless authentication and access control security (WAACS) model involving expert elicitation and theoretical analysis approaches.

Results from various validation approaches indicate that the model developed enables design or selection and configuration of security features for WLAN authentication and access control.

Conceptual model validation established that the theories and assumptions underlying the model concept were correctly applied. It also established that the model's representation of the problem entity, its structure, logic and mathematical causal relationships are reasonable for the intended purpose.

Operational model validation results established that the model's output behaviour has sufficient accuracy required for its intended purpose over the domain of its intended applicability.

These results therefore indicate that the model developed facilitates implementation of WLAN authentication and access control security in the context of large public WLANs such as universities.

The key outcomes of the study and hence our major contributions are summarized as follows:

1. Simulation Model for implementing and evaluating WLAN authentication and access Control security. The model includes:
    - Value function tables that map security features to security levels
    - An Algorithm for combining and propagating model input values
    - An algorithm for EAP method selection

2. Methodological contribution: we introduced the use of attack tree modeling combined with CVSS in analyzing severity of vulnerabilities in a system.
3. Practical contributions: we implemented theoretical principles via development of a prototype. The prototype is a working tool that can be used to address many practical concerns related to WLAN authentication and access control security.

This research made several achievements in relation to WLAN security implementation advancement. These include:

- Providing an enabling tool for implementing and evaluating WLAN authentication and Access Control Security.
- Abstraction of Complex WLAN Security.
- Complementation of Current approaches to WLAN security Configuration.

5.2 Research Conclusions

This study, which provides several opportunities for future research, is indeed valuable. In this section, the researcher presents a summary of the key research questions whose key outcomes constitute major contributions. The study attempted to answer these questions through descriptive survey, literature survey and analysis, expert elicitation and theoretical analysis.

RQ1: What are the implementation specific vulnerabilities that may contribute to poor WLAN authentication and access control security performance in selected university WLANs in Kenya?

The results collected through a descriptive survey indicate that many universities have implemented highly vulnerable wireless path security and back-end authentication systems features and configurations. This means that many of these implementations are susceptible to unauthorized access/connection, sniffing of confidential data such as authentication traffic and WLAN spoofing/cloning.

The researcher also identified various security features and configurations implemented on various artifacts that influence WLAN security during authentication and access control.

RQ2:What is the attack susceptibility of the vulnerabilities exploited by known attacks on WLAN cipher suite, authentication and access control mechanisms, end-user and server system software that implement authentication and access control in a WLAN?

Several vulnerabilities exploited to launch attacks on WLAN cipher suite, authentication and access control mechanisms, end-user and server system software that implement authentication and access control in a WLAN were analyzed based on common vulnerability scoring system (CVSS).

The main outcome from this question was attack susceptibilities (CVSS scores)of security features and configurations implemented on typical public WLANs .The results of CVSS analysis were used to develop model function tables.

RQ3: What are the relevant architectural components of consideration for developing a simulation model for selection or design as well as configuration of security features for public WLAN authentication and access control?

Relevant architectural components/artifacts for developing a simulation model for selection or design as well as configuration of security features for public WLAN authentication and access control were established through literature analysis. Not only are the components clear, the strength of specific component value and overall effect of a combination of component values can be established.

The related security features and configurations were identified through a descriptive survey. Value function tables that map security features or configurations to security levels for each of the architectural components/artifacts were developed. Two key model algorithms developed to operationalize the model are: the algorithm for combining and propagating model input values and algorithm for EAP method selection.

RQ4: Is the developed model valid for its intended purpose over the domain of its intended applicability?

Results from validation using expert intuition indicate researcher and practitioner confidence in the model as high on average. This indicates that the theories and assumptions underlying the model are correct and that the model's representation of the problem entity, its structure, logic and mathematical causal relationships are “reasonable’ for the intended purpose of the model.

Results from theoretical analysis show that the combination and propagation mechanism used to aggregate attack susceptibilities in the model obeys key operational laws. This indicates that the model behavior is satisfactory and that it is consistent with study objectives.

Therefore, the model developed, which is a major research contribution, facilitates implementation of WLAN authentication and access control security in the context of large public WLANs such as universities.

This research has demonstrated that deploying WLANs because of their convenience and ease of deployment is not good enough. Given the potential loss that an organization can incur due to attacks, a good understanding of the important WLAN security components (Trusted computing base) and relative security level provided by a combination of security features specific to the component is useful to enable implementers optimize WLAN security based on their resources and level of security required.

5.3 Limitations

The main limitations of the model developed are:

i. The model developed relies on user supplied data. When used to audit security level, it requires the user to collect data about an implementation using other tools and then use this data to supply input to the model. Though the main application of the model is decision making, when used for audit, it would be better for it to mine data directly from the devices.

ii. The Model provides qualitative outputs on an ordinal scale. Although the qualitative outputs are sufficient for decision making, quantitative outputs are more accurate.

5.4 Recommendations for Further Work

This research work has made several contributions to the body of knowledge, however due to some of the specified limitations some few areas have the potential to be advanced further. These areas are highlighted here:

i. Developing a quantitative model: The model presented in this study is largely qualitative. However, quantitative models are more accurate because they provide results with exact values unlike qualitative ones like this model which gives values of low, medium and high. Use of Bayesian Belief Network (BBN) would be an important approach to pursue.

ii. The model developed relies on user supplied data. Through further research, the model can be improved so that it relies on data mined directly from devices without raising ethical issues of intrusion.

iii. Evaluation of the usability and generalizability of the model: Based on validation results especially from practitioners, we can deduce that the developed simulation model will help improve WLAN security levels through selection, design and configuration of more secure features for WLAN authentication and access control. However, this has not been proven. To address this concern, a usability experiment can be done to compare security improvements in a set of WLANs applying the model (experimental group) and another set of WLANs not applying it (control group).To improve the generalizability of the model, it can again be validated using a different set of practitioners in different environments based on the method employed in this research.

5.5 Policy Recommendation

The results of model validation indicated that most Universities have implemented highly vulnerable wireless path and backend authentication systems features and configurations. Particularly few Universities have moderate wireless path security level and none has high level of security for back-end authentication systems.

To eliminate extremely vulnerable security features from implementation, there is need for administators in organisations implementing public WLANs to develop a policy that prohibits selection and configuration of highly vulnerable security features especially those captured by the model. This is in order to avert possible unauthorized access to their WLANs, sniffing of confidential data such as authentication traffic and WLAN spoofing/cloning.

5.6 Relevant Publications and Associated Conferences

Book Chapters

Mwathi, D., Okelo-Odongo., W. and Opiyo., E. (2014). Wireless LAN (WLAN) hacking tools in developing countries. In: W.Okelo-Odongo, E. Opiyo, and E.Ayienga (Eds), *Trends in distributed computing applications: Real life ongoing research work,*pp 125-136.University of Nairobi: School of computing and informatics. ISBN 978-9966-074-13-3.

Mwathi, D., Okelo-Odongo., W. and Opiyo., E. (2014).). Dangerous wireless local area network (WLAN) risks students & university employees need to know about. In: W.Okelo-Odongo, E. Opiyo, and E.Ayienga (Eds), *Trends in distributed computing applications: Real life ongoing research work*, pp. 76-84, University of Nairobi: School of computing and informatics. ISBN 978-9966-074-13-3.

Journal Publication

Mwathi, D., Okelo-Odongo., W. and Opiyo., E. (2017).Vulnerability Analysis of 802.11 Authentication and Encryption protocols: CVSS Based Approach. In: *International Research Journal of Computer Science.* [Online] Vol. 4*(6),pp16-23.* Available *at: http://www.irjcs.com/.*

Mwathi, D., Okelo-Odongo., W. and Opiyo. E. (2016). Selection of EAP Authentication Method for use in a Public WLAN: Implementation Environment Based Approach. In:*International Research Journal of Computer Science.* [Online] Vol. *3(5), pp.47-52.* Available *at: http://www.irjcs.com/.*

Mwathi, D., Okelo-Odongo., W. and Opiyo., E. (2016). Algorithm for Selection of EAP Authentication Method for Use In A Public WLAN. In: J*ournal of Emerging Trends in Computing and Information Sciences*. [Online] Vol *7(6), pp.311-316.* Available at: *http://www.cisjournal.org/.*

Conference proceedings

Mwathi, D., Okelo-Odongo, W. and Opiyo, E. (2015). Attack Susceptibility of Known Attacks on IEEE 802.11 Public WLAN. *Proceedings of Chuka University 2nd International Research Conference.*

Mwathi, D., Okelo-Odongo, W. and Opiyo, E. (2014).Dangerous Wireless Local Area Network (WLAN) Risks Students & University Employees Need to Know About. *Trends in Distributed Computing Applications: Real life ongoing research work, 2014*

Mwathi, D., Okelo-Odongo, W. and Opiyo, E. (2014).Wireless LAN (WLAN) Hacking Tools in Developing Countries: Trends in Distributed Computing Applications: Real life Ongoing Research Work.

REFERENCES

Aboba, B. and Simon, D. (1999). Point to point EAP TLS Authentication Protocol. *The Internet Society*.[Online].Available at: https://www.ietf.org/rfc/rfc2716.txt [Accessed 30 June.2013].

Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J. and Levkowetz, H. (2004). Extensible Authentication Protocol (EAP).*The Internet Society* [Online]. Available at: https://tools.ietf.org/html/rfc3748[Accessed 30 June.2013].

Agni, C. Azween, A. and Low-Tan, J. (2008). Simulation of EAP method selection and negotiation mechanism. In: *Proceedings of the 3rd International Symposium on Information Technology*. [Online] Kuala Lumpur: IEEE, Vol 3, pp. 26-29. Available at: http://ieeexplore.ieee.org/document/4632025/citations[Accessed 30 June 2013].

Aircrack-ng, (2010). Aircrack-ng. [Online].Available at: https://aircrack-ng.org[Accessed 20, Apr. 2014].

AirDefense. (2006).*Wireless Protection for the Mobile Enterprise*.[Online] Available at: www.airdefense.net[Accessed 30 July. 2013].

AirTight Networks. (2010).*Windows 7 Virtual Wi-Fi: The Easiest Way to Install a Rogue AP on Your Corporate Network.* [Online].*Available at:* https://www.windows-7-virtual-wifi-the-easiest-way-to-install-a-rogue-ap-on-your-corporate-network [Accessed 30 Dec. 2014].

Alikira, R. (2012).*Evaluation of WLAN security and Performance.* [Online] Munich: GRIN Verlag. Available at http://www.grin.com/en/e-book/205389[Accessed 30 Dec.2014].

Amosa, B., Orisawale, B., Kawonise, K., Fabiyi, A. and Fabiyi, A. (2015). Development of a Web Based Expert System for Diagnosis and Management of Childhood Pneumonia. *International Journal of Science and Advanced Technology,* Vol 5(12), pp. 7-18.

Andy, C., Junfeng, Y., Benjamin, C., Seth, H. and Dawson, R. (2001).An Empirical Study of Operating System Errors. In: *Proceedings of Symposium on Operating Systems Principles,* Montana: ACM.

Anh, N. and Shorey, R. (2005).Network sniffing tools for WLANs: merits and limitations. In: Proceedings of International Conference on Personal Wireless Communications, Kuala Lumpur: Institute of electrical and electronic Engineers. Available at: http://ieeexplore.ieee.org/document/[Accessed 30 June 2013].

Arkko, J. and Haverinen, H. (2006). Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA). *The Internet Society.* [Online]Available at: https://www.ietf.org/rfc/rfc4187.txt [Accessed 30 June.2013].

Armstrong, J. (1985). *Long-term Forecasting: From Crystal Ball to Computer* .2nd ed).New York: John Wiley.

Ashton, R. (1986).Combining the Judgments of Experts: How Many and Which Ones. *Organizational Behavior and Human Decision Processes*, Vol 38(3), pp.405-414.

Asokan,N.,Valtteri, N. and Kaisa, N.(2002).Man-in-the-Middle in Tunneled Authentication Protocols. *International association for cryptology research.* [Online] Available at: http://eprint.iacr.org/2002/163/ [Accessed 30 Dec. 2013].

Balci, O. (1995). Principles and Techniques of Simulation Validation, Verification, and Testing. In: Proceedings of the 1995 Winter Simulation Conference, Piscataway: Institute of Electrical and Electronics Engineers, pp. 147–154.

Batchelor, R. and Dua, P. (1995). Forecaster Diversity and the Benefits of Combining Forecasts. *Management Science,* Vol 41(1), 68-75.

Bellardo, J. and Savage, S. (2003).802.11 Denial of service attacks: Real vulnerabilities & Practical solutions. In*: proceedings of USENIX Security Symposium,* pp. 15-28.

Borisov,N. , Goldberg,I. and Wagner, D.(2001). Intercepting Mobile Communications: The Insecurity of 802.11. In: *Proceedings of 7th Annual International Conference on Mobile Computing and Networking*, Rome, Italy: ACM Press.

Briand, L., El Emam, K. and Bomarius, F. (1998). COBRA: A Hybrid Method for Software Cost Estimation, Benchmarking, and Risk Assessment. In: Proceedings of the 20th International Conference on Software. IEEE. pp 390-399

Brookes, C., Vikas, S. and Lanea. (2010). A comparison of Fuzzy, Bayesian and Weighted Average formulations of an in-stream habitat suitability model**.** In: *International Congress on Environmental Modeling and Software.* [Online] Available at: http://www.iemss.org/iemss2010/index.php?n=Main.[Accessed 21 Nov .2013.

Charlie, O. and Benjamin. (2011).Vulnerabilities of LDAP as an authentication service. *Journal of information security*.[Online] Vol 2, pp.151-157.Available at: http://www.sciRP.org/journal/jis [Accessed 1 Sept.2013].

Convery, S., Cook, D. and Franz, M. (2004). An Attack Tree for the Border Gateway Protocol. *The Internet Engineering Task Force Working Draft Proposed Standard* [online] Available at: https://tools.ietf.org/html/draft-ietf-rpsec-bgpattack-00 [Accessed 23 Nov 2013].

Cukier, M., Lyons, J., Pandey, P., Ramasamy, H., Sanders, W., Pal, P.,Webber, F., Schantz, R., Loyall, J., Watro,R., Atighetchi, M. and Gossett,J.(2001). Intrusion Tolerance Approaches in ITUA. In: *Proceedings of International conference on Dependable Systems and Networks*, pp. B-64-B-65.

Daniel, P. and Edward, G. (2010). Weaknesses and Strengths Analysis over Wireless Network Security Standards. *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering.*[Online] Vol 4(12).Available at:https://waset.org/journal/Electrical/2010/12?new=1[Accessed 4 August.2013].

Danielle, C., Michel, C. and Ali, M, (2011). *Model-based support for information technology security decision making.* PhD. University of Maryland, College Park .

David, M., William, H., Sanders, K. and Trivedi, S. (2004). Model-Based Evaluation: From Dependability to Security. *IEEE Transactions on Dependable and Secure Computing,* Vol. 1(1).

Dean, T. (2006). *Network+ Guide to Networks*. Boston, MA: Thomson Course Technology.

Deswarte, Y., Blain, L. and Fabre, J. (1991).Intrusion Tolerance in Distributed Computing Systems. In: *Proceedings of IEEE Symposium. Research in Security and Privacy,* pp. 110-121.

Dokurer, S. (2006). Simulation of Black Hole Attack in Wireless Ad-Hoc Networks. Masters thesis .Atılım University.

Dutertre, B., Crettaz, V., and Stavridou, V. (2002).Intrusion-Tolerant Enclaves. In: *Proceedings of. IEEE International Symposium on Security and Privacy*, pp. 216-224.

Edney, J. and Arbaugh, W. (2004). *Real 802.11 Security: Wi-Fi Protected Access and 802.11i.* Boston, MA: Addison-Wesley.

Eian, M. (2009).Fragility of the Robust Security Network 802.11 Denial of service. In: *Applied Cryptography and Network Security: 7th International Conference*. Paris: Springer, pp. 400-416.

Ellis, T. and Levy,Y. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: The International Journal of an Emerging Transdiscipline.* [Online] *Vol 9* pp. 181-212. Available at:http://inform.nu/Articles/Vol9/V9p181-212Levy99.pdf[Accessed 10 July 2012].

Ellis, T. and Levy, Y. (2008). A framework of problem-based research: A guide for novice researchers on the development of a research-worthy problem. *Informing Science: The International Journal of an Emerging Transdiscipline.[online] Vol 11*,pp. 17-33. Available at: http://inform.nu/Articles/Vol11/ISJv11p017-033Ellis486.pdf[Accessed 10 July .2012].

Ellis, T. and Levy, Y. (2009). Towards a Guide for Novice Researchers on Research Methodology: Proposed Methods. *Issues in Informing Science and Information Technology*.[Online].Vol6.Available at: http://inform.nu/Articles/Vol6/ISJv11p017-033Ellis486.pdf[Accessed 10 July.2012].

Expertise2go. (2014). *Web enabled expert system shell e2glite v3.04a*.[Online], Available at:http://www.expertise2go.com/webesie/e2gdoc/e2gmod2.htm[Accessed 8 Dec.2014).

FIRST. (2014).*Common vulnerability scoring system version 3.0 calculator*.[Online] Available at: https://www.first.org/cvss/calculator/3.0[Accessed 12 July .2016].

FIRST. (2014). Common Vulnerability Scoring System SIG.[Online] Available at: https://www.first.org/cvss/ [Accessed 12 July .2016].

FHI. (2012). *Research Methods Overview, from Qualitative Research Methods: A Data Collector's Field Guide* [Online].Available at: http://www.fhi360.org/nr/rdonlyres/ [Accessed 1 Feb.2013].

Fluhrer, S., Mantin, I. and Shamir, A. (2001).Weaknesses in the key scheduling algorithm of RC4.In: *Proceedings of the 4th annual workshop on selected areas of cryptography*, pp. 1-24.

Funk, P. and Blake-Wilson, S. (2007). EAP Tunneled TLS Authentication Protocol. Version01. *IETF Internet-Draft.* [Online].Available at: https://tools.ietf.org/html/draft-funk-eap-ttls-v1-00 [Accessed 23 Dec. 2013].

Gable, G. G. (2010). Integrating Case Study and Survey Research Methods: An Example in Information Systems. *European Journal of Information Systems,* Vol 3(2), pp.112-126.

Gast, M. (2005). *802.11 Wireless Networks: The Definitive Guide*.2rd ed. O'Reilly Media, Inc.

Geer, D., Hoo, .K. and Jaquith, A. (2003). Information Security: Why the Future Belongs to the Quants. Security & Privacy. *Institute of Electrical and Electronic Engineers*, Vol 1(4), pp. 24-32.

Gibson, R. (2007). Who's really in your top 8: network security in the age of social Networking. In: *Proceedings of the 35th annual ACM SIGUCCS fall conference,* ACM, pp 131-134.

Glass, R. (1995).A Structure-based critique of contemporary computing research. *Journal of Systems and Software, Vol 5(2), pp.26-34.*

Gollman, D . (1999). *Computer Security*. Chichester: John Wiley and Sons Ltd.

