Strathmore University
SU+ @ Strathmore University Library

Electronic Theses and Dissertations

2016

Security risks mitigation in session initiation protocol based VoIP networks implementation using MPLS

Kamuti, F. G.
Faculty of Information Technology (FIT)
Strathmore University

Follow this and additional works at: https://su-plus.strathmore.edu/handle/11071/2474

Recommended Citation

Kamuti, F. G. (2016). *Security risks mitigation in session initiation protocol based VoIP networks implementation using MPLS* (Thesis). Strathmore University. Retrieved from http://su-plus.strathmore.edu/handle/11071/4847

This Thesis - Open Access is brought to you for free and open access by DSpace @Strathmore University. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of DSpace @Strathmore University. For more information, please contact librarian@strathmore.edu

Security Risks Mitigation in Session Initiation Protocol Based VoIP Networks Implementation Using MPLS

FARIDA GAKII KAMUTI

Masters of Science in Computer Based Information Systems

2016

Security Risks Mitigation in Session Initiation Protocol Based VoIP Networks Implementation Using MPLS

Farida Gakii Kamuti

072501

Submitted in partial fulfillment of the requirements for the Degree of Masters of Science in Computer-based Information Systems at Strathmore University

Faculty of Information Technology
Strathmore University
Nairobi, Kenya

June, 2016

This thesis is available for Library use on the understanding that it is copyright material and that no quotation from the thesis may be published without proper acknowledgement.

DECLARATION

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

© No part of this thesis may be reproduced without the permission of the author and Strathmore University.

Name: Farida Gakii Kamuti

Signature:……...……..

Date:……..……

Approval

The thesis of Farida Gakii Kamuti was reviewed and approved by the following:

Dr Vincent Omwenga

Faculty of Information Technology

Strathmore University

Dr. Joseph Orero

Dean of Faculty of Information Technology

Strathmore University

Professor Ruth Kiraka

Dean, School of Graduate Studies

Strathmore University

ABSTRACT

VoIP is described as, “transfer of voice (and associated services) in digital form in discrete data packets using Internet Protocol (IP) over some or the entire communication route”. SIP on the other hand is a signaling protocol used to initiate interactive communication between end users. SIP-based VoIP therefore is the use of SIP as the signaling protocol during VoIP implementation. SIP has become the predominant protocol used in the implementation of VoIP services in organization; however the protocol has no inbuilt security measures in place. It is therefore very important to come up with a proper security solution that can ensure that SIP-based VoIP networks are fully secured from exiting security risks so as organizations information security (confidentiality, integrity and availability) is achieved at all times.

The purpose of this research was to analyze security risks that face organizations using SIP-based VoIP, analyze existing security models used and evaluate how MPLS can be effectively used in securing Sip-based VoIP networks. Through analyzing existing architectures used in securing SIP-based VoIP networks and collection of data, a security model was proposed with the aim of ensuring an all rounded security approach is taken during implementation of a secure SIP-based VoIP network.

The research used an applied research method as it aimed at mitigating security risks faced on the SIP-based VoIP network. To come up with an all rounded solution, online questionnaires were used with structured questions which aimed at getting a deeper insight on the current state of SIP-based VoIP networks and the organizations’ security. This greatly influenced in the development of the proposed SIP-based VoIP security model.

Research results showed that organizations have greatly neglected the security aspect when it comes to implementation of a SIP-based VoIP network. It also showed that through use of the proposed security model, organizations can better plan and secure their voice network not only on the technology aspect but also on the user aspect. Through the proposed security model, this research sets a platform on which future research can fully incorporate quality of service in proposed security model. In addition further research is highly recommended as security is an ongoing process as new security risks continually emerge.

DEDICATION

This work is dedicated to my family for their unending love and support. I also dedicate it to those who value and appreciate education.

ACKNOWLEDGEMENT

First and foremost, I would like to thank my supervisor, Dr. Vincent Omwenga for the invaluable guidance and advice in doing and writing this project. He inspired me greatly, his willingness to motivate me contributed tremendously to the project. I also would like to thank him for showing me some examples related to my project's topic. I would also like to thank God for good health and grace experienced during the learning period. Finally gratitude goes to my family and friends for their wonderful support and encouragement throughout the learning period.

ACRONYMS/ABBREVIATIONS

ATM – Asynchronous Transfer Mode

CE - Customer Edge

DHCP - Dynamic Host Configuration Protocol

DNS - Domain Name Server

DoS - Denial of Service

HTTP - Hyper Text Transfer Protocol

ICT- Information Communication and Technology

IP – Internet Protocol

IPS - Intrusion Prevention System

ISP- Internet Service Provider

IT - Information Technology

LAN- Local Area Network

MAC - Media Access Control

MGCP - Media Gateway Control Protocol

MPLS - Multi- protocol label switching

PBX -Public Branch exchanges

PE - Provider Edge

PSTN - public switched telephone networks

QoS - Quality of Service

ROI - Return on Investment

SCTP - Stream Control Transmission Protocol

SIP - Session Initiation Protocol

SMTP- Simple Mail Transfer Protocol

SRTP - Secure Real-time Transport Protocol

SSL - Secure Sockets Layer

TAM - Technology Acceptance Model

TCP- Transmission Control protocol

TEA- Technology Acceptance Model

TRA - Theory of Reasonable Action

RTP - Real-time Transport Protocol

UA -User Agents

UAC - User Agent Client

UAS - User Agent Server

UDP - User Datagram Protocol

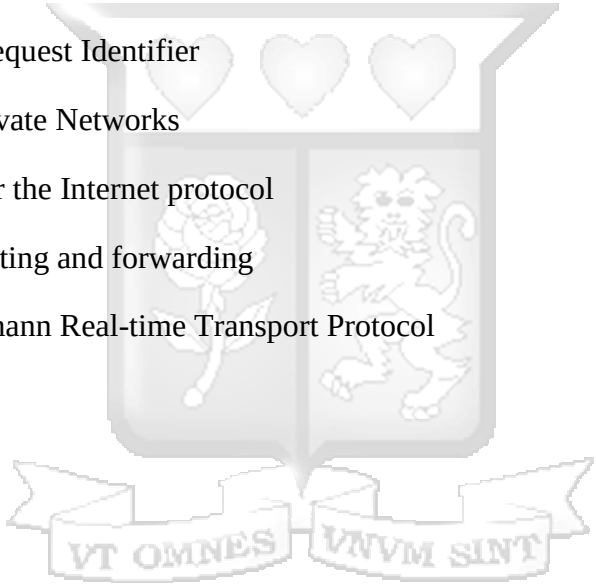
URI - Uniform Request Identifier

VPN - Virtual Private Networks

VoIP - Voice over the Internet protocol

VRF - Virtual routing and forwarding

ZRTP - Zimmermann Real-time Transport Protocol



DEFINATION OF TERMS

Return on Investment	Financial gain expressed as a percentage of funds invested to generate that gain.
Multi-Protocol Label Switching	A protocol that provides a mechanism for forwarding packets for any network protocol.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER ONE: INTRODUCTION

1.1 Introduction

This chapter gives a background of the study and describes the mitigation of security risks in SIP-based VoIP networks. It discusses security risks and ways of mitigating those risks. The problem statement, general and specific objectives of the study, research questions, limitations of the study, operational definition of terms and justification of the study have been stated and discussed in this chapter.

1.2 Background of the Study

Due to the rise in use of applications on the packet switched platform especially the internet, a parallel rise in malware and cyber-attacks not previously experienced in the analogues platform has been noted. This has made it vital for measures and controls to be put in place to secure internet consumers and organizations from such attacks.

There has been a spread in use of information communications technologies leading to countries especially developing ones, realizing the importance of implementing efficient telecommunication networks for the development of their economy (Ogunsola, 2005; World Economic Forum, 2012). Since the emergence of the packet-switched networks and their growing acceptance, telecommunication providers are coming up with new ways of combining both data and communication on an all IP network infrastructures (Ehlert, 2009).