Goffee, N., Kim, S., Smith, S., Taylor, P., Zhao, M. and Marchesini. J. (2004). Greenpass: Decentralized, PKI based Authorization for WLANs. In: Proceedings of 3rd Annual PKI Research and development workshop. [Online].pp.26-41.Available at: http://www.cs.dartmouth.edu/%7Esws/abstracts/gks04.shtml[Accessed 28 NOV 2013].

Haidong, X. and Jose, B. (2004). Detecting and Blocking Unauthorized Access in Wi-Fi Networks. *Third International IFIP-TC6 Networking Conference.* Athens, Greece.[Online], Available at :https://link.springer.com/chapter/10.1007%2F978-3-540-24693-0_65?LI=true, [Accessed 10 March. 2014].

Haverinen, H. (Ed.) and Saloway, J., Ed.(2006). RFC 4186, *Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)*. The Internet Society.

Hill, G. (1982). Group vs. individual performance: Are N+1 heads better than one? Psychological Bulletin, 91, pp. 517-539.

Hoffman, D. (2006). *Advanced Hacking Techniques: Implications for a Mobile Workforce* [Online] Available at: www.fiberlink.com[Accessed 10 November.2012].

Hogarth, R. (1978). A note on aggregating opinions. *Organizational Behavior and Human Performance*, Vol 21, pp.40-46.

Hohmuth, M., Peter, M., Hartig,H. and Shapiro,J.(2004). Reducing TCB size by using untrusted components- small kernels versus virtual-machine monitors. In: 11th SIGOPS Eur. WS.

IEEE 802.11. (1997) Number Part 11: Wireless LAN Moderate Access Control (MAC) and Physical Layer (PHY) Specifications: Specific Requirements, IEEE Std. 802.11.

IEEE Standard 802.11. (1999). Information technology –Telecommunications and information exchange between systems – Local and metropolitan area networks – Specific requirements – Part 11: Wireless LAN Moderate Access Control and Physical Layer Specifications. IEEE.

IEEE 802.1x. (2004). IEEE Standard for Local and metropolitan area networks – Port-Based Network Access Control. IEEE.

IEEE 802.11i. (2004). ANSI/IEEE 802.11w-2009-IEEE Standard for Information Technology - Telecommunication and information exchange between systems - Local and metropolitan area networks - Specific requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications, Amendment 6: Medium Access Control (MAC) Security Enhancements.

IEEE 802.11w. (2009).ANSI/IEEE 802.11w-2009 - IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 4: Protected Management Frames. https://standards.ieee.org/findstds/standard/802.11w-2009.html.

Jaquith, A. (2007).Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison-Wesley Professional.

Jason, F., Damon, M., Vicenti, N., Jamie, V. and Douglas, S. (2006). Passive data link layer 802.11 wireless device driver fingerprinting. In: Proceedings of the 15th conference on USENIX Security Symposium [Online].Vol 15(12).Available at: https://www.usenix.org/legacy/event/sec06/tech/full_papers/franklin/franklin_html/ [Accessed 15 March.2013].

Jiang ,L. and Garuba, M.(2008). Encryption as an Effective Tool in Reducing Wireless LAN Vulnerabilities. *Information Technology: New Generations[Online],Available at* http://ieeexplore.ieee.org/xpl/abstractAuthors.jsp?arnumber=4492539&abstractAccess=no&userType=inst[Accessed on 2.Nov 2013].

John V. and Moskowitz .(2002). *Wireless LAN Access Control and Authentication* .Interlink Networks [Online].Available at : www.interlinknetworks.com[Accessed 12 August.2012]

John, V., Ann, A. and Robert, M. (2002). *802.11b Wireless Networking and Why It Needs Authentication.* Interlink Networks. [Online]Available at: www.interlinknetworks.com [Accessed 12 August 2012].

Kamath, V., Palekar, A. and Wodrich, M. (2002), Microsoft's PEAP version 0 (Implementation in Windows XP SP1), *IETF Internet Draft*, Rome, available at: http://tools.ietf.org/id/draft-kamath-pppext-peapv0-00.txt[Accessed 10 Feb 2013].

Karppinen, K. (2005). *Security Measurement based on Attack Trees in a Mobile Ad Hoc Network Environment.* VTT INFORMATION SERVICE http://www.vtt.fi/inf/pdf/)

Kashorda, M. and Waema, T. (2014). E-Readiness Survey of Kenyan Universities Report. Nairobi*: Kenya Education Network*. [Online].Available at: https://www.kenet.or.ke/ [Accessed 10 Nov.2014].

Ken, A., Dawson, R. and Engler. (2002). Using Programmer-Written Compiler Extensions to Catch Security Holes. In: *Proceedings of IEEE Symposium on Security and Privacy*.

Khidir, M. and Owens, T. (2007).Selection of an EAP authentication method for a WLAN, *International journal of Information and Computer Security*. [Online] *Vol.1 (1/2) pp. 210-233.* Available at: http://www.cob.calpoly.edu/~ijics/ijics-9.pdf [Accessed 15 June.2013].

Khidir, M. and Ali, A. (2011).A Comparative Study of Authentication Methods for Wi-Fi Networks. In: *Proceedings of International Conference on Computational Intelligence, Communication Systems and Networks* [Online], pp. 190-194.Available at: http://www.computer.org/csdl/proceedings/cicsyn/2011/4482/00/4482a190-abs.html[Accesed 10 Jan 2014].

Kleijnen, J. (1999). Validation of models: statistical techniques and data availability. In: *Winter Simulation Conference Proceedings*, Vol 1, pp. 647-654.

Kleijnen, J. (1995. Verification and Validation of Simulation Models. *European Journal of Operational Research*, 82 (1), pp.145-162.

Klein, G., Elphinstone, K., *Heiser, G*., Andronick, J. Cock, D., Derrin, P., Elkaduwe, D., Engelhardt, K., Kolanski, R.,; Norrish, M., Sewell, T., Tuch, H. and Winwood, S. (2009). seL4: Formal verification of an OS kernel. *22nd ACM Symposium on Operating System Principles*. Big Sky, Montana, pp. 207–220.

Kotulic, A. and Clark, J. (2004). Why There Aren't More Information Security Research Studies. *Information & Management*.[Online]*Vol 41(5).* pp.597-607 Amsterdam: Elsevier Science Publishers, Vol 41(5).Available at: https://dl.acm.org/citation.cfm?id=1005444 [Accessed 10 Jan.2014].

Kshitij,R., Dhananjay, M. and Ravindra,L.(2013).Authentication Methods for WI-Fi Networks, *International journal of Applications or innovation in Engineering and*

Management.[Online],Vol 2(3) ,Available at: www.ijaiem.org/volume2issue3/IJAIEM-2013-03-31-123.pdf[Accessed 26.June 2013].

Kwang-Hyun, B., Sean, W. and David, K. (2004). A Survey of WPA and 802.11i RSN Authentication Protocols. Dartmouth College:Computer Science Technial Report TR2004-524.Available at:www.cs.dartmouth.edu/~dfk/papers/baek-survey-tr.pdf.

Lampson, B., Abadi, M., Burrows, M., and Wobber, E. (1992).Authentication in Distributed Systems: Theory and Practice. *ACM Transactions on Computer Systems.* Vol.10 (4), pp.265-310.

Laurent, B. and Julien, T. (2007). Discovering and Exploiting 802.11 Wireless Driver Vulnerabilities**.** *Journal in Computer Virology.* [Online] Vol 4(1), pp.25-37**,** Available at: http://link.springer.com/article/10.1007%2Fs11416-007-0065-x#page-1 [Accessed 27 Sept . 2014].

Leedy, P. and Ormrod, J. (2005). *Practical Research: Planning and Design* (8th ed.). Upper Saddle River, NJ: Prentice Hall.

Li-Chuan, G., Cheng, Z., Shao-Wen, S. and You-hua, Z. (2009).A new network access control Method Based on Diameter Protocol.*WRI International Conference on Communications and Mobile Computing* [Online] IEEE, Vol 1, pp.600-604. Available at: http://ieeexplore.ieee.org/document/4797323/authors[Accessed 10 Jan. 2014].

Maiwald, E. (2003) *Network Security: A Beginner's Guide*, Emeryville, CA: McGraw-Hill/Osborne.

Martin, B. and Erik, T.(2008).*Practical attacks against WEP and WPA.*TU-Dresden, Germany, TU-Darmstadt, Germany.

Martin, E. (2009) Fragility of the Robust Security Network: 802.11 Denial of Service. In: *proceedings of the 7th international conference on applied cryptography & network security,* IEEE.

Mathews, M., Hunt. (2007). *Evolution of WLAN Architecture IEEE 802.11i.* Newzealand: University of Canterbury.

Michael, R. (2007) *Wireless Hacking Tools* [Online], *Available at:* http://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking.pdf [Accessed on 30 June.2013]**.**

Mitnick, K., Simon, W. (2003). *The Art of Deception: Controlling the Human Element of Security.* John Wiley & Sons, Inc. New York, NY, USA.

Moore, A., Ellison, R. and LingerMoore, R. (2001). Attack Modeling for Information Security and Survivability. *Survivable Systems.*[Online]Carnegie Mellon University**.** Available at: repository.cmu.edu/cgi/ [Accessed on 10 June 2013].

Morris, P. (1974). Decision Analysis Expert Use. *Management Science*, 20, pp.1233-1241.

Morris, P. (1977). Combining Expert Judgments: a Bayesian approach. *Management Science*, 23, pp.679-693.

Morris, P. (1983). An axiomatic approach to expert resolution. *Management Science,* 29, pp.24-32.

Morris, P. (1986). Observations on Expert Aggregation. *Management Science,* 32, pp. 321-328.

Mory, M. and Meech. (2000).Application of fuzzy logic in environmental risk assessment: some thoughts on fuzzy sets. *Cybernetics and Systems*, *Vol* 31(3), pp. 317-332.

Mugenda, A., and Mugenda, O. (2003). *Research Methods: Quantitative and Qualitative Approaches.* Nairobi, Kenya.

Mwathi, D., Okelo-Odongo., W. and Opiyo., E. (2016).Algorithm Selection of EAP Authentication Method for use in a Public WLAN: Implementation Environment Based Approach. *International Research Journal of Computer Science,* [Online] Vol 3(5), pp.47-52.Available at: http://www.irjcs.com[Accessed 8 June.2016].

Newell, A. and Simon, H. (1972). *Human problem solving.* Englewood Cliffs, NJ: Prentice-Hall, pp.920.

Nistir, W., Jansen, W. and Gallagher, P. (2009). Directions in Security Metrics Research.

Park, J. and Dicoi, D. (2003).WLAN security: Current and future. *IEEE Internet computing*, Vol 7(5,) pp. 60-65.

Pat, R., Calhoun, John, L., Erik, G., Glen, Z. and Jarki, A. (2002). *Diameter Base Protoco*l, IETF AAA Working Group.

Penta, D. (2002). *Computing and expert system*. Adision Wesley, 2nd ed. pp. 5-9.

Petre, M. and Rugg, G. (2010). *The Unwritten Rules of PhD Research -Open up Study Skills).* [Online], Available at: http://postgrado.bio.uc.cl/wp-content [Accessed 28 Oct 2016].

Pfleeger,C. and Pfleeger, S.(1997).*Security in Computing.* Fourth Edition, Pearson Education, New Jersey Prentice Hall.

Poorinma, N., Gowri, S., Abinaya, R. (2015). Issues and the Advantages of Wireless Network. *International Journal of Engineering Development and Research*, *Vol 4(2), pp.28-36.*

Rakesh, M., Ankur, G. (2008). *Securing WIFI: Network. Center for Research and prevention of Computer crimes* [Online] Available at: www.sysman.org/wifi-security-ebook-RakeshGoyal-Sysman-2008-10-09-V001.pdf [Accessed 10 Dec 2014].

Rigney, C., Willens, S., Rubens, A. and Simpson. (2000). *Remote Authentication Dial In User Service (RADIUS).* RFC 2865, IETF Network Working Group.

Rushby, J. (1981).Design and verification of secure systems,*8th ACM Symposium on operating system principles*, Pacific Grove California ,US. pp. 12-21.

Sankar, K., Sundaralingam, S., Miller, D. and Balinsky, A. (2005) *Cisco Wireless LAN Security*. N.York: Cisco Press.

SANS Institute InfoSec Reading Room. (2003).Wireless LAN: Security issues and solution, US; SANS Institute, Vol 1(4).

Sargent,R.,Wilson,J.(eds), Henriksen,J.(eds) and Roberts,S.(eds).(1986).The Use of Graphical Models in Model validation. *In: Proceedings of Winter Simulation Conference,* Piscataway, New Jersey: IEEE, pp. 237-241.

Sargent. , Robert, G. (2011).Verification and validation of simulation models. In: Proceedings of the 2011 Winter Simulation Conference [Online], Available at: http://informs-sim.org/wsc02papers/008.pdf [Accessed 18 Dec. 2014].

Savola, R. and Holappa J. (2005). Self-Measurement of the Information Security Level in a Monitoring System Based on Mobile Ad Hoc Networks. In: *Proceedings of the 2005 IEEE Int. Workshop on Homeland Security, Contraband Detection and Personal Safety,* Orlando, FL: IEEE, pp.8.Available at: www.ieeexplore.ieee.org/document/1502553/.

Scott, A. (2011). Known Wireless Attacks, Loughborough University.

Schneier.B.(1999).*Attack trees: Modeling security threats*. Dr. Dobb's Journal.

Schneier, B. (2000) *Secrets and Lies: Digital Security in a Networked World.*New York: John Wiley & Sons.

Sheila, F., Bernard, E., Les, O., Karen, S.(2007). *Establishing Wireless Robust security Networks: A Guide to IEEE 802.11i*, NIST.US.

Shirazi, C. (2009).*Data-Informed Calibration and Aggregation of Expert Judgment in a Bayesian Framework*. PhD, University of Maryland.

Shumman, W. & Ran, T. (2003) WLAN and it's Security Problems. In: proceedings of the *2003 International conference on Parallel and Distributed Computing, Applications and Technologies*, *IEEE*, pp.241–245.

Simon, L., John, S., Jerry, O. (2001).A Practical Approach to Enterprise IT security.*IT Professional.* Vol 3(5), pp. 35-42.

Stacewicz, P. and Włodarczy, K. (2010).*Modeling in the Context of Computer Science –A Methodological approach* [Online], Available at: http://logika.uwb.edu.pl [Accessed 4 June. 2014].

Steven, B. (2015).The Birth and Death of the orange book. *IEEE annals of the history of computing*, Vol.37 (2) pp.19-31.

Stewart, R. (1997).Simulation model verification and validation: increasing the users' confidence, *Proceedings of winter simulation conference*, pp53-59.

Stone, M. (1961). The opinion pool. *Annals of Math. Statistics*, Vol 32, pp. 1339-1342.

Swatzell, K. and Jennings. (2007).*Descriptive research: The Nuts and Bolts* [Online], Available at: http://iaapa.com/issues/i20070701/articles/researchon0707.htm [Accessed 10 Apr 2014].

Tal, G., Ben, P., Jim, C., Mendel, R. and Dan, T. (2003). A Virtual Machine-Based Platform for Trusted Computing. In: *Proceedings of Symposium on Operating Systems Principles.*

Umesh, K., Praveen, K., Sapna, G. (2014).Analysis and literature review of IEEE 802.1x (Authentication) protocols. *International journal of Engineering and advanced Technology*, Vol.3 (5).

Waliullah, M. (2015).An Experimental Study Analysis of Security attacks at IEEE 802.11 Wireless local Area Network. *International Journal of Future Generation Communication and Networking*, Vol 8(1), pp 9-18.

Wang, A. (2005). Information Security Models and Metrics. In: *Proceedings of the 43rd Annual Southeast Regional Conference*, ACM. Vol 2, pp. 178-184.

Wegner, P. (1976). Abstraction: A Tool for the Management of Complexity. *Proceedings of 4th Texas Conference on Computing*. Texas, ACM.

Wei-Lin, C., Quincy, W.(2010).A Proof of MITM Vulnerability in Public WLANs Guarded by Captive Portal. In: *Proceedings of Asian- pacific advanced network 2010* [Online] Vol 30, pp. 66-69, Available at http://dx.doi.org/10.7125/APAN.30.10 [Accessed 15 march, 2014].

Yaniv, I. (2004).The Benefit of Additional Opinions. *Current Directions in Psychological Science*, Vol 13(2) pp. 75-80.

Yizhan, S. (2006). *Complexity of System Configuration Management*, PhD thesis, Tufts University.

Zajonc, R. (1962). A note on group judgments and group size. *Human Relations*, Vol 15,pp. 177–180.

Appendix 1: Questionnaire A-Preliminary Survey

UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING & INFORMATICS

PHD RESEARCH

SECURE AUTHENTICATION AND ACCESS CONTROL IMPLEMENTATION MODEL FOR PUBLIC Wireless Local area Networks (WLANs)

QUESTIONNAIRE A-PRELIMINARY SURVEY

Kindly respond to the following questions. The responses provided will be treated with utmost confidentiality and will only be used for the purpose of developing theory for the research.

NB: In this questionnaire, a 'WLAN device' refers to WLAN enabled laptop, tablet, PDA, phone or desktop that is registered/known to university Wireless local area network(WLAN).The WLAN device, user of the device or both may be required to authenticate to access the WLAN.

PART A: Demography

(1)Date ……………………………………………………………………………..

(2)University Name………………………………………………………………

(3)Designation……………………………………………………………………

PART B: University WLAN Environment Awareness

(1)Do you have a WLAN infrastructure in the university? Yes | No

If Yes to (1) above, estimate the number of WLAN devices that connect to the university WLAN…………………………………………………………

(2)Indicate the number of IT staff working specifically in IT security…………………..

(3)Kindly name any FOUR systems in the university that are accessed via WLAN?

………………………………………………………………………………………

…………………………………………………………………………

(4)Are you aware of security features employed on the university WLAN? Yes | No

(5)In your own opinion, does the university place high value for its information resources

Yes	No

PART C: University WLAN Authentication and access control Security

(Tick the most appropriate option.)

(1)Which of the following cipher suites (confidentiality and integrity protocols) are configured on university WLAN?

[A]WEP
[B]TKIP
[C]CCMP
[D]A combination of any of the above(Specify)…………………………………………….

(2)Which authentication method is used to provide access to WLAN devices into your network?

[A]Open authentication/No authentication
[B]Pre-shared Key (PSK)
[C]EAP method with 802.1x (RADIUS server)
[D]Captive portal only
[E]A combination of any of the above (Specify)………………………………..

(3)Does the university WLAN use Authentication server (RADIUS or other) during authentication

Yes	No

If yes in (4) above respond to parts (i) and (ii) below;

(i)Which of the following EAP methods are used in your WLAN authentication

[A]EAP TLS
[B]EAP TTLS
[C]PEAP
[D]LEAP
[E]EAP –SIM
[F]Other(Specify)………………………………………………

(ii)Give a brief description of the authentication process including all the server types used.

....
....
....
....
....