As a result of growing acceptance and use of IP packet switched networks; there has been an increase in the use and invention for new IP-based multimedia applications in the global communication market (World Economic Forum, 2012). These applications include interactive TV, network gaming, Voice over IP (VoIP), multiparty conferencing, PC clients, video on demand and instant messaging (Pavlovski, 2007; Jaber et al. 2012).

The use and deployment of Voice over the Internet protocol (VoIP) is on the rise. This has resulted to a rise of a third dimension in voice communication; public switched telephone networks (PSTN) and cellular networks accounting for the other two (Dantu et al. 2009). VoIP can be used to call any PSTN telephone or mobile phone anywhere in the world through the use of the internet. In order for VoIP to fully function it incorporates use of

signaling protocols such as Session Initiation Protocol (SIP) to manage, terminate and initiate calls.

SIP as a protocol has been greatly affected by security risks leading to attacks such as billing, registration and denial of service (Dos) attacks. SIP as a VoIP protocol is not designed with security as a primary concern (Dantu et al. 2009). Despite the latest versions having incorporated some security features, it is still not fully secure. Due to this, there is need for incorporation of more security measures with the aim of mitigating existing security risks further.

MPLS (Multi- protocol label switching) is the security measure proposed in tackling Sip-based security risks in this dissertation due to it is ability to not only enhance SIP-based VoIP security but at the same time ensure quality of service (Qos).

1.2.1 Computer Networks

A computer network is the interconnection of computers and peripherals through various media which could be through wires/fiber or wireless. Networking started after the invention of the first commercial modem, Data phone by AT&T and the ARPANET back in the 60^{s} (Mowery & Simcoe, 1998).

As the technology advanced, the ability to interconnect more devices also advanced for example the ARPANET, the first network had only four nodes as compared to now in the 21st Century we have the ability to network the whole world through devices like televisions, cell phones even home appliances. With this level of interconnection, various needs or applications to use on this network came up, like the ease of communication through electronic mail (email) as compared to snail mail, then information sharing through websites to shopping online.

1.2.2 VoIP networks

VoIP is described as, “transfer of voice (and associated services) in digital form in discrete data packets using Internet Protocol (IP) over some or the entire communication route “(ITU, 2007).VoIP is not only limited to voice communication, it can also be used in the making of video calls (video conferencing) and data conferencing. It is an important technology as it brings forth significant changes in the way people communicate as; in

addition to use of telephones for real-time communication one can use IP-based phones, desktop computers (softphones), videophones, mobile phones and wireless phones (Packetizer inc, 2013).

As in figure 1.1, VoIP is able to use different transmission technologies to transmit data. VoIP calls can be initiated or received on a wireless networks, mobile networks, cable networks and PSTN networks through the use of appropriate network architectures and systems. This can be through the use of devices such as modems; VoIP client applications on mobile phones, VoIP gateways, a PBX, IP based phones, managed IP PBX and even computers. Through its usability on different networks and devices, VoIP is able to achieve a convergence of different networks.

Figure 1.1: Hybrid VoIP network
Source: (TELES, 2009)

1.2.3 SIP- based VoIP networks

SIP-based VoIP has evolved as the de-facto standard for voice communication (Aziz et al. 2014). Due to this, support of open SIP-based interfaces is becoming increasingly important for IP-based Public Branch exchanges (PBXs) in organizations.

SIP is a text-based lightweight protocol similar to (SMTP) Simple Mail Transfer Protocol and Hyper Text Transfer Protocol (HTTP) (Ubiquity Software Corporation Limited, 2003). It is used to initiate interactive communication between end users. As a signaling protocol it creates, modifies and terminates sessions between one or more participants using signaling messages (Microsoft Corporation, 2015; Rahangdale, Tijare, & Sawalkar, 2014). These sessions include internet media conferencing, multimedia distribution and internet telephone calls.

Despite being a growing technology, it has been identified as the biggest security threat facing firms and results to significant loss of money, through illegal or unauthorized use (Serianu Limited, 2014). In order to devise countermeasures that are effective, it is imperative to know how these attacks are executed in reality.