(4) Does the entire university WLAN use similar authentication method for all WLAN devices across the u

Yes	No

If response is No in (5) above, name all authentication methods used and the circumstances under which they are used…………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

……………………………………………………………………………………

(5) Has the university WLAN ever experienced a WLAN related security attack Yes | No

If Yes in (5) above, respond to part (i), (ii), (iii) and (iv)

(i) What type of attack do you think it was?

[A]Denial of service(Not able to access WLAN network

[B]Man in the middle (where an agent of attack(hardware or software) between LAN device and authentication servers was used to perpetrate the attack; includes social engineering)

[C]Cipher suite attack (Attack on cryptographic algorithms, cryptoanalysis)

[D]A combination of A, B and C

[E] Other(Specify)........................

[F]I don't know

(ii)What in your opinion was the cause of the attack………………………………………..

....

....

....

....

....

....

....

(iii)What in your opinion were the vulnerabilities exploited…………………………………………………………………………

....

....

....

....

....

(iv)How easy, in your opinion, was it for the attackers to carry the attack?

[A]Very easy

[B]Easy

[C]Neither easy nor difficult

[D]Difficult

[E]Very difficult

(6)Do you maintain a database of attack incidences on university WLAN? Yes | No

If yes, name the most common attacks and the vulnerabilities exploited
....
....
....
....
....

(7)Kindly tick where appropriate and applicable

	Weekly	Monthly	Semesterly	Yearly	Never changed	Not Applicable
(i)How often do you change preshared secret where you using PSK authentication						
(ii)How often do you change pre-shared **RADIUS** server – Accesspoint passphrase.(AS-AP)						

(8)Kindly tick where appropriate and Applicable.

	Strongly disagree	Disagree	Neither Agree Nor Disagree	Agree	Strongly Agree	Not Applicable
(i)WLAN devices/users in university WLAN authenticate once[No authentication is required in subsequent WLAN network accesses(sessions)]						
(ii)A WLAN device verifies the certificates provided by the authentication server of university WLAN whenever it connects to it?						
(iii)Both WLAN devices and authentication server of university WLAN (RADIUS						

or other) authenticate each other before a WLAN device connects to it.						
(iv)University WLAN is configured to use IEEE 802.11w						
(v)University WLAN supports configuration of Virtual WiFi Soft Access points by WLAN devices.						
(vi)Access points and Authentication server of university WLAN have a way of authenticating each other.						
(vii)Sensitive and confidential documents are sent via university WLAN						
(viii)Sensitive and confidential documents sent via university WLAN are secure.						
(ix)There is a system in the university where students can register to request for digital certificates for WLAN authentication						
(x)University WLAN supports RSN associations						

(9)Kindly explain how you think an implementation (configuration) model/framework for WLAN authentication and access control can be used to increase the security of WLAN authentication in the university WLAN

....
....
....
………………………………………………………………………………………
……………..……………………………………………………………………
………………………….……………………………………………………
……………………………………………

Thank you for taking time to respond.

Appendix 2: Questionnaire B-Conceptual Model Validation by Experts

UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING & INFORMATICS

PHD RESEARCH

SECURE AUTHENTICATION AND ACCESS CONTROL IMPLEMENTATION MODEL FOR PUBLIC Wireless Local area Networks (WLANs)

QUESTIONNAIRE B-CONCEPTUAL MODEL VALIDATION BY EXPERTS

This questionnaire is part of research that aims to develop a model whose intended purpose is to enable design or selection and configuration of security features for WLAN authentication and access control. Its main objective is to determine if the model is correct and reasonable for its intended purpose.

Kindly familiarlise yourself with the model [See Annex 1,Annex 2, Annex3] and model prototype [http://chuka.ac.ke/dcsict/Web/] before responding to the questionnaire.

Information that may identify you will remain strictly confidential and will never be shared with third party and that the results of this study will be anonymised for further publications.

PART A- COMPONENTS/PARAMETERS OF WLAN AUTHENTICATION AND ACCESS CONTROL SECURITY MODEL

In this section, we want to capture your approval rating of the correctness of model's underlying theory, structure and assumptions for achieving its intended purpose **[See Annex 1]**

[1] Attack Susceptibility is a variable that assesses how susceptible vulnerabilities are to exploitation and how complex it is to develop an attack against a security framework. It is an indicator of security strength of a WLAN in that the stronger the attack Susceptibility, the weak the security and Vice-versa. The model identifies eight components whose features and configurations influence attack Susceptibility; Cipher suite, Authentication and access control mechanism, WLAN Client Driver, WLAN Client Utility, Accesspoint Firmware, Authentication Server , User Database and Authentication Credentials.

(i)How confident are you in the following components as influencers of Attack Susceptibility.

Component	**Very Confident**	**Confident**	**Neither confident nor not confident**	**Somewhat confident**	**I don't agree with this parameter**
Cipher Suite(CS)					
Authentication Credentials(AC)					
WLAN Client Driver(WCD)					
WLAN Client Utility (WCU)					
Accesspoint Utility(AU)					
Authentication Server (AS)					
User Database Server(UDS)					
Authentication and access control Mechanism(AAM)					

(ii)If you don't believe in some or all of these components, recommend appropriate alternative components.

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

[2] Trusted computing base (TCB) is a small amount of software, firmware, hardware and procedural components that security depends on and that we distinguish from a much larger amount that can misbehave without affecting security. A secure path between trusted computing base elements is a mandatory requirement. Based on this concept, the eight components identified in [1] above were categorized into TWO Main Dimensions; **Wireless Path Security (WPS**) which refers to the wireless MAC layer security between end devices and accesspoint and **WLAN Trusted Computing base Security (WTCBS)** which refers to security critical computing platform in a WLAN and consist of end user devices, access points, authentication systems and their configurations.

(i)How confident are you in this categorisation of components.

Dimension	**Component**	**Very Confident**	**Confident**	**Neither confident nor not confident**	**Somewhat confident**	**I don't agree with this Categorizatio**
Wireless Trusted Path Security(WTPS)	Authentication Credentials					
	Cipher Suite					
Wireless Trusted Computing Base Security(WTCBS)	WLAN Client Driver					
	WLAN Client Utility					
	Access point Utility					
	Authentication Server					
	User Database Server					
	Authentication and access control Mechanism					

(ii)If you don't believe in this categorization, recommend appropriate alternative categorization…………………………………………………………………………...

…...

....

....

....

....

....

[3]Based on client server nature of WLAN computing base**,** WLAN Trusted Computing Base Security (WTCBS) components in [2] were further categorized into **TWO** Main Components (i) **Front-end System Software** which refers to security features and configurations on utility and driver softwares associated with both end user devices and access point and (ii) **Back-end Authentication Systems** which refers to the security features and configurations on Server and access point software components associated with authentication of users to the WLAN.

(i)How Confident are you in this categorization of WLAN Trusted Computing base Security (WTCBS) components.

Dimension	**Category**	**Component**	**Very Confident**	**Confident**	**Neither confident nor not confident**	**Somewhat confident**	**I don't agree with this Categorization.**
WLAN Trusted Computing Base Security (WTCBS)	Front-end System Software	WLAN Client driver					
		WLAN Client utility					
		Access point Utility					
	Back-end Authentication Systems	Authentication Server					
		User Database Server					
		Authentication and access control Mechanism					

(ii)If you don't believe in this Categorization, recommend appropriate alternative Categorization.

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

………………………………………………………………………………………………

[4]An attacker is an individual with a motive, opportunity and capability who attempts one or more attacks in order to achieve an objective. Attacker capability refers to availability of resources such as attack tools, knowledge, experience and funding necessary for launching attacks. Attacker motivation refers to perceived benefit to the attacker after a successful attack. Opportunity refers to a favourable situation that the attacker exploits to achieve the intended goal.

The model assumes that there exists attackers who have motivation and capability and therefore ready to compromise any WLAN implementation whenever there is an opportunity.

How confident are you in this assumption?

[A]Very Confident

[B] Confident

[C]Neither confident nor not confident

[D]Somewhat confident

[E]I don't believe in this assumption

[5] Preliminary research established that the exploit code targeting each of the eight parameters is mature (i.e There is at least a functional exploit code available for each parameter or sufficient technical details to exploit the parameter vulnerabilities exist).For that reason, the model assumes that all the eight parameters have equal potential of vulnerability exploitation and therefore have equal relative importance in the model.

How confident are you in this assumption?

[A]Very Confident

[B] Confident

[C]Neither confident nor not confident

[D]Somewhat confident

[E]I don't believe in this assumption

PART B- SECURITY STRENGTH OF A PUBLIC WLAN AUTHENTICATION AND ACCESS CONTROL IMPLEMENTATION

In this section we want to capture your confidence in the security weights/strengths assigned to various component features when selected for a public WLAN authentication and access control implementation. We also want to capture your confidence in the algorithm for selection of a Secure Extensible Authentication Protocol (EAP) method. Kindly familiarlise yourself with Annex 2 and Annex 3 before responding to this section.

[1](i)How confident are you in the correctness of the security weights/strengths assigned next to the security features of each of the following components. (Interpretation of weights: 0-Very weak, 1-Weak, 2-Moderate, 3-Strong).

	Very Confident	**Confident**	**Neither confident nor not confident**	**Somewhat confident**	**I don't believe in the security strengths**
(a)Cipher Suite **(3)** CCMP (WPA2 +AES) **(2)** TKIP(WPA +AES) **(1)** TKIP(WPA +RC4) **(1)**TKIP(WPA2 +RC4) **(0)**WEP					
(b)Authentication Credentials **(3)**Both Client and Server Certificates **(2)**PAC, One time password OR Server Side certificate only(Tunneled) **(1)**Static Password/Secret Key **(0)**SSID **(0)**MAC address **(0)**PIN					
(c)WLAN Client Driver **(3)**Supports management frame protection (MFP/IEEE 802.11w).Supports configurable active scanning approach. **(2)**Supports management frame protection (MFP/IEEE 802.11w).Lacks Support for Configurable active scanning approach. **(2)**Lacks support for management frame protection (IEEE 802.11w).Supports IEEE 802.11i.Supports configurable active scanning approach**.** **(1)** Lacks support for management frame protection (MFP/IEEE 802.11w).Lacks support for Configurable active scanning approach. Supports IEEE 802.11i **(0)** Lacks support for IEEE 802.11i.					
(d) WLAN Client Utility **(3)**Configured to support both client and server side Certificate based mutual Authentication. Supports Management frame protection. Configured to enforce validation of server certificates and server name. Configured not to allow Self signed certificates. **(2)**Configured to support server side only Certificate based mutual Authentication. Supports Management frame protection (IEEE					

802.11w).Configured to enforce validation of server certificates and server name. Configured not to allow Self signed certificates. **(1)**Configured to support Password, pre-shared key or MAC address based mutual Authentication mechanism. Supports Management frame protection (IEEE 802.11w) **(1)**Configured to support server side only or both client and server side Certificate based mutual Authentication Lacks Support for Management frame protection (IEEE 802.11w).Supports IEEE 802.11i **(1)**Configured to support Password, pre-shared key or MAC address based mutual Authentication mechanism. Lacks Support for Management frame protection (IEEE 802.11w).Supports IEEE 802.11i. **(0)**Lacks support for IEEE 802.11i **(0)**Configured to support server side only or both client and server side certificate but Validation of server certificates and/or server name not enforced **(0)**Configured to support server side only or both client and server side certificate but allows Self signed certificates. **(0)**Mutual authentication not supported.					
(e)Access point Utility **(3)**Firmware configured to support management frame protection (MFP/IEEE 802.11w) and is set to required. Firmware configured to Support only RSNA connections(RSNA enabled) **(2)**Firmware configured to support optional management frame protection (MFP/IEEE 802.11w).Firmware configured to support only RSNA connections(RSNA enabled) **(1)**Firmware does not support MFP/IEEE 802.11w.Firmware configured to Support only RSNA connections(RSNA enabled) **(0)**Firmware not configured to Support only RSNA connections(Pre-RSNA enabled)					
(f)Authentication Server **(3)**DIAMETER. Configured to Support mutual authentication **(2)**RADIUS. Configured to Support mutual authentication **(1)**DIAMETER. Not Configured to Support mutual authentication **(1)**RADIUS. Not Configured to Support mutual authentication **(1)**KERBEROS **(0)**Integrated Authenticator/ Authentication Server					
(g) Authentication and access control Mechanism **(3)**IEEE 802.1x With EAP method **(3)**Captive portal and IEEE 802.1x With EAP Method **(2)**Captive Portal and Pre-shared Key **(1)**Captive Portal Only **(1)**Pre-shared Key Only **(0)** MAC address filtering **(0)**Open SSID **(0)**PIN Based authentication(WPS)					

(0) Button press based authentication(WPS)					
(h)User Database Server **(3)**Distributed Database Servers with an Intrusion Detection System(IDS) **(2)**Distributed Database Servers without an Intrusion Detection System(IDS) **(2)**Centralised Database Server with an Intrusion Detection System(IDS) **(1)**Centralised Database Server without an Intrusion Detection System(IDS) **(0)**Independent on each Access point					

(ii)If you don't believe in the security strength indicated for any of these components, indicate your recommended strength next to the feature.

[2]How Confident are you in the mathematical logic of the technique for propagation of values in the model?

[A]Very Confident

[B] Confident

[C]Neither confident nor not confident

[D]Somewhat confident

[E]I don't believe in the correctness of this algorithm

[3]How confident are you in the correctness of the algorithm for selection of a Secure Extensible Authentication Protocol (EAP) method (See Annex 3)

[A]Very Confident

[B] Confident

[C]Neither confident nor not confident

[D]Somewhat confident

[E]I don't believe in the correctness of this algorithm

[4]How confident are you in the effectiveness of the algorithm for selection of a Secure Extensible Authentication Protocol (EAP) method (See Annex 3)

[A]Very Confident

[B] Confident

[C]Neither confident nor not confident

[D]Somewhat confident

[E]I don’t believe in the effectiveness of this algorithm

PART C-ABOUT YOU

[1] What is the Name of your organization **(optional)**……………………………………

[2]Kindly indicate your highest level of academic Qualifications…………………………

[3] Indicate any Professional Qualifications……………………………………………..

[4] What is your job title:………………………………………………………………..

[5] How long have you been at this position………………………………………………

[A]Less than 1 Year

[B]1-3 Years

[C] Over Three Years

[6]Please List your previous IT Security/Computer Security/Network security related research or consultancy experiences along with the number of years spent in research/consultancy (Use the format shown in the first row of the table)

Experience	**No. Of Years**
WLAN security research	*4*

[7] Assess your level of competency on the following areas by ticking the option that best describes your Level

	Less Comptetent	**Moderately Competent**	**Highly Competent**
Intrusion analysis			
System administration			
Incident handling			
Penetration testing			
Network security			
WLAN security			

[8]Do you know **somebody in a different organization** who can help in giving similar information as required above? Please recommend someone and give contact information.
…………………………………………………………………………………………………

[9]Please leave here any comment you may have regarding the research goals of the study. If you wish to be contacted for clarification, you may leave your email and phone number here……………………………………………………………………………....

Thank you for your participation.

Preliminary research established that the exploit code targeting each of the eight parameters is mature(i.e There is at least a functional exploit code available for each parameter or sufficient technical details to exploit the parameter vulnerabilities exist).For that reason, the model assumes that all the eight parameters have equal potential of vulnerability exploitation and therefore have equal relative importance.
To what extent do you agree with this assumption

Appendix 3: Questionnaire C-Operational Validation by Practitioners

UNIVERSITY OF NAIROBI

SCHOOL OF COMPUTING & INFORMATICS

PHD RESEARCH

SECURE AUTHENTICATION AND ACCESS CONTROL IMPLEMENTATION MODEL FOR PUBLIC Wireless Local Area Networks (WLANs)

QUESTIONNAIRE C-OPERATIONAL VALIDATION BY PRACTITIONERS

This questionnaire is part of research that aims to develop a model whose purpose is to enable design or selection and configuration of security features for WLAN authentication and access control. Its main objective is determining whether the Computerised model's output behaviour has the accuracy required for the model's intended purpose over the domain of the model's intended applicability.

You are expected to experiment with the Prototype/Computerized model in detail by varying input parameters and observing the output behaviour (parameter variability-sensitivity) before filling the questionnaire. The model prototype is accessible from the following URL: **http://chuka.ac.ke/dcsict/Web/**

Specifically you are expected to do the following;

(i) Collect data on security features and configurations from either an operational or hypothetical WLAN environment.

(ii) Feed the data collected into the prototype

(iii) Process results using Computer model /prototype

(iv) Assess accuracy of results (Magnitude and direction of output behaviour)

(v) Repeat steps i-iv until you have sufficient data to enable you evaluate the model

(vi) Provide Feedback on the questionnaire.

Information that may identify you will remain strictly confidential and the results of this study will be anonymised for further publications.

PART A-EVALUATION OF MODEL RESULTS

This part captures the opinion of the practitioner after experimenting with the prototype of the model.

[1](a)To what extent do you agree with the accuracy of the following results/output from the prototype? Tick appropriately.

	Strongly Agree	**Agree**	**Neither Agree Nor Disagree**	**Disagree**	**Strongly Disagree**
Strengths/Magnitude of **Wireless Path** for various component inputs(Cipher suite, Authentication and access control mechanism)					
Strengths/Magnitude of **Front-end System software** for various component inputs(Client Driver, Client Utility, Access point firmware)					
Strengths/Magnitude of **Back-end Authentication Systems** for various component inputs (Authentication Server, User database, Authentication Credentials).					
Strengths/Magnitude of **Wireless Trusted Computing Base Security** for various component inputs					
Strengths/Magnitude of **Attack Susceptibility** for various component inputs					
Strengths/Magnitude of **Wireless Authentication and**					

access control Security for various component inputs					
Remarks/Recommendations provided for various component inputs					
Extensible Authentication Protocol (EAP) method recommended for various parameter inputs					

[1](b)Where you disagree or strongly disagree, briefly describe why you disagree.

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

[2] To what extent do you agree with the following statements about the model? Tick Appropriately.

	Strongly Agree	**Agree**	**Neither Agree nor Disagree**	**Disagree**	**Strongly Disagree**
The model correctly provides results useful for **design** of security features for WLAN Authentication and access control					
The model correctly provides results useful for **selection** of security features for WLAN Authentication and access control					
The model correctly provides results useful for **configuration** of security features for WLAN Authentication and access control					

[3]What are your general thoughts on the model……………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

[4]How could this model help you in your work?……………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

……………………………………………………………………………………………

PART B-ABOUT YOU

[1] What is the Name of your organization:……………………………………………..

[2] Kindly indicate your highest level of academic qualifications………………………

[3] Indicate any Professional Qualifications……………………………………………

[4] What is your job title:……………………………………………………………..

[5] How long have you been at this position……………………………………………

[A]Less than 1 Year

[B]1-3 Years

[C] Over Three Years

[6]Please List your previous IT related job experiences along with the number of years spent at that position (Use the format shown in the first row of the table).

Experience	**No. Of Years**
Network security administration	**2**

[7] Assess your level of competence on the following areas by ticking the option that best describes your Level

	Low Competence	**Moderately Competent**	**Highly Competent**
Intrusion analysis			
System administration			
Incident handling			
Penetration testing			
Network security			
WLAN security			

[8]Do you know **somebody in a different organization** who can help in giving similar information as required above? Please recommend someone and give contact information.
…………………………………………………………………………………………………
…………………………………………………………………………………………………

[9]Please leave here any comment you may have regarding the research goals of the study. If you wish to be contacted for clarification, you may leave your email and phone number here………………………………………………………………………………....

Thank you for your participation.

Appendix 4: Test Data

Cipher Suite	**AM**	**WPS**	**Client Utility**	**Client driver**	**Accesspoint Utility**	**FESS**	**Authentication Server**	**Authentication Credentials**	**User Database**	**BAS**	WTCB	AS	WAACS
Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Low	Strong
Low	Moderate	Moderate	Low	Low	Moderate	Moderate	Low	Low	Moderate	Moderate	Moderate	Moderate	Moderate
Low	High	Moderate	Low	Low	High	Moderate	Low	Low	High	Moderate	Moderate	Moderate	Moderate
Moderate	Low	Moderate	Low	Moderate	Low	Moderate	Low	Moderate	Low	Moderate	Moderate	Moderate	Moderate
Moderate	Moderate	Moderate	Low	Moderate	Moderate	Moderate	Low	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Moderate	High	High	Low	Moderate	High	Moderate	Low	Moderate	High	Moderate	Moderate	High	Weak
High	Low	Moderate	Low	High	Low	Moderate	Low	High	Low	Moderate	Moderate	Moderate	Moderate
High	Moderate	High	Low	High	Moderate	Moderate	Low	High	Moderate	Moderate	Moderate	High	Weak
High	High	High	Low	High	High	High	Low	High	High	High	High	High	Weak
Low	Low	Low	Moderate	Low	Low	Moderate	Moderate	Low	Low	Moderate	Moderate	Moderate	Moderate
Low	Moderate	Moderate	Moderate	Low	Moderate	Moderate	Moderate	Low	Moderate	Moderate	Moderate	Moderate	Moderate
Low	High	Moderate	Moderate	Low	High	Moderate	Moderate	Low	High	Moderate	Moderate	Moderate	Moderate
Moderate	Low	Moderate	Moderate	Moderate	Low	Moderate	Moderate	Moderate	Low	Moderate	Moderate	Moderate	Moderate
Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Moderate	High	High	Moderate	Moderate	High	Moderate	Moderate	Moderate	High	Moderate	Moderate	High	Weak
High	Low	Moderate	Moderate	High	Low	Moderate	Moderate	High	Low	Moderate	Moderate	Moderate	Moderate
High	Moderate	High	Moderate	High	Moderate	Moderate	Moderate	High	Moderate	Moderate	Moderate	High	Weak
High	High	High	Moderate	High	High	Moderate	Moderate	High	High	Moderate	Moderate	High	Weak
Low	Low	Low	High	Low	Low	Moderate	High	Low	Low	Moderate	Moderate	Moderate	Moderate
Low	Moderate	Moderate	High	Low	Moderate	Moderate	High	Low	Moderate	Moderate	Moderate	Moderate	Moderate
Low	High	Moderate	High	Low	High	High	High	Low	High	High	High	High	Weak
Moderate	Low	Moderate	High	Moderate	Low	Moderate	High	Moderate	Low	Moderate	Moderate	Moderate	Moderate
Moderate	Moderate	Moderate	High	Moderate	Moderate	Moderate	High	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
Moderate	High	High	High	Moderate	High	High	High	Moderate	High	High	High	High	Weak
High	Low	Moderate	High	High	Low	High	High	High	Low	High	High	High	Weak
High	Moderate	High	High	High	Moderate	High	High	High	Moderate	High	High	High	Weak
High	High	High	High	High	High	High	High	High	High	High	High	High	Weak

Appendix 5: CVSS Metrics

Base Metrics

Attack Vector (AV)

This metric reflects the context in which the vulnerability exploitation occurs. The values for this metric are;Network(N),adjacent Network(A),Local(L) and physical(P).The more remote an attacker can be to the target, the greater the vulnerability score. The possible values for this metric are listed in Table 1. This rationale is that, in general, the number of potential attackers for a remotely exploitable vulnerability would be much larger than that for an attack requiring local access.

Metric Value	**Description**
Network (N)	A vulnerability exploitable with network access means the Exploitable Scope is bound to the network stack and the attacker's path to the vulnerable system is at the network layer. Such a vulnerability is often termed "remotely exploitable". An example of a network attack is an RPC buffer overflow.
Adjacent Network (A)	A vulnerability exploitable with adjacent network access means the Exploitable Scope is bound to the network stack and the attacker's path to the vulnerable system is at the data link layer. Examples include local IP subnet, Bluetooth, IEEE 802.11, and local Ethernet segment. For instance, a vulnerability in this category would be a bug in application software that processes Ethernet frames.
Local (L)	A vulnerability exploitable with local access means the Exploitable Scope is not bound to the network stack and the attacker's path to the Exploitable Scope is via read / write / execute capabilities. If the attacker has the necessary Privileges Required to interact with the Exploitable Scope, they may be logged in locally; otherwise, they may deliver an exploit to a user and rely on User Interaction. An example of a locally exploitable vulnerability is a flaw in a word processing application when processing a malformed document.
Physical (P)	A vulnerability exploitable with physical access requires the ability to physically touch or manipulate the Exploitable Scope. Physical interaction may be brief (evil maid

attack) or persistent. Example of such an attack is cold boot attack [1] which allows an attacker to get access to disk encryption keys after gaining physical access to the system, or peripheral attacks such as Firewire/USB Direct Memory Access attacks.

Attack Complexity (AC)

This metric describes the conditions beyond the attacker’s control that must occur in order to place the system in a vulnerable state, this also excludes any user interaction requirements. The possible values for this metric are listed in Table 2.

Metric Value	**New Description**
High (H)	A successful attack depends on conditions outside the attacker's control. That is, a successful attack cannot be accomplished at-will, but requires the attacker to invest in some measurable amount of effort in preparation or execution against a specific target before successful attack can be expected. A successful attack depends on attackers overcoming one OR both of the following conditions: □ The attacker must gather target-specific reconnaissance; examples of this may include: target configuration settings, sequence numbers, shared secrets, etc. □ The attacker must prepare the target environment to improve exploit reliability; examples of preparation may include: repeated exploitation to win a race condition, performing a heap spray, etc
Low (L)	Specialized access conditions or extenuating circumstances do not exist. An attacker can expect repeatable exploit success against a vulnerable target

Privileges Required (PR)

This metric describes the privileges an attacker requires before successfully exploiting the vulnerability, and the potential impact they could inflict on a system after exploiting it. The possible values for this metric are listed in Table 3.

Metric Value	**Description**
High (H)	The attacker is authenticated with privileges that provide significant control over component resources. With these starting privileges an attacker can cause a Complete impact to one or more of: Confidentiality, Integrity, or Availability. Alternatively, an attacker with High privileges may have the ability to cause a Partial impact to sensitive resources.

Low (L)	The attacker is authenticated with privileges that provide basic, low-impact capabilities. With these starting privileges an attacker is able to cause a Partial impact to one or more of: Confidentiality, Integrity, or Availability. Alternatively, an attacker with Low privileges may have the ability to cause an impact only to non-sensitive resources.
None (N)	The attacker is unprivileged or unauthenticated.

User Interaction (UI)

This metric captures the requirement for a user (other than the attacker) to participate in the successful exploit of the target information system. The possible values for this metric are listed in Table 4. This new user interaction metric will determine whether or not the vulnerability can be exploited solely at the will of the attacker, or if a user must participate by taking action.

Metric Value	**Description**
None (N)	The vulnerable system can be exploited without any interaction from any user.
Required (R)	Successful exploitation of this vulnerability requires a user to take one or more actions that may or may not be expected in a scenario involving no exploitation, or a scenario involving content provided by a seemingly trustworthy source.

Confidentiality Impact (C)

This metric measures the impact to confidentiality of a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. The possible values for this metric are listed in Table 6. Increased confidentiality impact increases the vulnerability score.

Metric Value	**Description**
None (N)	There is no impact to confidentiality within the affected scope.
Low (L)	There is informational disclosure or a bypass of access controls. Access to some restricted information is obtained, but the attacker does not have control over what is obtained, or the scope of the loss is constrained. The information disclosure does not have a direct, serious impact on the affected scope.

High (H)	There is total information disclosure, resulting in all resources in the affected scope being divulged to the attacker. Alternatively, access to only some restricted information is obtained, but the disclosed information presents a direct, serious impact to the affected scope (e.g. the attacker can read the administrator's password, or private keys in memory are disclosed to the attacker).

Integrity Impact (I)

This metric measures the impact to integrity of a successfully exploited vulnerability. Integrity refers to the trustworthiness and guaranteed veracity of information. The possible values for this metric are listed in Table 7. Increased integrity impact increases the vulnerability score.

Metric Value	**Description**
None (N)	There is no impact to integrity within the affected scope.
Low (L)	Modification of data is possible, but the attacker does not have control over the end result of a modification, or the scope of modification is constrained. The data modification does not have a direct, serious impact on the affected scope.
High (H)	There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised. The attacker is able to modify any files on the target system.

Availability Impact (A)

This metric measures the impact to the availability of the affected Impact Scope resulting from a successfully exploited vulnerability. While the Confidentiality and Integrity impact metrics apply to the loss of confidentiality or integrity of data (e.g. information, files) used by a affected Impact Scope, this metric refers to the loss of availability of the affected Impact Scope, itself, such as networked service (e.g. web, database, email, etc). Since availability refers to the accessibility of information resources, attacks that consume network bandwidth, processor cycles, or disk space all impact the availability of an affected Impact Scope. The possible values for this metric are listed in Table 8. Increased availability impact increases the vulnerability score.

Metric Value	**Description**
None (N)	There is no impact to availability within the affected scope.
Low (L)	There is reduced performance or interruptions in resource availability. The attacker does not have the ability to completely deny service to legitimate users, even through repeated exploitation of the vulnerability. The resources in the affected scope are either partially available all of the time, or fully available only some of the time, but the overall there is no direct, serious impact to the affected scope.
High (H)	There is total loss of availability, resulting in the attacker being able to fully deny access to resources in the affected scope; this loss is either sustained (while the attacker continues to deliver the attack) or persistent (the condition persists even after the attack has completed). Alternatively, the attacker has the ability to deny some availability, but the loss of availability presents a direct, serious impact to the affected scope (e.g. the attacker cannot disrupt existing connections, but can prevent new connections; the attacker can repeatedly exploit a vulnerability that, in each instance of a successful attack, leaks a only small amount of memory, but after repeated exploitation causes a service to become completely unavailable).

Temporal Metrics

Exploitability (E)

This metric measures the current state of exploit techniques or code availability. Public availability of easy-to-use exploit code increases the number of potential attackers by including those who are unskilled, thereby increasing the severity of the vulnerability.

Initially, real-world exploitation may only be theoretical. Publication of proof of concept code, functional exploit code, or sufficient technical details necessary to exploit the vulnerability may follow. Furthermore, the exploit code available may progress from a proof-of-concept demonstration to exploit code that is successful in exploiting the vulnerability consistently. In severe cases, it may be delivered as the payload of a network-based worm or virus. The possible values for this metric are listed in Table 9. The more easily a vulnerability can be exploited, the higher the vulnerability score.

Metric Value	Description
Unproven (U)	No exploit code is available, or an exploit is entirely theoretical
Proof-of-Concept (P)	Proof-of-concept exploit code or an attack demonstration that is not practical for most systems is available. The code or technique is not functional in all situations and may require substantial modification by a skilled attacker.
Functional (F)	Functional exploit code is available. The code works in most situations where the vulnerability exists.
High (H)	Either the vulnerability is exploitable by functional mobile autonomous code, or no exploit is required (manual trigger) and details are widely available. The code works in every situation, or is actively being delivered via a mobile autonomous agent (such as a worm or virus).
Not Defined (X)	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

Remediation Level (RL)
The remediation level of a vulnerability is an important factor for prioritization. The typical vulnerability is unpatched when initially published. Workarounds or hotfixes may offer interim remediation until an official patch or upgrade is issued. Each of these respective stages adjusts the temporal score downwards, reflecting the decreasing urgency as remediation becomes final. The possible values for this metric are listed in Table 10. The less official and permanent a fix, the higher the vulnerability score is.

Metric Value	Description
Official Fix (O)	A complete vendor solution is available. Either the vendor has issued an official patch, or an upgrade is available.
Temporary Fix (T)	There is an official but temporary fix available. This includes instances where the vendor issues a temporary hotfix, tool, or workaround.
Workaround (W)	There is an unofficial, non-vendor solution available. In some cases, users of the affected technology will create a patch of their own or provide steps to work around or otherwise mitigate the vulnerability.
Unavailable (U)	There is either no solution available or it is impossible to apply.
Not Defined (X)	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

Report Confidence (RC)

This metric measures the degree of confidence in the existence of the vulnerability and the credibility of the known technical details. Sometimes, only the existence of vulnerabilities are publicized, but without specific details. For example, an impact may be recognized as undesirable, but the root cause may not be known. The vulnerability may later be corroborated by research which suggests where the vulnerability may lie, though the research may not be certain. Finally, a vulnerability may be confirmed through acknowledgement by the author or vendor of the affected technology. The urgency of a vulnerability is higher when a vulnerability is known to exist with certainty. This metric also suggests the level of technical knowledge available to would-be attackers. The possible values for this metric are listed in Table 11. The more a vulnerability is validated by the vendor or other reputable sources, the higher the score.

Metric Value	**Description**
Unknown [U]	There are reports of impacts that indicate a vulnerability is present. The reports indicate that the cause of the vulnerability is unknown, or reports may differ on the cause or impacts of the vulnerability. Reporters are uncertain of the true nature of the vulnerability, and there is little confidence in the validity of the reports or whether a static Base Score can be applied given the differences described. An example is a bug report which notes that an intermittent but non-reproducible crash occurs, with evidence of memory corruption suggesting that denial of service, or possible more serious impacts, may result.
Reasonable (R)	Significant details are published, but Researchers either do not have full confidence in the root cause, or do not have access to source code to fully confirm all of the interactions that may lead to the result. Reasonable confidence exists, however, that the bug is reproducible and at least one impact is able to be verified (Proof-of-concept exploits may provide this). An example is a detailed write-up of research into a vulnerability with an explanation (possibly obfuscated or "left as an exercise to the reader") that gives assurances on how to reproduce the results.
Confirmed (C)	Detailed reports exist, or functional reproduction is possible (functional exploits may provide this). Source code is available to independently verify the assertions of the research, or the author or vendor of the affected code has confirmed the presence of the vulnerability.
Not Defined (X)	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

Environmental Metrics
Security Requirements (CR, IR, AR)
These metrics enable the analyst to customize the CVSS score depending on the importance of the affected IT asset to a user's organization, measured in terms of confidentiality, integrity, and availability, That is, if an IT asset supports a business function for which availability is most important, the analyst can assign a greater value to availability, relative to confidentiality and integrity. Each security requirement has three possible values: "low," "Moderate," or "high."

The full effect on the environmental score is determined by the corresponding base impact metrics. That is, these metrics modify the environmental score by reweighting the (base) confidentiality, integrity, and availability impact metrics. For example, the confidentiality impact (C) metric has increased weight if the confidentiality requirement (CR) is "high." Likewise, the confidentiality impact metric has decreased weight if the confidentiality requirement is "low." The confidentiality impact metric weighting is neutral if the confidentiality requirement is "Moderate." This same logic is applied to the integrity and availability requirements.

Note that the confidentiality requirement will not affect the environmental score if the (base) confidentiality impact is set to "none." Also, increasing the confidentiality requirement from "Moderate" to "high" will not change the environmental score when the (base) impact metrics are set to "complete." This is because the impact sub score (part of the base score that calculates impact) is already at a maximum value of 10.

The possible values for the security requirements are listed in Table 12. For brevity, the same table is used for all three metrics. The greater the security requirement, the higher the score (remember that "Moderate" is considered the default). These metrics will modify the score as much as plus or minus 2.5.

Metric Value	**Description**
Low (L)	Loss of [confidentiality | integrity | availability] is likely to have only a limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
Moderate (M)	Loss of [confidentiality | integrity | availability] is likely to have a serious adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
High (H)	Loss of [confidentiality | integrity | availability] is likely to have a catastrophic adverse effect on the organization or individuals associated with the organization (e.g., employees, customers).
Not Defined (X)	Assigning this value to the metric will not influence the score. It is a signal to the equation to skip this metric.