As VoIP systems become ever more prevalent and risk grows security professionals need to make sure they are undertaking more precautions to prevent security breaches (Shawn et al, 2005). The study seeks to incorporate use of MPLS in mitigation of SIP-based VoIP security risks to enhance security on VoIP networks in organizations

1.3 Problem statement

Organizations are increasingly adopting VoIP services as a cost cutting measure more so in undertaking international calls, especially for multinational organizations. These services are mostly offered using SIP; as it is the de-facto standard for voice communication (Rosenberg, et. al, 2013; Cisco, 2014). This however opens up the organization to VoIP SIP-based networks security risks. In Kenya, VoIP security risks have been identified as the biggest security threat facing firms resulting to loss of money, through illegal or unauthorized use (Serianu Limited, 2014).

One of the essential issues in VoIP security is protecting the signaling messages (SIP messages) being exchanged between VoIP infrastructures (Zhang, 2009). The protection of signaling includes integrity and confidentiality of signaling messages, as well as availability and confidentiality of signaling services (Lazzez, 2013). As stated in the background, SIP as a VoIP protocol is not designed with security as a primary concern (Dantu et al. 2009). Despite the latest versions having incorporated some security features, it is still not fully secure.

If an organization uses SIP-based VoIP over the Internet, security risks on the network, such as billing attacks and DOS attacks rise considerably. A study by Cisco (2014) indicated that the internet makes the VoIP network vulnerable to malicious attackers as it is a public network. The security risks can be greatly mitigated if the SIP-based VoIP network is migrated or implemented on a managed private connection through use of networks such as MPLS on which security and Quality of Service (QoS) can be better guaranteed, as opposed to the Internet where they cannot be guaranteed (Cisco, 2014).

1.4 Research Objective

The main objective of this study is to analyze security risks mitigation in SIP-based VoIP networks and develop a MPLS model for SIP-based VoIP networks. Specific objective of the study were:

1. To analyze security risks faced by organizations using SIP-based VoIP networks.
2. To analyze existing security mitigation models for organizations using SIP-based VoIP networks.
3. To analyze effectiveness of MPLS in mitigating security risks on SIP-based VoIP networks.
4. To develop a security model for organizations using SIP-based VoIP networks.
5. To validate the proposed security model using contextual analysis.

1.5 Research Questions

1. Which security risks are faced by organizations using SIP-based VoIP networks?
2. What are the existing security mitigation models for organizations using SIP-based VoIP networks?
3. How effective is MPLS in mitigating security risks on SIP-based VoIP networks?
4. How will the proposed security model for organizations using SIP-based VoIP networks be developed?
5. How does the proposed security model contextually incorporate SIP-based VoIP security concepts for an organization?

VT OMNES VNVM SINT

1.6 Justification of the Study

The study will benefit information technology (IT) security personnel and service providers identify various security risks faced on VoIP networks, their effects and how they can be mitigated. VoIP service providers can use this information to implement better secured networks in organizations they provide SIP-based VoIP service to. The study findings will help the government, through the Ministry of Information Communications and technology formulate more effective security policies that better suit the ICT environment with the aim of mitigating security risks especially in VoIP networks.

The pool of knowledge on VoIP, especially SIP-Based, is limited. This research will extend the existing knowledge on SIP-based VoIP networks security risks, preparedness of firms against this risks and how they can be mitigated. Thus the study will be useful to researchers and scholars in addressing any gaps that might arise from the findings thereof and in undertaking comprehensive research.

1.7 Scope of the Study

The study mainly focused on SIP signaling security risks in Sip-based VoIP networks. This study targeted the IT staff in organizations using SIP-based VoIP. It covered organizations that have adopted SIP-based VoIP networks as their Voice communication platform and the VoIP service providers in Nairobi County, Kenya. The variables under the study included; SIP-based VoIP security risks awareness level, type's security risks, and mitigation measures to those threats. The focus was informed by background information on the VoIP networks vulnerabilities and some of the organizations having been attacked.