Appendix 6: Code for Propagating Values in the Model

```
<script language= "javascript">
function propagate()
{
var AMV = eval(document.getElementById("AM").value);
var CSV = eval(document.getElementById("CS").value);
var CDV = eval(document.getElementById("CD").value);
var CUV = eval(document.getElementById("CU").value);
var AFV = eval(document.getElementById("AF").value);
var ASPV = eval(document.getElementById("ASP").value);
var UDSV = eval(document.getElementById("UDS").value);
var ACSV = eval(document.getElementById("AC").value);
var WPSvalue=((AMV *AMV)+(CSV*CSV))/(AMV+CSV);
var FESSvalue=((CDV *CDV)+(CUV*CUV) +(AFV*AFV))/(CDV + CUV+ AFV) ;
var BASvalue=((ASPV *ASPV)+(UDSV*UDSV) +(ACSV*ACSV))/(ASPV +
UDSV+ACSV) ;
if (WPSvalue>2.5)
{
var WPSvalueR=1;
var WPSweight=3;
document.main.WPS.value= ("Strong");
}
else if(WPSvalue>=1.5)
{
WPSvalueR=2;
WPSweight=2;
document.main.WPS.value=("Moderate")
}
else if(WPSvalue<1.5)
{
 WPSvalueR=3;
 WPSweight=1;
```

```
document.main.WPS.value=("Weak")
}
else
{
document.main.WPS.value=("Unknown")
}
if (FESSvalue>2.5)
{
var FESSvalueR=3;
var FESSweight=3;
document.main.FESS.value= ("Strong");
}
else if(FESSvalue>=1.5)
{
FESSvalueR=2;
FESSweight=2;
document.main.FESS.value=("Moderate")
}
else if(FESSvalue<1.5)
{
FESSvalueR=1;
FESSweight=1;
document.main.FESS.value=("Weak")
}
else
{
document.main.FESS.value=("Unknown")
}
if (BASvalue>2.5)
{
var BASvalueR=3;
var BASweight=3;
```

```
document.main.BAS.value= ("Strong")
}
else if(BASvalue>=1.5)
{
BASvalueR=2;
BASweight=2;
document.main.BAS.value=("Moderate")
}
else if(BASvalue<1.5)
{
BASvalueR=1;
BASweight=1;
document.main.BAS.value=("Weak")
}
else
{
document.main.BAS.value=("Unknown")
}
WTCBvalue=((FESSweight*FESSvalueR) +(BASweight*BASvalueR))/((FESSweight)
+(BASweight));
if (WTCBvalue >2.5)
{
var WTCBvalueR=1;
var WTCBweight=3;
document.main.WTCB.value= ("Strong")
}
else if(WTCBvalue>=1.5)
{
WTCBvalueR=2;
WTCBweight=2;
document.main.WTCB.value=("Moderate")
}
```

```
else if(WTCBvalue<1.5)
{
WTCBvalueR=3;
WTCBweight=1;
document.main.WTCB.value=("Weak")
}
else
{
document.main.WTCB.value=("Unknown")
}
ASvalue=((WPSweight* WPSvalueR) +(WTCBweight *WTCBvalueR))/(WPSweight
+WTCBweight);

if (ASvalue>2.5)
{
document.main.AS.value= ("High")
document.main.WAACS.value= ("Weak")
}
else if (ASvalue>2.0)
{
document.main.AS.value= ("Moderate High")
document.main.WAACS.value= ("Moderate Weak")
}
else if (ASvalue==2.0)
{
document.main.AS.value= ("Moderate")
document.main.WAACS.value= ("Moderate")
}
else if (ASvalue>=1.5)
{
document.main.AS.value= ("Moderate Low")
document.main.WAACS.value= ("Moderate Strong")
```

```
}
else if(ASvalue<1.5)
{
document.main.AS.value=("Low")
document.main.WAACS.value= ("Strong")
}
else
{
document.main.AS.value=("Unknown")
}
 if (CSV==0)
{
document.main.Remarks2.value=("Cipher Suite extremely vulnerable:Not
Recommended");
document.main.WAACS.value=("Very Weak")
document.main.AS.value=("Very High")
document.main.WPS.value=("Very Weak");
 }

 if (AMV==0)
   {
document.main.Remarks1.value=("Authentication Mechanism  extremely vulnerable:Not
Recommended");
document.main.WAACS.value=("Very Weak")
document.main.AS.value=("Very High")
document.main.WPS.value=("Very Weak");
   }
 if (AFV==0)
   {
document.main.Remarks5.value=("Accesspoint firmware  extremely vulnerable: Not
Recommended");
document.main.WAACS.value=("Very Weak")
document.main.AS.value=("Very High")
document.main.FESS.value=("Very Weak");
document.main.WTCB.value=("Very weak");
   }
if (CUV==0)
   {
document.main.Remarks4.value=("Client Utility extremely vulnerable:Not
Recommended");
document.main.WAACS.value=("Very Weak");
document.main.AS.value=("Very High");
document.main.FESS.value=("Very Weak");
document.main.WTCB.value=("Very weak");
   }
if (CDV==0)
   {
document.main.Remarks3.value=("Client Driver extremely vulnerable:Not
Recommended");
document.main.WAACS.value=("Very Weak");
document.main.AS.value=("Very High");
document.main.FESS.value=("Very Weak");
document.main.WTCB.value=("Very weak");
   }
if (ASPV==0)
   {
document.main.Remarks6.value=("Authentication Server  extremely vulnerable:Not
Recommended");
document.main.WAACS.value=("Very Weak");
document.main.AS.value=("Very High");
document.main.BAS.value=("Very Weak");
document.main.WTCB.value=("Very Weak");
   }
  if (UDSV==0)
```

```
{
document.main.Remarks7.value=("User database  extremely vulnerable:Not
Recommended");
document.main.WAACS.value=("Very Weak");
document.main.AS.value=("Very High");
document.main.BAS.value=("Very Weak");
document.main.WTCB.value=("Very weak");
   }
  if (ACSV==0)
{
document.main.Remarks8.value=("Authentication credentials  extremely vulnerable:Not
Recommended");
document.main.WAACS.value=("Very Weak");
document.main.AS.value=("Very High");
document.main.BAS.value=("Very Weak");
document.main.WTCB.value=("Very weak");
   }
}
</script>
```

Appendix 7: Rule Base Code for EAP Method Selection

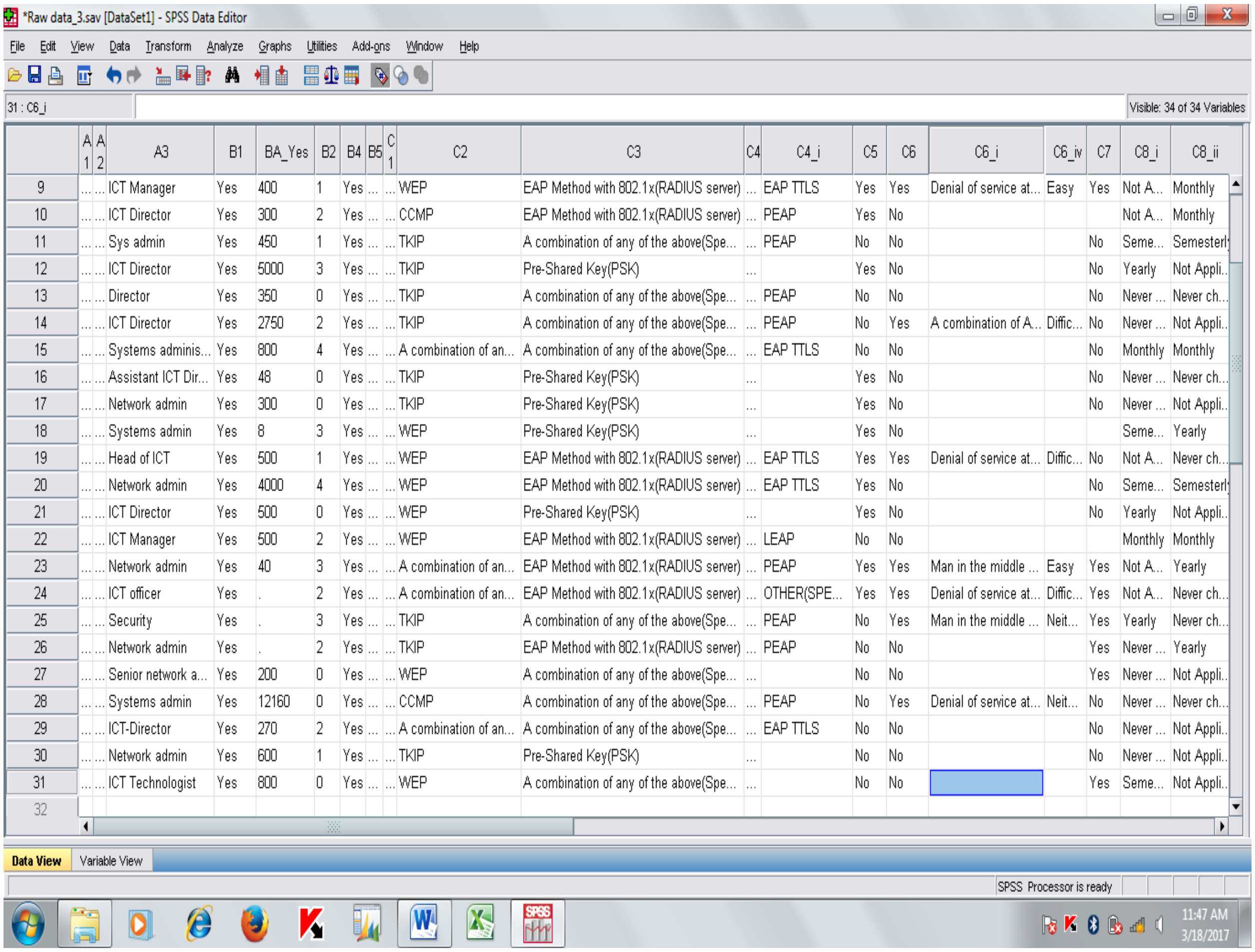
```
RULE [WEAK CIPHER SUITE IMPLEMENTED]
If   [CIPHER SUITE]="No"
Then [EAP METHOD]="WEAK CIPHER SUITE IMPLEMENTED"
RULE [NO_EAP_METHOD_IS_APPLICABLE]
If   [802.1x_IMPLEMENTED]="No" and
     [UPGRADABLE]="No"
Then [EAP METHOD]="NO EAP METHOD IS APPLICABLE"
RULE [NO_EAP_METHOD_IS_APPLICABLE]
If   [802.1x_IMPLEMENTED] = "No" and
     [UPGRADABLE]="Yes" and
     [READY_TO_UPGRADE]="No"
Then [EAP METHOD]="NO EAP METHOD IS APPLICABLE"
RULE [TTLS]
If   [CIPHER SUITE]="Yes" and
     [802.1x_IMPLEMENTED] = "Yes" and
     [Communicating parties protection] ="Yes" and
     [Legacy Methods]="Yes"
Then [EAP METHOD]="TUNNELED TRANSPORT LAYER SECURITY [EAP-TTLS] RECOMMENDED"
RULE [TTLS]
If   [CIPHER SUITE]="Yes" and
     [802.1x_IMPLEMENTED] = "No" and
     [UPGRADABLE]="Yes" and
     [READY_TO_UPGRADE]="Yes" and
     [Communicating parties protection] ="Yes" and
     [Legacy Methods]="Yes"
Then [EAP METHOD]="TUNNELED TRANSPORT LAYER SECURITY [EAP-TTLS] RECOMMENDED"
RULE [PEAP]
If   [CIPHER SUITE]="Yes" and
     [802.1x_IMPLEMENTED] = "Yes" and
```

```
    [Communicating parties protection] ="Yes" and
    [Legacy Methods]="No"
Then [EAP METHOD]=" PROTECTED EAP[PEAP] RECOMMENDED"
RULE [PEAP]
If   [CIPHER SUITE]="Yes" and
    [802.1x_IMPLEMENTED] = "No" and
    [UPGRADABLE]="Yes" and
    [READY_TO_UPGRADE]="Yes" and
    [Communicating parties protection] ="Yes" and
    [Legacy Methods]="No"
Then [EAP METHOD]=" PROTECTED EAP[PEAP] RECOMMENDED"
RULE [TLS]
If   [CIPHER SUITE]="Yes" and
    [802.1x_IMPLEMENTED] = "Yes" and
    [Communicating parties protection] ="No" and
    [Digital certificates]="Yes"
Then [EAP METHOD]="TRANSPORT LAYER SECURITY[TLS] RECOMMENDED"
RULE [TLS]
If   [CIPHER SUITE]="Yes" and
    [802.1x_IMPLEMENTED] = "No" and
    [UPGRADABLE]="Yes" and
    [READY_TO_UPGRADE]="Yes" and
    [Communicating parties protection] ="No" and
    [Digital certificates]="Yes"
Then [EAP METHOD]="TRANSPORT LAYER SECURITY[TLS] RECOMMENDED"
RULE [EAP-FAST]
If   [CIPHER SUITE]="Yes" and
    [802.1x_IMPLEMENTED] = "Yes" and
    [Communicating parties protection] ="No" and
    [Digital certificates]="No" and
    [Difficulties in enforcing password security]= "Yes"
```

```
Then [EAP METHOD]=" FLEXIBLE AUTHENTICATION VIA SECURE
TUNNELING[EAP-FAST] RECOMMENDED"
RULE [EAP-FAST]
If   [CIPHER SUITE]="Yes" and
     [802.1x_IMPLEMENTED] = "No" and
     [UPGRADABLE]="Yes" and
     [READY_TO_UPGRADE]="Yes" and
     [Communicating parties protection] ="No" and
     [Digital certificates]="No"and
     [Difficulties in enforcing password security]= "Yes"
Then [EAP METHOD]=" FLEXIBLE AUTHENTICATION VIA SECURE
TUNNELING[EAP-FAST] RECOMMENDED"
RULE [LEAP]
If   [CIPHER SUITE]="Yes" and
     [802.1x_IMPLEMENTED] = "Yes" and
     [Communicating parties protection] ="No" and
     [Digital certificates]="No" and
     [Difficulties in enforcing password security]= "No"
Then [EAP METHOD]=" LIGHTWEIGHT Extensible authentication protocol[LEAP]
RECOMMENDED"
RULE [LEAP]
If   [CIPHER SUITE]="Yes" and
     [802.1x_IMPLEMENTED] = "No" and
     [UPGRADABLE]="Yes" and
     [READY_TO_UPGRADE]="Yes" and
     [Communicating parties protection] ="No" and
     [Digital certificates]="No"and
     [Difficulties in enforcing password security]= "No"
Then [EAP METHOD]="LIGHTWEIGHT Extensible authentication protocol[LEAP]
RECOMMENDED"
REM =======END OF RULES========
REM ===START OF EAP PROMPTS========
PROMPT [CIPHER SUITE]MultChoice
"Is your infrastructure currently implemented/configured to support CCMP OR TKIP or a
combination of both?"
  "Yes"
  "No"
PROMPT [802.1x_IMPLEMENTED]MultChoice
"Is your infrastructure currently implemented/configured to support 802.1x?"
  "Yes"
  "No"
PROMPT [UPGRADABLE]MultChoice
"If Your Infrastructure is not currently implemented/configured to support 802.1x,is it
upgradable?"
  "Yes"
  "No"
PROMPT [READY_TO_UPGRADE]MultChoice
"If Your Infrastructure is not currently implemented/configured to support 802.1x and is
upgradable,are you as an implementer ready to upgrade?"
  "Yes"
  "No"
PROMPT [Communicating parties protection]MultChoice
"Do you need to protect Communicating parties in your WLAN?"
  "Yes"
  "No"
PROMPT [Legacy Methods]MultChoice
"Do you need to use legacy EAP authentication methods in your WLAN?"
  "Yes"
  "No"
PROMPT [Digital certificates]MultChoice
"Are you currently using digital certificates for other applications in your LAN?"
  "Yes"
  "No"
PROMPT [Difficulties in enforcing password security]MultChoice
```

```
"Are you currently facing difficulties in enforcing password security among your Network users??"
   "Yes"
   "No"
REM ====================================
REM ===== END OF EAP PROMPTS =====
REM ====================================
GOAL [EAP METHOD]
REM THE [GOAL] SETS THE TERMINATING POINT OF A SUCCESSFUL INQUIRY IN THE EXPERT SYSTEM
```

Appendix 8:Preliminary Survey Raw Data



*Raw data_3.sav [DataSet1] - SPSS Data Editor

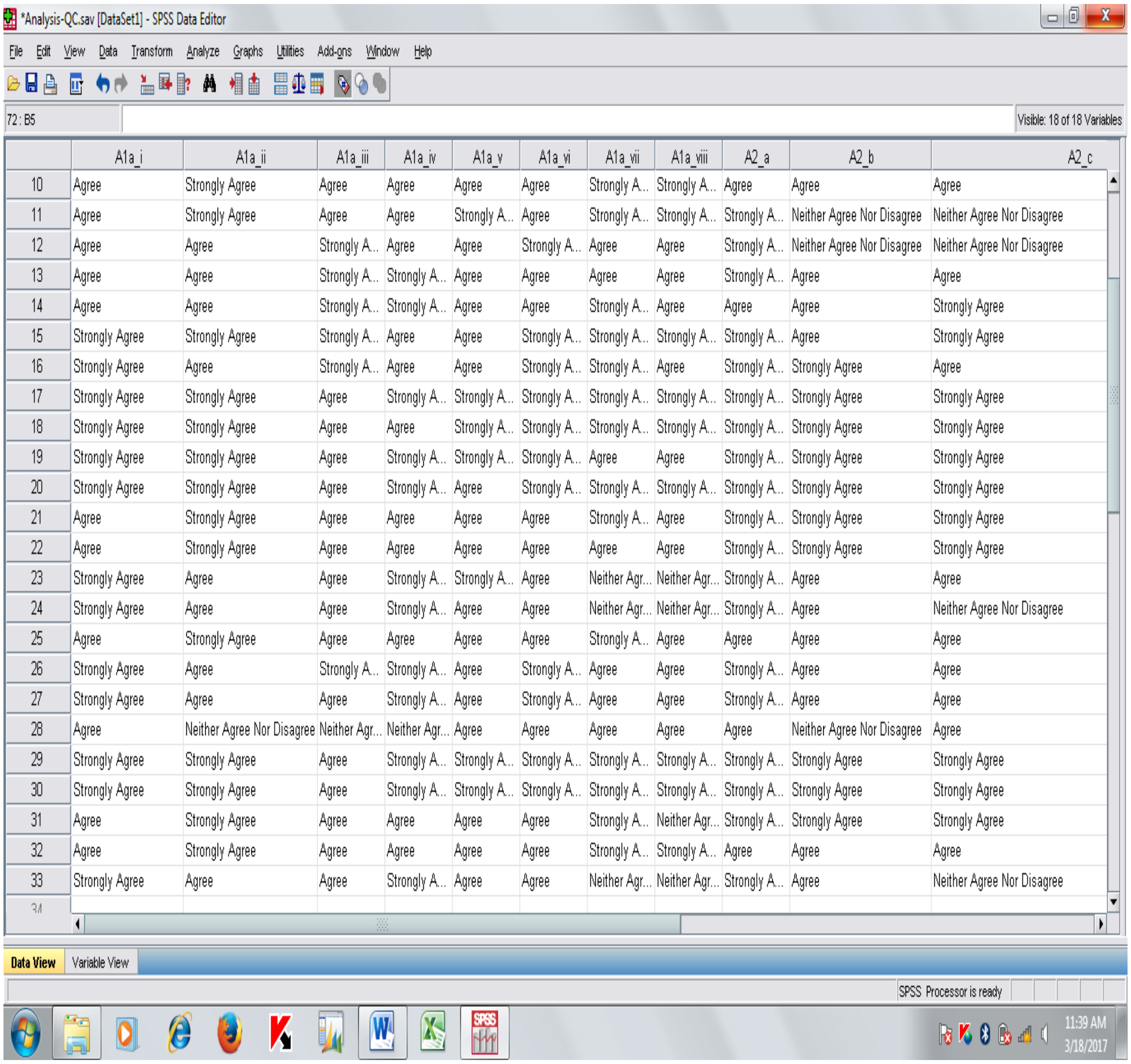
31 : C6_i

Visible: 34 of 34 Variables

	A 1	A 2	A3	B1	BA_Yes	B2	B4	B5	C 1	C2	C3	C4	C4_i	C5	C6	C6_i	C6_iv	C7	C8_i	C8_ii
9	...	...	ICT Manager	Yes	400	1	Yes	...	...	WEP	EAP Method with 802.1x(RADIUS server)	...	EAP TTLS	Yes	Yes	Denial of service at...	Easy	Yes	Not A...	Monthly
10	...	...	ICT Director	Yes	300	2	Yes	...	...	CCMP	EAP Method with 802.1x(RADIUS server)	...	PEAP	Yes	No				Not A...	Monthly
11	...	...	Sys admin	Yes	450	1	Yes	...	...	TKIP	A combination of any of the above(Spe...	...	PEAP	No	No			No	Seme...	Semesterl
12	...	...	ICT Director	Yes	5000	3	Yes	...	...	TKIP	Pre-Shared Key(PSK)	...		Yes	No			No	Yearly	Not Appli...
13	...	...	Director	Yes	350	0	Yes	...	...	TKIP	A combination of any of the above(Spe...	...	PEAP	No	No			No	Never ...	Never ch...
14	...	...	ICT Director	Yes	2750	2	Yes	...	...	TKIP	A combination of any of the above(Spe...	...	PEAP	No	Yes	A combination of A...	Diffic...	No	Never ...	Not Appli...
15	...	...	Systems adminis...	Yes	800	4	Yes	...	...	A combination of an...	A combination of any of the above(Spe...	...	EAP TTLS	No	No			No	Monthly	Monthly
16	...	...	Assistant ICT Dir...	Yes	48	0	Yes	...	...	TKIP	Pre-Shared Key(PSK)	...		Yes	No			No	Never ...	Never ch...
17	...	...	Network admin	Yes	300	0	Yes	...	...	TKIP	Pre-Shared Key(PSK)	...		Yes	No			No	Never ...	Not Appli...
18	...	...	Systems admin	Yes	8	3	Yes	...	...	WEP	Pre-Shared Key(PSK)	...		Yes	No				Seme...	Yearly
19	...	...	Head of ICT	Yes	500	1	Yes	...	...	WEP	EAP Method with 802.1x(RADIUS server)	...	EAP TTLS	Yes	Yes	Denial of service at...	Diffic...	No	Not A...	Never ch...
20	...	...	Network admin	Yes	4000	4	Yes	...	...	WEP	EAP Method with 802.1x(RADIUS server)	...	EAP TTLS	Yes	No			No	Seme...	Semesterl
21	...	...	ICT Director	Yes	500	0	Yes	...	...	WEP	Pre-Shared Key(PSK)	...		Yes	No			No	Yearly	Not Appli...
22	...	...	ICT Manager	Yes	500	2	Yes	...	...	WEP	EAP Method with 802.1x(RADIUS server)	...	LEAP	No	No				Monthly	Monthly
23	...	...	Network admin	Yes	40	3	Yes	...	...	A combination of an...	EAP Method with 802.1x(RADIUS server)	...	PEAP	Yes	Yes	Man in the middle ...	Easy	Yes	Not A...	Yearly
24	...	...	ICT officer	Yes	.	2	Yes	...	...	A combination of an...	EAP Method with 802.1x(RADIUS server)	...	OTHER(SPE...	Yes	Yes	Denial of service at...	Diffic...	Yes	Not A...	Never ch...
25	...	...	Security	Yes	.	3	Yes	...	...	TKIP	A combination of any of the above(Spe...	...	PEAP	No	Yes	Man in the middle ...	Neit...	Yes	Yearly	Never ch...
26	...	...	Network admin	Yes	.	2	Yes	...	...	TKIP	EAP Method with 802.1x(RADIUS server)	...	PEAP	No	No			Yes	Never ...	Yearly
27	...	...	Senior network a...	Yes	200	0	Yes	...	...	WEP	A combination of any of the above(Spe...	...		No	No			Yes	Never ...	Not Appli...
28	...	...	Systems admin	Yes	12160	0	Yes	...	...	CCMP	A combination of any of the above(Spe...	...	PEAP	No	Yes	Denial of service at...	Neit...	No	Never ...	Never ch...
29	...	...	ICT-Director	Yes	270	2	Yes	...	...	A combination of an...	A combination of any of the above(Spe...	...	EAP TTLS	No	No			No	Never ...	Not Appli...
30	...	...	Network admin	Yes	600	1	Yes	...	...	TKIP	Pre-Shared Key(PSK)	...		No	No			No	Never ...	Not Appli...
31	...	...	ICT Technologist	Yes	800	0	Yes	...	...	WEP	A combination of any of the above(Spe...	...		No	No			Yes	Seme...	Not Appli...
32																				

SPSS Processor is ready

Appendix 9:Conceptual Model Validation Raw Data



*Analysis-QC.sav [DataSet1] - SPSS Data Editor

File Edit View Data Transform Analyze Graphs Utilities Add-ons Window Help

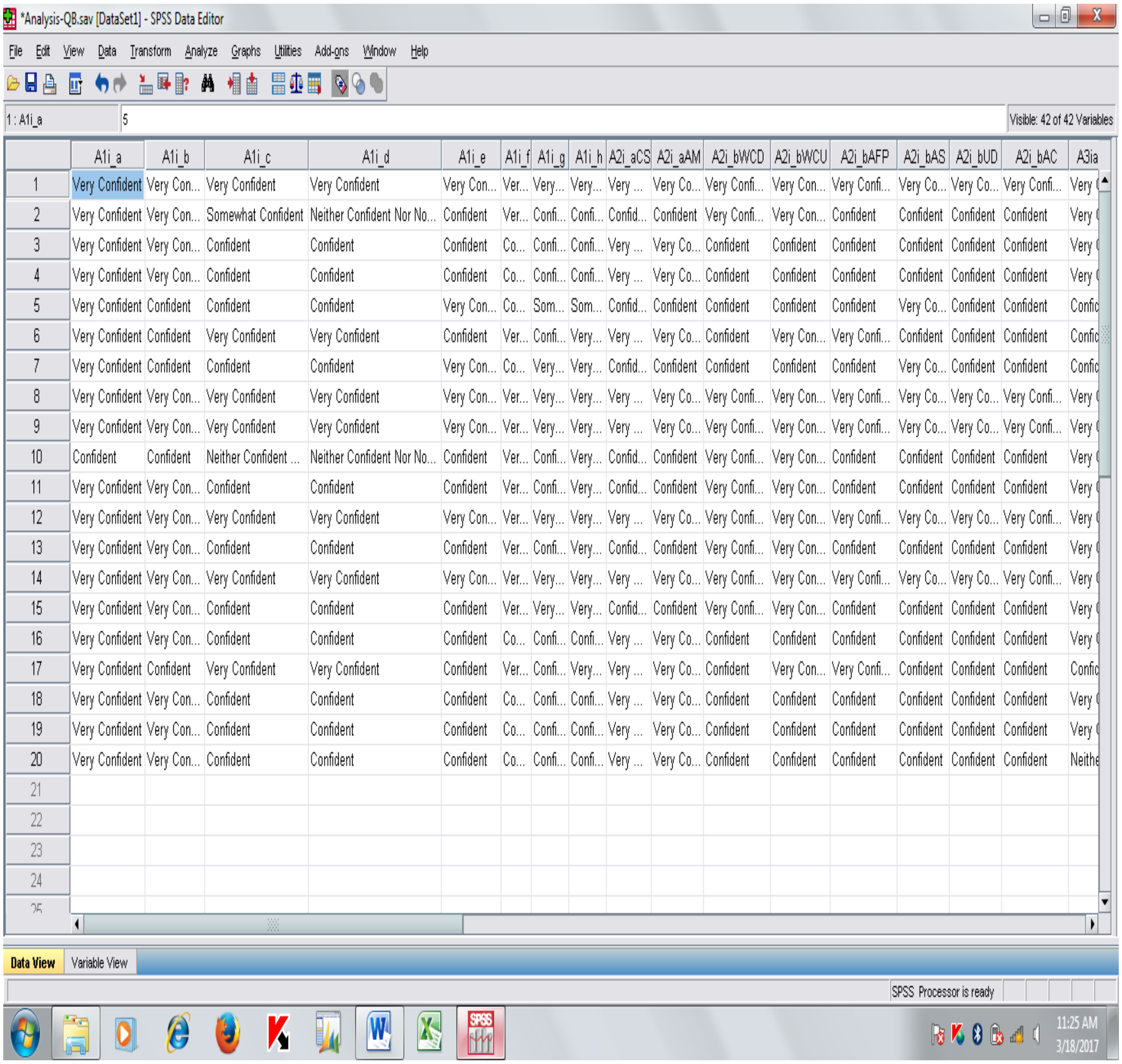
72 : B5

Visible: 18 of 18 Variables

	A1a_i	A1a_ii	A1a_iii	A1a_iv	A1a_v	A1a_vi	A1a_vii	A1a_viii	A2_a	A2_b	A2_c
10	Agree	Strongly Agree	Agree	Agree	Agree	Agree	Strongly A...	Strongly A...	Agree	Agree	Agree
11	Agree	Strongly Agree	Agree	Agree	Strongly A...	Agree	Strongly A...	Strongly A...	Strongly A...	Neither Agree Nor Disagree	Neither Agree Nor Disagree
12	Agree	Agree	Strongly A...	Agree	Agree	Strongly A...	Agree	Agree	Strongly A...	Neither Agree Nor Disagree	Neither Agree Nor Disagree
13	Agree	Agree	Strongly A...	Strongly A...	Agree	Agree	Agree	Agree	Strongly A...	Agree	Agree
14	Agree	Agree	Strongly A...	Strongly A...	Agree	Agree	Strongly A...	Agree	Agree	Agree	Strongly Agree
15	Strongly Agree	Strongly Agree	Strongly A...	Agree	Agree	Strongly A...	Strongly A...	Strongly A...	Strongly A...	Agree	Strongly Agree
16	Strongly Agree	Agree	Strongly A...	Agree	Agree	Strongly A...	Strongly A...	Agree	Strongly A...	Strongly Agree	Agree
17	Strongly Agree	Strongly Agree	Agree	Strongly A...	Strongly A...	Strongly A...	Strongly A...	Strongly A...	Strongly A...	Strongly Agree	Strongly Agree
18	Strongly Agree	Strongly Agree	Agree	Agree	Strongly A...	Strongly A...	Strongly A...	Strongly A...	Strongly A...	Strongly Agree	Strongly Agree
19	Strongly Agree	Strongly Agree	Agree	Strongly A...	Strongly A...	Strongly A...	Agree	Agree	Strongly A...	Strongly Agree	Strongly Agree
20	Strongly Agree	Strongly Agree	Agree	Strongly A...	Agree	Strongly A...	Strongly A...	Strongly A...	Strongly A...	Strongly Agree	Strongly Agree
21	Agree	Strongly Agree	Agree	Agree	Agree	Agree	Strongly A...	Agree	Strongly A...	Strongly Agree	Strongly Agree
22	Agree	Strongly Agree	Agree	Agree	Agree	Agree	Agree	Agree	Strongly A...	Strongly Agree	Strongly Agree
23	Strongly Agree	Agree	Agree	Strongly A...	Strongly A...	Agree	Neither Agr...	Neither Agr...	Strongly A...	Agree	Agree
24	Strongly Agree	Agree	Agree	Strongly A...	Agree	Agree	Neither Agr...	Neither Agr...	Strongly A...	Agree	Neither Agree Nor Disagree
25	Agree	Strongly Agree	Agree	Agree	Agree	Agree	Strongly A...	Agree	Agree	Agree	Agree
26	Strongly Agree	Agree	Strongly A...	Strongly A...	Agree	Strongly A...	Agree	Agree	Strongly A...	Agree	Agree
27	Strongly Agree	Agree	Agree	Strongly A...	Agree	Strongly A...	Agree	Agree	Strongly A...	Agree	Agree
28	Agree	Neither Agree Nor Disagree	Neither Agr...	Neither Agr...	Agree	Agree	Agree	Agree	Agree	Neither Agree Nor Disagree	Agree
29	Strongly Agree	Strongly Agree	Agree	Strongly A...	Strongly A...	Strongly A...	Strongly A...	Strongly A...	Strongly A...	Strongly Agree	Strongly Agree
30	Strongly Agree	Strongly Agree	Agree	Strongly A...	Strongly A...	Strongly A...	Strongly A...	Strongly A...	Strongly A...	Strongly Agree	Strongly Agree
31	Agree	Strongly Agree	Agree	Agree	Agree	Agree	Strongly A...	Neither Agr...	Strongly A...	Strongly Agree	Strongly Agree
32	Agree	Strongly Agree	Agree	Agree	Agree	Agree	Strongly A...	Strongly A...	Agree	Agree	Agree
33	Strongly Agree	Agree	Agree	Strongly A...	Agree	Agree	Neither Agr...	Neither Agr...	Strongly A...	Agree	Neither Agree Nor Disagree
34											

SPSS Processor is ready

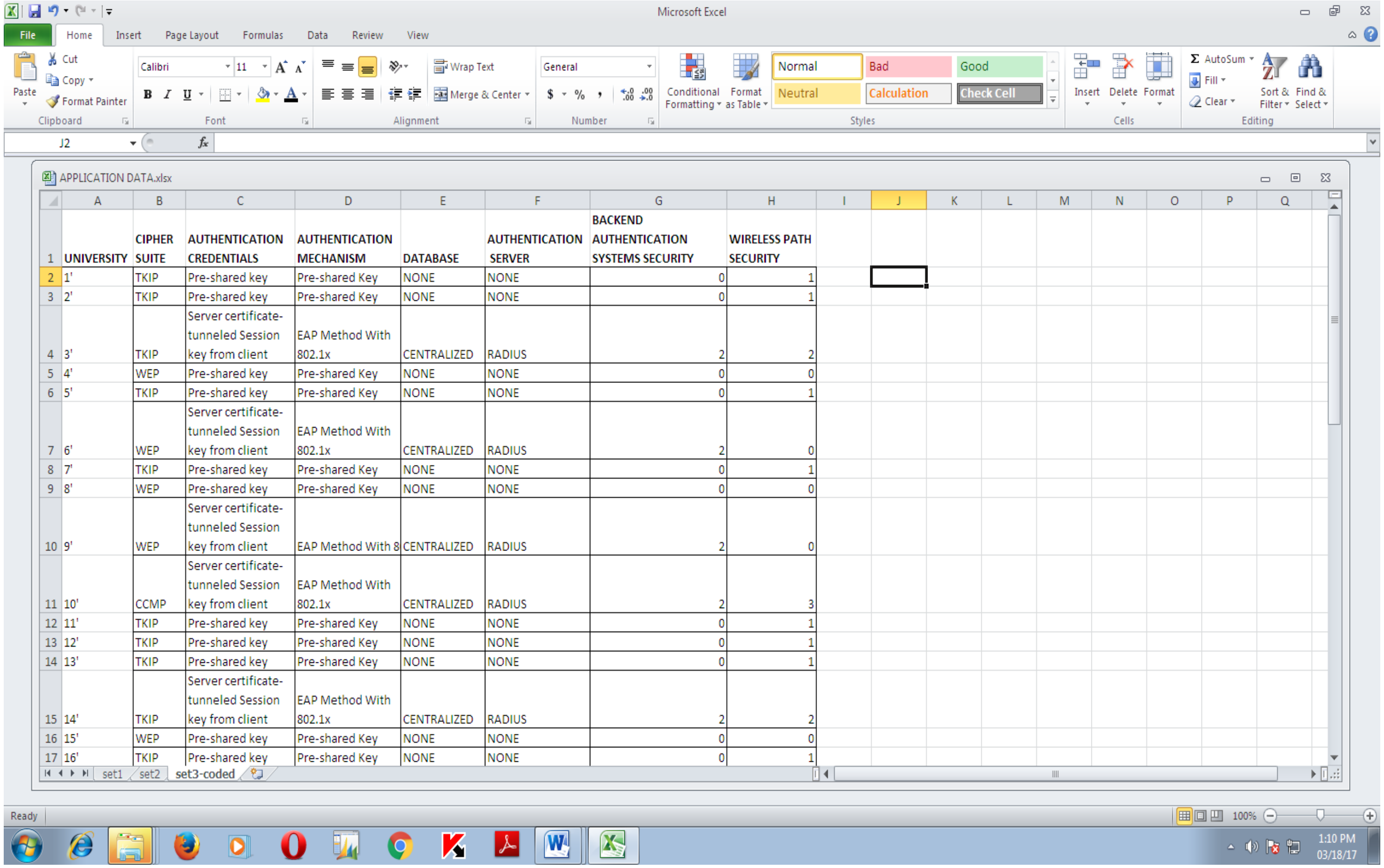
Appendix 10:Operational Model Validation Raw Data



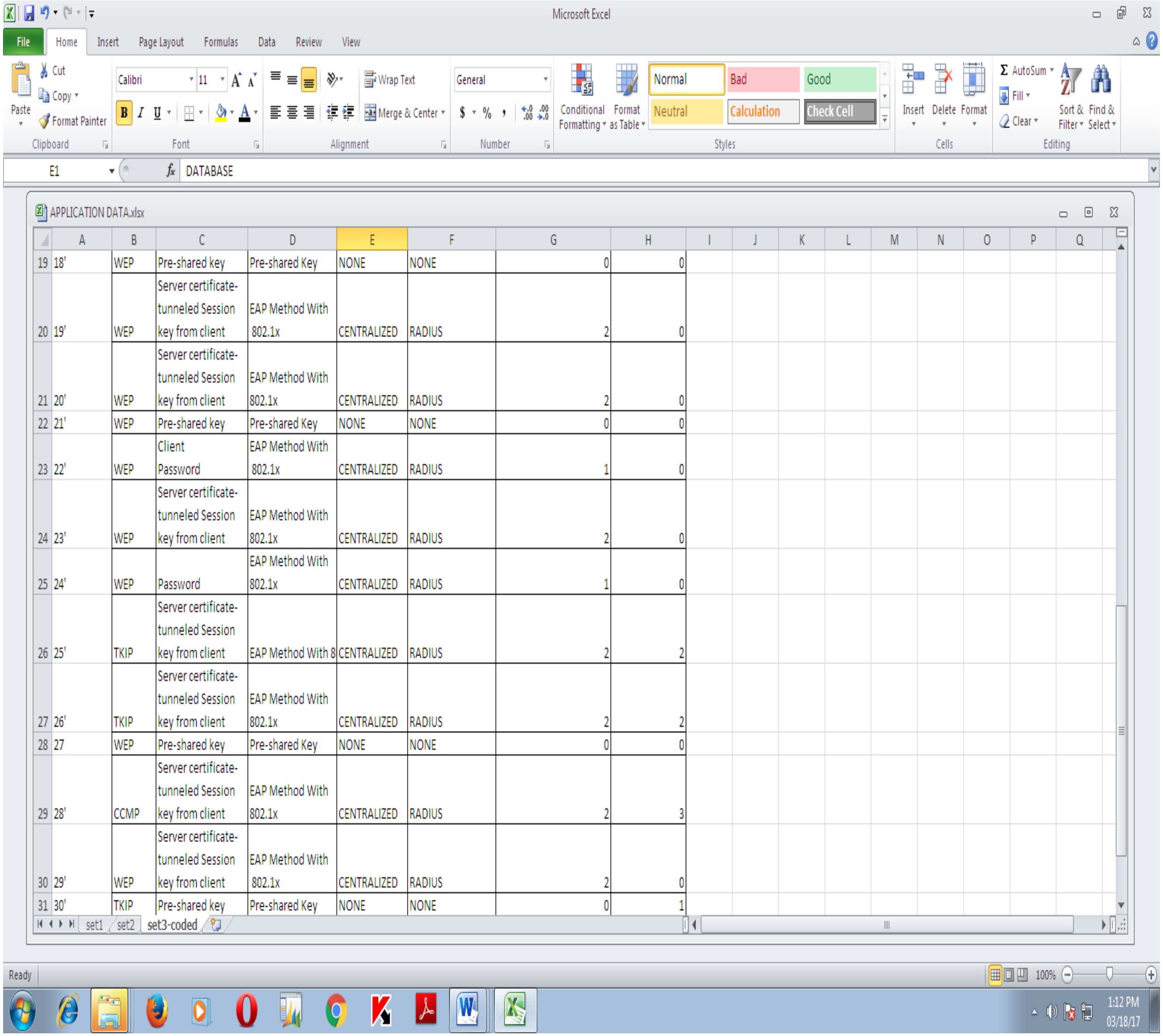
*Analysis-QB.sav [DataSet1] - SPSS Data Editor
File Edit View Data Transform Analyze Graphs Utilities Add-ons Window Help
1 : A1i_a
5
Visible: 42 of 42 Variables