1.8 Limitations

Organizations were suspicious of how exactly the information will be used and, if in any way it may land in the hands of their competitors. Some organizations saw this as strategic information that might be used by their competition and therefore were unwilling to share the information. This was mitigated by developing a generic questionnaire and assurance that no organization's name will appear in the final report. From the onset clarity was provided that no customer information will be required for this research. Benefits were also

articulated since the individual organizations can use the findings to secure, improve or make some changes in the adoption of VoIP technology.

Availability of the respondents given their busy working schedules was also a limitation. This was mitigated by availing the questionnaire on-line in a portal where respondents gave feedback at their convenience and structuring the questionnaire in a brief, targeted and specific way.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

Literature has been reviewed in three focus areas: theoretical review, conceptual framework, and empirical review of previous studies. Organizations need to analyze security risks on their SIP-based VoIP networks and protect their Voice traffic from those risks while at the same time ensuring appropriate security awareness measure have been employed in the organization.

This chapter looks into various theories needed during adoption and assimilation of a technology in an organization. It also looks into SIP-based VoIP security risks from a technological and organization perspective and the existing security models used in the mitigation of those risks. The chapter finally analyses the MPLS architecture and proposes a SIP-based VoIP security model based on MPLS aimed at ensuring voice service availability, integrity and confidentiality.

2.2 Overview of SIP-based VoIP networks

VoIP has been the driver for IP-based communications due to the 'always on' and 'Everything over IP' (Suruhanjaya Komunikasi dan Multimedia Malaysia, 2007) era where a user has the flexibility to change his/her availability or presence. This leaves the user with the flexibility of changing their presence on the application to away, online or invisible among others at will and need. The emergence of IP-enabled devices like the smart mobile phones is fueling the growth of IP telephony exponentially bring about new IP telephony operators like Goggle Hangouts and Viber to the traditional VoIP infrastructure operators. This study will mainly focus on the traditional VoIP networks.

SIP is currently the main preferred signaling protocol used by VoIP services (Jaber et al. 2012). As a signaling protocol it creates, modifies and terminates multimedia sessions between one or more participants (Microsoft Corporation, 2015; Rahangdale, Tijare, & Sawalkar, 2014). These sessions include internet media conferencing, multimedia distribution and internet telephone calls.

2.2.1 VoIP Architecture

VoIP infrastructure inherits and uses several protocols on the internet stack architecture in delivery of its services. At network level it uses the Internet Protocol (IP) while at the transport level, it makes use of process to process delivery protocols such as Transmission Control protocol TCP, UDP User Datagram Protocol or Stream Control Transmission Protocol (SCTP) protocols respectively (Zafar & Gill , 2008; Wulff & Hunt, 2010). In addition; at the application level, it not only exploits well known protocols like DNS (Domain Name Server), and DHCP (Dynamic Host Configuration Protocol); but also dedicated ones that are used to handle sessions and transport media data.

As illustrated in Figure 2.1 below, the above protocols can be categorized under the following groups:

1. Signaling Protocols used in handling a voice or multimedia sessions between two or more VoIP network entities. These protocols include: H.3232, SIP and Media Gateway Control Protocol (MGCP).
2. Utility protocols used in offering additional services such as name address resolution done by the DNS and IP provisioning done using DHCP .
3. Media protocols used in transmission of media data among entities during a session. They include; Real-time Transport Protocol (RTP), Secure Real-time Transport Protocol (SRTP) and Zimmermann Real-time Transport Protocol (ZRTP).

Table 2.1: VoIP protocol stack

<table>
<tr><td rowspan="4">Internet Stack</td><td rowspan="2">Application</td><td rowspan="4">VoIP Stack</td><td colspan="4">Signaling</td><td></td><td>Media</td></tr>
<tr><td>H.323</td><td>SIP</td><td>MGCP</td><td>OTHER</td><td></td><td>RTP</td></tr>
<tr><td>UDP/TCP</td><td colspan="6" rowspan="3">Internet Stack protocols</td></tr>
<tr><td>IP</td></tr>
<tr><td>Data Link</td></tr>
</table>

Source: (Geneiatakis, Lambrinoudakis, & Kambourakis, 2008)

2.2.2 SIP Architecture

SIP handles its functions on a SIP-based VoIP through use of various components, protocol and methods. The crucial components are the devices used during initiation and setup of a call between users that allows them to communicate with each other. A number of protocols, discussed in section 2.2.1 are used to carrying the voice between SIP enabled devices.