	A1i_a	A1i_b	A1i_c	A1i_d	A1i_e	A1i_f	A1i_g	A1i_h	A2i_aCS	A2i_aAM	A2i_bWCD	A2i_bWCU	A2i_bAFP	A2i_bAS	A2i_bUD	A2i_bAC	A3ia
1	Very Confident	Very Con...	Very Confident	Very Confident	Very Con...	Ver...	Very...	Very...	Very ...	Very Co...	Very Confi...	Very Con...	Very Confi...	Very Co...	Very Co...	Very Confi...	Very C
2	Very Confident	Very Con...	Somewhat Confident	Neither Confident Nor No...	Confident	Ver...	Confi...	Confi...	Confid...	Confident	Very Confi...	Very Con...	Confident	Confident	Confident	Confident	Very C
3	Very Confident	Very Con...	Confident	Confident	Confident	Co...	Confi...	Confi...	Very ...	Very Co...	Confident	Confident	Confident	Confident	Confident	Confident	Very C
4	Very Confident	Very Con...	Confident	Confident	Confident	Co...	Confi...	Confi...	Very ...	Very Co...	Confident	Confident	Confident	Confident	Confident	Confident	Very C
5	Very Confident	Confident	Confident	Confident	Very Con...	Co...	Som...	Som...	Confid...	Confident	Confident	Confident	Confident	Very Co...	Confident	Confident	Confid
6	Very Confident	Confident	Very Confident	Very Confident	Confident	Ver...	Confi...	Very...	Very ...	Very Co...	Confident	Very Con...	Very Confi...	Confident	Confident	Confident	Confid
7	Very Confident	Confident	Confident	Confident	Very Con...	Co...	Very...	Very...	Confid...	Confident	Confident	Confident	Confident	Very Co...	Confident	Confident	Confid
8	Very Confident	Very Con...	Very Confident	Very Confident	Very Con...	Ver...	Very...	Very...	Very ...	Very Co...	Very Confi...	Very Con...	Very Confi...	Very Co...	Very Co...	Very Confi...	Very C
9	Very Confident	Very Con...	Very Confident	Very Confident	Very Con...	Ver...	Very...	Very...	Very ...	Very Co...	Very Confi...	Very Con...	Very Confi...	Very Co...	Very Co...	Very Confi...	Very C
10	Confident	Confident	Neither Confident ...	Neither Confident Nor No...	Confident	Ver...	Confi...	Very...	Confid...	Confident	Very Confi...	Very Con...	Confident	Confident	Confident	Confident	Very C
11	Very Confident	Very Con...	Confident	Confident	Confident	Ver...	Confi...	Very...	Confid...	Confident	Very Confi...	Very Con...	Confident	Confident	Confident	Confident	Very C
12	Very Confident	Very Con...	Very Confident	Very Confident	Very Con...	Ver...	Very...	Very...	Very ...	Very Co...	Very Confi...	Very Con...	Very Confi...	Very Co...	Very Co...	Very Confi...	Very C
13	Very Confident	Very Con...	Confident	Confident	Confident	Ver...	Confi...	Very...	Confid...	Confident	Very Confi...	Very Con...	Confident	Confident	Confident	Confident	Very C
14	Very Confident	Very Con...	Very Confident	Very Confident	Very Con...	Ver...	Very...	Very...	Very ...	Very Co...	Very Confi...	Very Con...	Very Confi...	Very Co...	Very Co...	Very Confi...	Very C
15	Very Confident	Very Con...	Confident	Confident	Confident	Ver...	Very...	Very...	Confid...	Confident	Very Confi...	Very Con...	Confident	Confident	Confident	Confident	Very C
16	Very Confident	Very Con...	Confident	Confident	Confident	Co...	Confi...	Confi...	Very ...	Very Co...	Confident	Confident	Confident	Confident	Confident	Confident	Very C
17	Very Confident	Confident	Very Confident	Very Confident	Confident	Ver...	Confi...	Very...	Very ...	Very Co...	Confident	Very Con...	Very Confi...	Confident	Confident	Confident	Confid
18	Very Confident	Very Con...	Confident	Confident	Confident	Co...	Confi...	Confi...	Very ...	Very Co...	Confident	Confident	Confident	Confident	Confident	Confident	Very C
19	Very Confident	Very Con...	Confident	Confident	Confident	Co...	Confi...	Confi...	Very ...	Very Co...	Confident	Confident	Confident	Confident	Confident	Confident	Very C
20	Very Confident	Very Con...	Confident	Confident	Confident	Co...	Confi...	Confi...	Very ...	Very Co...	Confident	Confident	Confident	Confident	Confident	Confident	Neithe
21																	
22																	
23																	
24																	
25																	

Appendix 11: Model Application-Raw Data



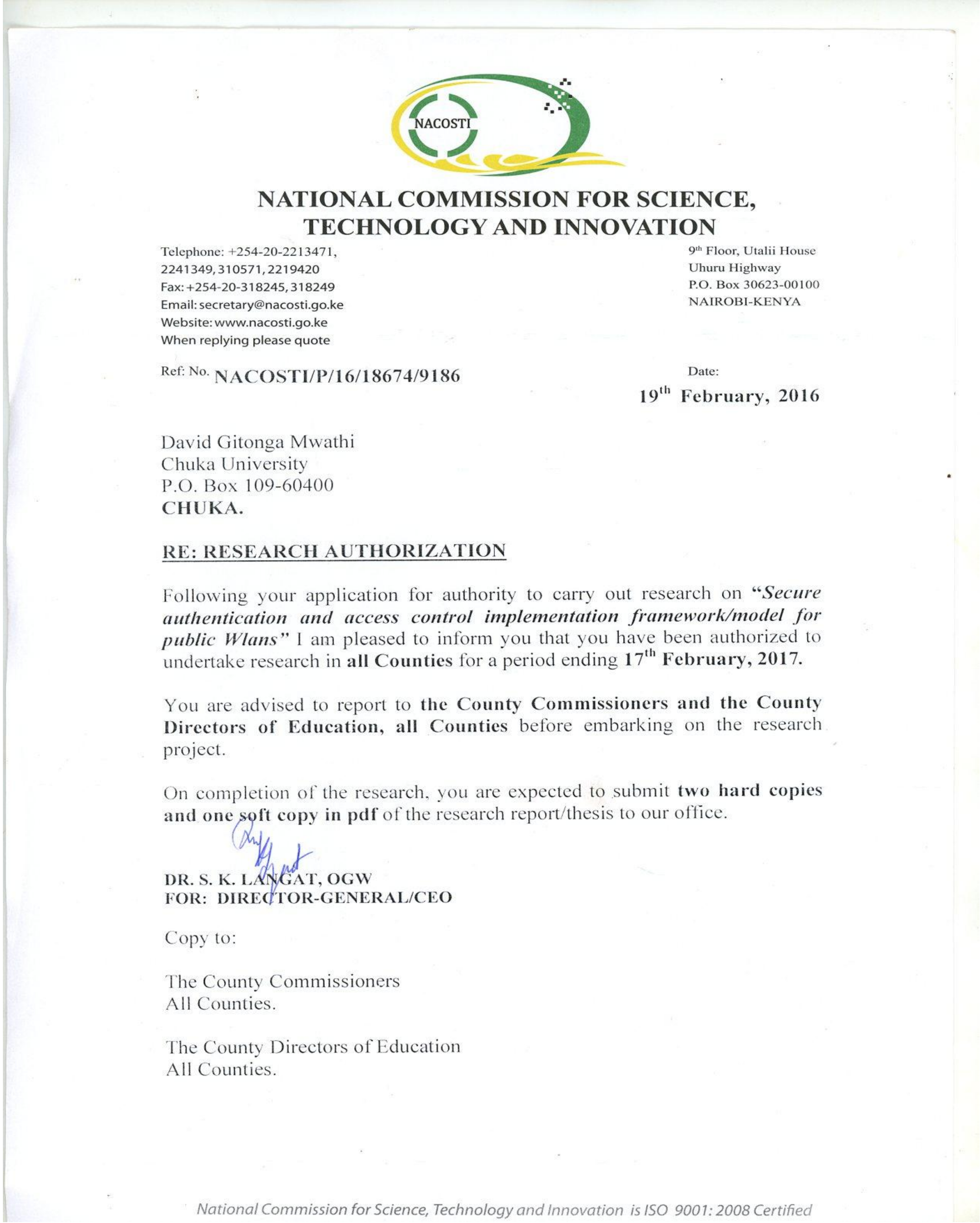
	A	B	C	D	E	F	G	H
1	UNIVERSITY	CIPHER SUITE	AUTHENTICATION CREDENTIALS	AUTHENTICATION MECHANISM	DATABASE	AUTHENTICATION SERVER	BACKEND AUTHENTICATION SYSTEMS SECURITY	WIRELESS PATH SECURITY
2	1'	TKIP	Pre-shared key	Pre-shared Key	NONE	NONE	0	1
3	2'	TKIP	Pre-shared key	Pre-shared Key	NONE	NONE	0	1
4	3'	TKIP	Server certificate-tunneled Session key from client	EAP Method With 802.1x	CENTRALIZED	RADIUS	2	2
5	4'	WEP	Pre-shared key	Pre-shared Key	NONE	NONE	0	0
6	5'	TKIP	Pre-shared key	Pre-shared Key	NONE	NONE	0	1
7	6'	WEP	Server certificate-tunneled Session key from client	EAP Method With 802.1x	CENTRALIZED	RADIUS	2	0
8	7'	TKIP	Pre-shared key	Pre-shared Key	NONE	NONE	0	1
9	8'	WEP	Pre-shared key	Pre-shared Key	NONE	NONE	0	0
10	9'	WEP	Server certificate-tunneled Session key from client	EAP Method With 8	CENTRALIZED	RADIUS	2	0
11	10'	CCMP	Server certificate-tunneled Session key from client	EAP Method With 802.1x	CENTRALIZED	RADIUS	2	3
12	11'	TKIP	Pre-shared key	Pre-shared Key	NONE	NONE	0	1
13	12'	TKIP	Pre-shared key	Pre-shared Key	NONE	NONE	0	1
14	13'	TKIP	Pre-shared key	Pre-shared Key	NONE	NONE	0	1
15	14'	TKIP	Server certificate-tunneled Session key from client	EAP Method With 802.1x	CENTRALIZED	RADIUS	2	2
16	15'	WEP	Pre-shared key	Pre-shared Key	NONE	NONE	0	0
17	16'	TKIP	Pre-shared key	Pre-shared Key	NONE	NONE	0	1



E1 DATABASE

	A	B	C	D	E	F	G	H
19	18'	WEP	Pre-shared key	Pre-shared Key	NONE	NONE	0	0
20	19'	WEP	Server certificate-tunneled Session key from client	EAP Method With 802.1x	CENTRALIZED	RADIUS	2	0
21	20'	WEP	Server certificate-tunneled Session key from client	EAP Method With 802.1x	CENTRALIZED	RADIUS	2	0
22	21'	WEP	Pre-shared key	Pre-shared Key	NONE	NONE	0	0
23	22'	WEP	Client Password	EAP Method With 802.1x	CENTRALIZED	RADIUS	1	0
24	23'	WEP	Server certificate-tunneled Session key from client	EAP Method With 802.1x	CENTRALIZED	RADIUS	2	0
25	24'	WEP	Password	EAP Method With 802.1x	CENTRALIZED	RADIUS	1	0
26	25'	TKIP	Server certificate-tunneled Session key from client	EAP Method With 8	CENTRALIZED	RADIUS	2	2
27	26'	TKIP	Server certificate-tunneled Session key from client	EAP Method With 802.1x	CENTRALIZED	RADIUS	2	2
28	27	WEP	Pre-shared key	Pre-shared Key	NONE	NONE	0	0
29	28'	CCMP	Server certificate-tunneled Session key from client	EAP Method With 802.1x	CENTRALIZED	RADIUS	2	3
30	29'	WEP	Server certificate-tunneled Session key from client	EAP Method With 802.1x	CENTRALIZED	RADIUS	2	0
31	30'	TKIP	Pre-shared key	Pre-shared Key	NONE	NONE	0	1

Appendix 12: Research authorization



NACOSTI

NATIONAL COMMISSION FOR SCIENCE, TECHNOLOGY AND INNOVATION

Telephone: +254-20-2213471,
2241349, 310571, 2219420
Fax: +254-20-318245, 318249
Email: secretary@nacosti.go.ke
Website: www.nacosti.go.ke
When replying please quote

9th Floor, Utalii House
Uhuru Highway
P.O. Box 30623-00100
NAIROBI-KENYA

Ref: No. **NACOSTI/P/16/18674/9186**

Date:
19th February, 2016

David Gitonga Mwathi
Chuka University
P.O. Box 109-60400
CHUKA.

RE: RESEARCH AUTHORIZATION

Following your application for authority to carry out research on ***"Secure authentication and access control implementation framework/model for public Wlans"*** I am pleased to inform you that you have been authorized to undertake research in **all Counties** for a period ending **17th February, 2017.**

You are advised to report to **the County Commissioners and the County Directors of Education, all Counties** before embarking on the research project.

On completion of the research, you are expected to submit **two hard copies and one soft copy in pdf** of the research report/thesis to our office.

DR. S. K. LANGAT, OGW
FOR: DIRECTOR-GENERAL/CEO

Copy to:

The County Commissioners
All Counties.

The County Directors of Education
All Counties.

National Commission for Science, Technology and Innovation is ISO 9001: 2008 Certified

Appendix 13: Recognized Universities and University Constituent Colleges in Kenya

(Source: Commission for University education website, 2013, http://www.cue.or.ke/)

S/N	ACCREDITED UNIVERSITY/UNIVERSITY COLLEGE	Date of accreditation
	Public Chartered Universities	
1	University of Nairobi	Established- 1970 Chartered- 2013
2	Moi University	Established- 1984 Chartered-2013
3	Kenyatta University	Established 1985 Chartered-2013
4	Egerton University	-Established 1987 Chartered-2013
5	Jomo Kenyatta University of Agriculture and technology	Established -1994 Chartered-2013
6	Maseno University	Established -2001 Chartered-2013
7	Masinde Muliro University of science and technology	Established -2007 Chartered-2013
8	Dedan Kimathi University of Technology	Chartered -2012
9	Chuka University	Chartered-2013
10	Technical University of Kenya	Chartered-2013
11	Technical University of Mombasa	Chartered-2013
12	Pwani University	Chartered-2013
13	Kisii University	Chartered-2013
14	University of Eldoret	Chartered-2013
15	Maasai Mara University	Chartered-2013
16	Jaramogi Oginga Odinga University of Science and Technology	Chartered-2013
17	Laikipia University	Chartered-2013

18	South Eastern Kenya University	Chartered-2013
19	Meru University of Science and Technology	Chartered-2013
20	Multimedia University of Kenya	Chartered-2013
21	University of Kabianga	Chartered-2013
22	Karatina University	Chartered-2013
	Private Chartered Universities	
23	University of Eastern Africa-Baraton	Chartered-1991
24	Catholic university of east Africa	Chartered-1992
25	Dayster university	Chartered-1994
26	Scott Christian university	Chartered-1997
27	United states international university	Chartered-1999
28	Africa Nazarene university	Chartered-2002
29	Kenya Methodist University	Chartered-2006
30	St Pauls university	Chartered-2007
31	Pan Africa Christian University	Chartered-2008
32	Strathmore University	Chartered-2008
33	Kabarak University	Chartered-2008
34	Mount Kenya University	Chartered-2011
35	Africa international university	Chartered-2011
36	Kenya highlands evangelical university	Chartered-2011
37	Great lakes university of Kisumu	Chartered-2012
38	KCA University	Chartered-2013
39	Adventist university of Africa	Chartered-2013
	Public University constituent Colleges	
40.	Murang’a university College(J.K.U.A.T)	Established-2011
41.	Machakos university college(KU)	Established -2011
42.	The co-operative university college(JKUAT)	Established -2011
43.	Embu university College(UON)	Established -2011
44.	Kirinyaga university College(JKUAT)	Established -2011
45.	Rongo University College(MU)	Established -2011

46.	Kibabii University College(MMUST)	Established -2011
47.	Garissa University College(MU)	Established -2011
48.	Taita Taveta University College	Established -2011
	Private University constituent Colleges	
49.	Hekima university College(CUEA)	Established -1993
50.	Tangaza University College(CUEA)	Established -1997
51.	Marist International university college(CUEA)	Established -2002
52.	Regina Pacis University College(CUEA)	Established -2010
53.	Uzima University College(CUEA)	Established -2012

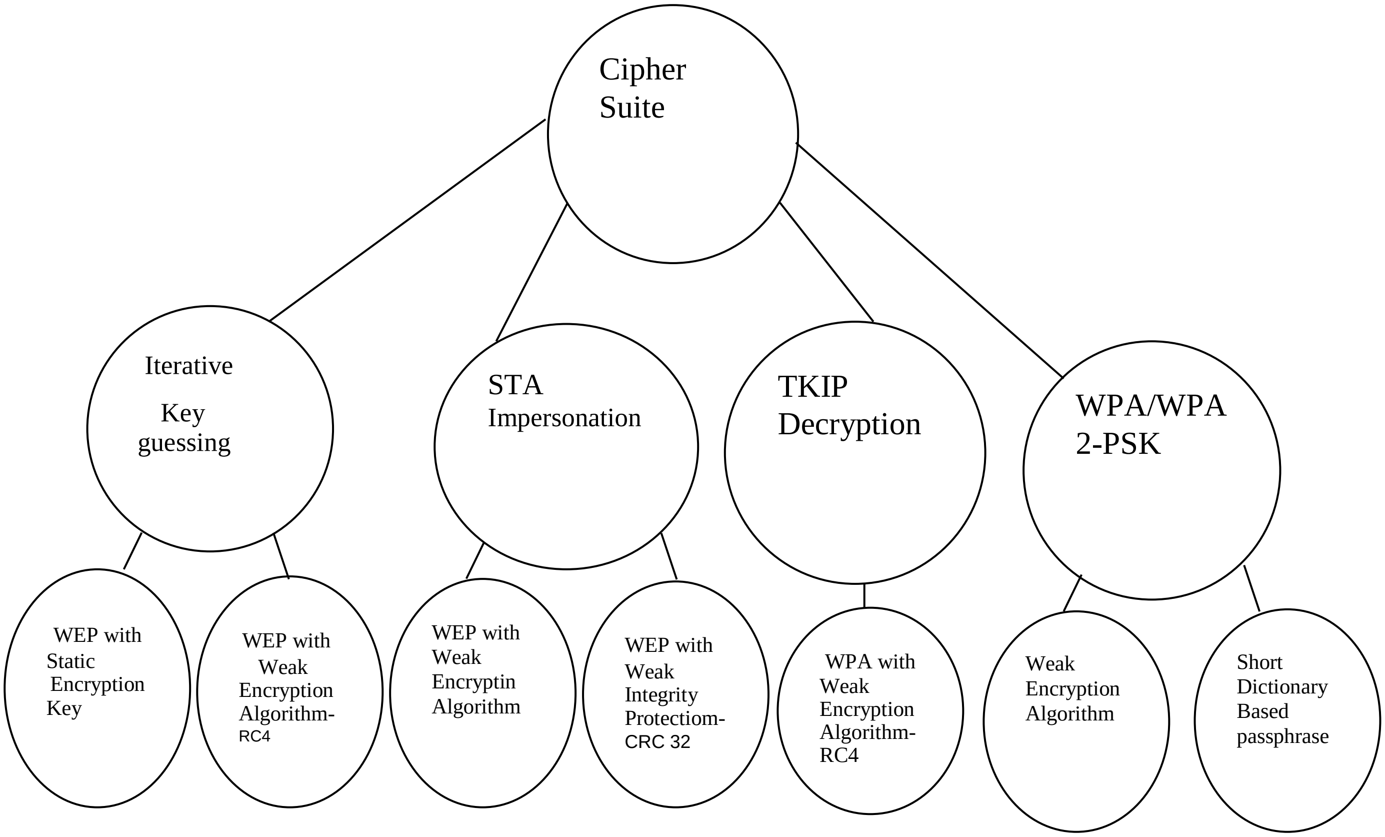
Appendix 14: Overall Staging for Universities on Networked Campus

(Kashorda & Waema, 2013)

University	**Networked Campus environment (Maximum Score 5)**
Very Large Universities	
University of Nairobi	3.8
Kenyatta University	3.8
Moi University	4.0
JKUAT	3.8
Average	**3.8**
Large Universities	
Masinde Muliro University of science and technology	3.1
Egerton	3.8
Technical University of Kenya	3.6
University of eldoret	3.0
Chuka University	2.6
Kenya Methodist University	3.7
Average	**3.3**
Medium Universities	
Maseno University	2.3
Dedan Kimathi University of Technology	3.1
Meru University of science and technology	2.9
University of Kabianga	3.3
Technical university of Mombasa	2.4
Pwani University	2.8
Laikipia University	3.4
Catholic university of eastern Africa	3.2
KCA University	3.1
Strathmore University	3.1
St Paul University	3.4

USIU	3.4
Kisii University	2.8
Average	**3.0**
Small Universities	
Maasai Mara University	3.0
Multimedia University	3.2
South Eastern University	2.3
Africa Nazarene University	2.8
Dayster University	4.0
Kabarak University	3.6
University of eastern Africa	2.8
Average	**3.1**

Appendix 15: Sample Attack Tree


Cipher Suite
Iterative Key guessing
STA Impersonation
TKIP Decryption
WPA/WPA 2-PSK
WEP with Static Encryption Key
WEP with Weak Encryption Algorithm-RC4
WEP with Weak Encryptin Algorithm
WEP with Weak Integrity Protectiom-CRC 32
WPA with Weak Encryption Algorithm-RC4
Weak Encryption Algorithm
Short Dictionary Based passphrase

Appendix 16: Raw Vulnerability Scores For WLAN Security Features and Configuration

Table 1a: Vulnerability Scores for Authentication and Access Control Mechanisms

S/N	Attack	Configuration issue/Vulnerable feature	AV	AC	PR	UI	S	C	I	A	CVSS Score
1	STA Impersonation attacks	-Use of MAC address filtering access control mechanism -MAC address spoofing -Open/Null Authentication -No Mutual Authentication	A	L	N	N	U	H	H	N	8.1 [Very High]
2	Captive Portal circumvention (Evil Twin)	-Use of captive portal authentication that is not SSL encrypted.	A	L	N	N	U	H	H	L	8.3 [Very High]
		-Allowing SSL Self signed certificates from the captive portal -Lack of Validation of SSL server certificate -Lack of validation of captive portal server name.	A	H	N	N	U	H	H	L	7.1 [High]
3	Pre-shared key recovery attacks	-Use of Pre-shared key authentication mechanism -Use of Weak Pre-shared key -Use of challenge handshake authentication protocol.	A	L	N	N	U	H	L	N	7.1 [High]
4	802.1x Identity theft	-Use of 802.1x with EAP TLS -Cleartext 802.1x	A	H	N	N	U	L	N	N	3.1 [Low]

		identity .									
5	802.1x password guessing	-Cleartext 802.1x identity -Weak session key/password	A	H	N	N	U	H	H	N	6.8 [Medium]

Table 1b: Vulnerability Scores for Authentication and Access Control Mechanisms

S/N	Attack	Configuration issue/Vulnerable feature	AV	AC	PR	UI	S	C	I	A	CVSS Score
6	AP impersonation attack	-Lack of support for mutual authentication(Access point not authenticated) -SSID Unencrypted	A	H	N	N	U	H	H	L	7.1 [High]
		-802.1x with EAP based authentication -Weak AP-AS passphrase -Not regularly changing AP-AS passphrase	A	H	N	N	U	L	N	N	3.1 [Low]
7	802.1x LEAP cracking	-Use of light weight EAP method.	A	H	N	N	U	H	N	N	5.3 [Medium]
8	802.1x EAP downgrade attack	-Use of an EAP method that does not provide replay attack resistance	A	H	N	N	U	N	L	N	3.1 [Low]
9	802.1x EAP length attacks	-lack of EAP message authentication	A	H	N	N	U	N	N	L	3.1 [Low]
10	802.1x EAP of death	-lack of EAP message authentication .	A	H	N	N	U	N	N	L	3.1 [Low]

Table 1c: Vulnerability Scores for Authentication and Access Control Mechanisms

	Attack	**Configuration issue/Vulnerable feature**	**AV**	**AC**	**PR**	**UI**	**S**	**C**	**I**	**A**	**CVSS Score**
11	802.1x EAP Start Flood	Low resources(memory and processing speed) on an accesspoint	A	H	N	N	U	N	N	L	3.1 [Low]
12	802.1x EAP Replay	- Use of an EAP method that does not provide replay attack resistance[nonce, timestamp/sequence No]	A	H	N	N	U	L	L	N	4.2 [Medium]
13	802.1x EAP failure	- Use of an EAP method that does not provide replay attack resistance[nonce, timestamp/sequence No]	A	H	N	N	U	N	L	L	4.2 [Medium]
14	Brute force attacks	-Use of PIN based WIFI protected setup for authentication -Use of pre-shared key authentication	A	L	N	N	U	H	H	N	8.1 [Very High]
15	WPA-PSK Dictionary/ PSK Cracking	Use of pre-shared key authentication	A	H	N	N	U	H	H	N	6.8 [Medium]

Table 2a: CVSS Vulnerability Scores for Authentication Credentials Based Attacks

S/N	Attack	Configuration issue/Vulnerable feature	AV	AC	PR	UI	S	C	I	A	CVSS Score
1	EAP Dictionary Attacks	Use of weak Ms-CHAP-password	A	L	N	N	U	H	H	N	8.1 [Very High]
2	WPA-PSK Dictionary / PSK Cracking	-Weak pre-shared key - Use of dictionary based passphrases.	A	H	N	N	U	H	H	N	6.8 [Medium]
3	Password based MITM attack	Use of Password/secret key as authentication credentials for an EAP method	A	H	N	N	U	H	H	N	6.8 [Medium]
4	STA Impersonation attacks	Use of MAC address as only authentication credential.	A	L	N	N	U	H	H	N	8.1 [Very High]
5	802.1x password guessing	-Cleartext 802.1x identity -Weak session key/password	A	H	N	N	U	H	H	N	6.8 [Medium]

Table 2b: CVSS Vulnerability Scores for Authentication Credentials Based Attacks

6	Brute force attacks	-Use of PIN as authentication credential -Weak pre-shared key - Use of dictionary based passphrases.	A	L	N	N	U	H	H	N	8.1 [Very High]
7	802.1x RADIUS Cracking	Weak AP-AS passphrase AS-AP passphrase that is never changed.	A	H	N	N	U	L	L	N	4.2 [Medium]
8	RADIUS certificate	Self-signed certificates.	A	L	N	N	U	H	H	N	8.1 [Very

	MITM attacks										High]
		Certificate signed by a public CA	A	L	N	N	U	H	H	N	8.1 [Very High]

Table 3a: Vulnerability Scores for Attacks on Cipher Suite

S/N	Attack	Configuration issue/Vulnerable feature	AV	AC	PR	UI	S	C	I	A	CVSS Score
1	FMS	-WEP with Weak encryption algorithm (RC4) -Use of static encryption key.	A	L	N	N	U	H	H	N	8.1 [Very High]
2	KoreK	WEP with Weak encryption algorithm(RC4)	A	L	N	N	U	H	H	N	8.1 [Very High]
3	PTW	WEP with Weak encryption algorithm(RC4)	A	L	N	N	U	H	H	N	8.1 [Very High]
4	ChopChop	WEP with Weak encryption algorithm(RC4)	A	L	N	N	U	H	H	N	8.1 [Very High]
5	Bit flipping attacks	-WEP with Weak integrity protection CRC-32 - WEP with Weak encryption algorithm(RC4)	A	L	N	N	U	H	H	N	8.1 [Very High]

Table 3b: Vulnerability Scores for Attacks on Cipher Suite

6	Iterative key guessing attacks	-WEP with static encryption key - WEP with Weak encryption algorithm(RC4)	A	L	N	N	U	H	H	N	8.1 [Very High]
7	STA Impersonation attacks	-WEP with Weak integrity algorithm -WEP with Weak confidentiality protection algorithm(RC4)	A	L	N	N	U	H	H	N	8.1 [Very High]
8	WPA/TKIP	-WPA with Weak	A	H	N	N	U	H	H	N	6.8

	Decryption attack.	encryption algorithm(RC4)									[Medium]
9	WPA-PSK Dictionary/ PSK Cracking	-WPA with Weak confidentiality algorithm	A	H	N	N	U	H	H	N	6.8 [Medium]

Table 3c: Vulnerability Scores for Attacks on Cipher Suite

10	TKIP Countermeasures	Implementing WPA/TKIP	A	H	N	N	U	H	H	L	7.1 [High]
11	WPA Hole 196 Denial of service	Implementing both WPA and WPA2 cipher suites in a WLAN -Virtual WLANs	A	H	L	N	U	L	L	N	3.7 [Low]
12	802.11 Management frame Replay attacks	-WEP with Weak integrity protection CRC-32 -Lack of support for MFP	A	L	N	N	U	H	H	N	8.1 [Very High]
13	Brute force attacks	-WEP with Weak integrity and confidentiality protection algorithm	A	L	N	N	U	H	H	N	8.1 [Very High]
		-WPA with Weak confidentiality algorithm	A	L	N	N	U	H	H	N	6.8 [Medium]
14	ARP Poisoning	Implementing both WPA and WPA2 cipher suites in a WLAN	A	H	L	N	U	N	L	L	3.7 [Low]

Table 4a: Vulnerability Scores for Client Utility Attacks

	Attack	**Configuration issue/Vulnerable feature**	**AV**	**AC**	**PR**	**UI**	**S**	**C**	**I**	**A**	**CVSS Score**
1	STA Impersonation attacks	Client utility configured for MAC address authentication	A	L	N	N	U	H	H	N	8.1 [Very High]
		Client utility lack of support for MFP	A	L	N	N	U	H	H	N	8.1 [Very High]
2	RADIUS certificate MITM attacks	Validation of server certificate and server name not enforced.	A	L	N	N	U	H	H	N	8.1 [Very High]
		Configured to allow self signed certificates.	A	L	N	N	U	H	H	N	8.1 [Very High]
		Configured to allow certificate signed by a public CA	A	L	N	N	U	H	H	N	8.1 [Very High]
		Prompting user to authorize new servers and new trusted certification authorities	A	L	N	R	U	H	H	N	7.3 [Very High]

Table 4b: Vulnerability Scores for Client Utility Attacks

3	Disassociate flooding	Client Utility Lacks support for MFP	A	H	N	N	U	H	L	H	7.1 [High]
4	De-Authentication flooding	Client Utility Lacks support for MFP	A	H	N	N	U	H	L	H	7.1 [High]
5	802.11 Management frame Replay attacks	Client Utility lacks Support for MFP	A	L	N	N	U	H	H	N	8.1 [Very High]
		MFP set to optional	A	L	N	N	U	H	H	N	8.1 [Very High]
6	Security level rollback attack(TSN)	Client utility Supports both Pre-RSNA and RSNA.	A	H	N	N	U	H	H	H	7.5 [High]

Table 4c: Vulnerability Scores for Client Utility Attacks

7	RSN IE poisoning/spoofing	-Lack of support for MFP -Unnecessary message exchanges between the RSN IE negotiation and confirmation.	A	H	N	N	U	H	H	H	7.5 [High]
8	AP impersonation attack	Validation of server certificate and server name not enforced	A	L	N	N	U	H	H	N	8.1 [Very High]
		Configured to allow self signed certificates.	A	L	N	N	U	H	H	N	8.1 [Very High]
		Configured to allow certificate signed by a public CA.	A	L	N	N	U	H	H	N	8.1 [Very High]
		Prompting user to authorize new servers and new trusted certification authorities	A	L	N	R	U	H	H	N	7.3 [Very High]

Table 5: Vulnerability Scores for Client Driver Attacks

	Attack	Configuration issue/Vulnerable feature	AV	AC	PR	UI	S	C	I	A	CVSS Score
1	STA Impersonation attacks	Lacks of driver support or optional driver support for MFP	A	L	N	N	U	H	H	N	8.1 [Very High]
2	Disassociate flooding	Lack of or optional support for MFP	A	H	N	N	U	H	L	H	7.1 [High]
3	De-Authentication flooding	Lack of or optional support for MFP	A	H	N	N	U	H	L	H	7.1 [High]

4	Driver finger printing attacks	Driver not set to a configurable scanning approach and instead set to a specific scanning approach.	A	H	N	N	U	H	N	N	5.3 [Medium]
5	Security level rollback attack(TSN)	-Client driver Supports both Pre-RSNA and RSNA. -Lack of or optional support for MFP	A	H	N	N	U	H	H	H	7.5 [High]

Table 6a: Vulnerability Scores for Access Point Utility

S/N	Attack	Configuration issue/Vulnerable feature	AV	AC	PR	UI	S	C	I	A	CVSS Score
1	STA Impersonation attacks	Access Point firmware Configured to support MAC address filtering	A	L	N	N	U	H	H	N	8.1 [Very High]
		Access point firmware is configured not to enforce MFP.	A	L	N	N	U	H	H	N	8.1 [Very High]
		Pre-RSN enabled on the accesspoint firmware.	A	L	N	N	U	H	H	N	8.1 [Very High]
2	Disassociate flooding	Access point firmware is configured not to enforce MFP.	A	H	N	N	U	H	L	H	7.1 [High]
		Accesspoint firmware MFP set to optional	A	H	N	N	U	H	L	H	7.1 [High]
3	Authentication flooding	Low memory & processor capability of Accesspoints	A	L	N	N	U	H	N	H	8.1 [Very High]
		-Broadcasting SSID	A	L	N	N	U	H	N	H	8.1 [Very High]
4	De-Authentication	Access point firmware is	A	H	N	N	U	H	L	H	7.1 [High]

	flooding	configured not to enforce MFP.								
		Accesspoint firmware MFP set to optional	A	H	N	N	U	H	L	H	7.1 [High]

Table 6b: Vulnerability Scores for Accesspoint Utility

5	Association Flooding	Low memory & processor capability of Accesspoints Memory and processor resources exhausted	A	H	N	N	U	H	L	H	7.1 [High]
		AP configured not to adopt a separate identifier counter for each association causing Counter space exhaustion.	A	L	N	N	U	H	L	H	8.3 [High]
6	Distributed flooding	Low memory & processor capability of Accesspoints	A	L	N	N	U	H	L	H	8.3 [High]
		-Broadcasting SSID -AP configured not to adopt a separate identifier counter for each association	A	L	N	N	U	H	L	H	8.3 [High]
7	Probe request flooding	SSID Unencrypted	A	L	N	N	U	H	L	H	8.3 [High]
8	802.11 Management frame Replay attacks	Access point firmware is configured not to enforce MFP.	A	L	N	N	U	H	H	N	8.1 [Very High]
		-Access Point firmware MFP set to optional	A	L	N	N	U	H	H	N	8.1 [Very High]

9	Security level rollback attack(TSN)	-Client utility Supports both Pre-RSNA and RSNA. -Management frame unencrypted.	A	H	N	N	U	H	H	H	7.5 [High]

Table 7: Vulnerability Scores for Authentication Server Based Attacks

S/N	**Attack**	**Configuration issue/Vulnerable feature**	**AV**	**AC**	**PR**	**UI**	**S**	**C**	**I**	**A**	**CVSS Score**
1	Authentication flooding	Authentication server integrated in access point	A	L	N	N	U	H	N	H	8.1 [Very High]
2	802.1x RADIUS Cracking	-Weak access point-authentication server passphrase -Not regularly changing Passphrase	A	H	N	N	U	L	L	N	4.2 [Medium]
3	RADIUS certificate MITM attacks	Mutual authentication not supported on RADIUS server.	A	L	N	N	U	H	H	N	8.1 [Very High]
		Using RADIUS Certificate signed by public CA	A	L	N	N	U	H	H	N	8.1 [Very High]
		Server configured to use self-signed certificates when authenticating to client	A	L	N	N	U	H	H	N	8.1 [Very High]
4	802.1x EAP length attacks	-Lack of EAP message authentication	A	H	N	N	U	N	N	L	3.1 [Low]
5	802.1x EAP of death	-Lack of EAP message authentication	A	H	N	N	U	N	N	L	3.1 [Low]

Table 8: Vulnerability Scores for Attacks on User Database System.

S/N	Attack	Configuration issue/Vulnerable feature	AV	AC	PR	UI	S	C	I	A	CVSS SCORE
1	Database server DOS	-Centralized user database.	A	L	N	N	U	H	N	H	8.1 [Very High]
		-User Database integrated in access point	A	L	N	N	U	H	N	H	8.1 [Very High]
2	Distributed flooding	User Database integrated in access point	A	L	N	N	U	H	N	H	8.1 [Very High]
3	Authentication flooding	Unmonitored automated authentication requests	A	L	N	N	U	H	N	H	8.1 [Very High]
4	Injection attacks	Unmonitored automated authentication requests	A	L	N	N	U	N	H	H	8.1 [Very High]