Since SIP is a text-based protocol, it makes it easy to manipulate SIP messages leading to various security risks. SIP-based architecture has mainly focused on providing new, dynamic SIP services and capabilities instead of focusing on more efficient security features and policies making SIP-based VoIP networks are susceptible to security risks and attacks (Ferdous, 2014).

I. SIP Components

SIP protocol requires the components highlighted below during the creation of a session. They include (Ferdous, 2014);

a) **User Agents (UA):** This is an end-point that creates or receives SIP messages, which in turn are used in managing a SIP session. It can have a client and server element, the User Agent Client (UAC) responsible for creation of SIP requests while the User Agent Server (UAS) is responsible for processing and responding to each request generated by the UAC. The UAC is responsible for creating requests and the UAS processes and responds to each request generated by a UAC.

b) **SIP Servers:** They are used in facilitating UA's establish SIP sessions and in performing other functions such as name resolution and establishing user location. They include;

1. **Proxy Server**- It is an intercessor component as it can acts as both a server and a client for the purpose of making requests on behalf of other clients. It primarily executes the part of routing, were it ensures a request is forwarded to another server closer to the targeted UA.
2. **Redirect Server** -The redirect server is used during session initiation to determine the address of the called device and it informs the caller's UA about the next hop server. The caller's UA then contacts the next hop server directly.
3. **Location Server**- It is used by a SIP proxy or redirect server in obtaining of information on the possible location of a callee. For this purpose, it maintains a database of SIP-address/IP address mapping.
4. **Registrar Server**- It contains database containing locations and users preferences as indicated by the User Agents. It receives SIP registration requests and binds the information to a SIP address and associated IP address of the registering device.

II. SIP Methods

They are requests from a client to a server or a response from a server to a client. Each request uses a method such as INVITE or ACK used to invoke a certain operation on the server. For each reply, a status code is stated to indicate the acceptance, rejection or redirection of a request. There are seven basic methods in core SIP, as shown in table 2.1 below;

Table 2.2: Seven basic methods in core SIP

METHODS	USE
REGISTER	Used by a UA to register to a SIP server
INVITE	Used when by a UA to initiate a SIP session.
CANCEL	Used to terminate a request that is pending, e.g. if a user gets tired of waiting for the targeted user to accept the INVITE.
ACK (ACKnowledgement)	Confirms successful completion of a SIP request or transaction.
BYE	Used in termination of a SIP session between UA's.
OPTIONS	Used by UA's when querying capabilities of UAs and proxies
NOTIFY	Updates current information of a UA and notifies on the presence of a UA such as whether they are busy, online, offline.

Source: (Toivanen, 2006)

III. SIP call initiation

Callers and callees are recognized via their addresses in SIP systems. The users are recognized through their SIP URL that is; sip:username@host.site. To initiate a call, the UAC either sends a SIP signaling request to a SIP proxy server or UAS or it can send it to the IP address and port matching to the Uniform Request Identifier (URI). Once the user request or URI, has been resolved, the client can send requests to SIP server. The requests are either sent through reliable TCP or unreliable UDP.

For a SIP call to be initiated between a caller and the receiver a three way handshake has to take place; if Alice wants to talk to Tim, an INVITE method is generated by Alice's UA, and sent to her local SIP proxy, upon dialing Tim's number. The INVITE method is then forwarded to the SIP proxy serving Tim via IP. Once the INVITE is received by Tim's UA, an OK message is sent to Alice upon receiving of the call by Tim, after which an ACK message is sent to Tim to signify that the session has been fully established. Once the call is terminate, a CANCEL message is sent to terminate the call. This call session is documented on the SIP proxies and is used in the service usage evaluation and billing process by the service provider (Thermos & Takanen, 2008). Figure 2.1below illustrates the above.

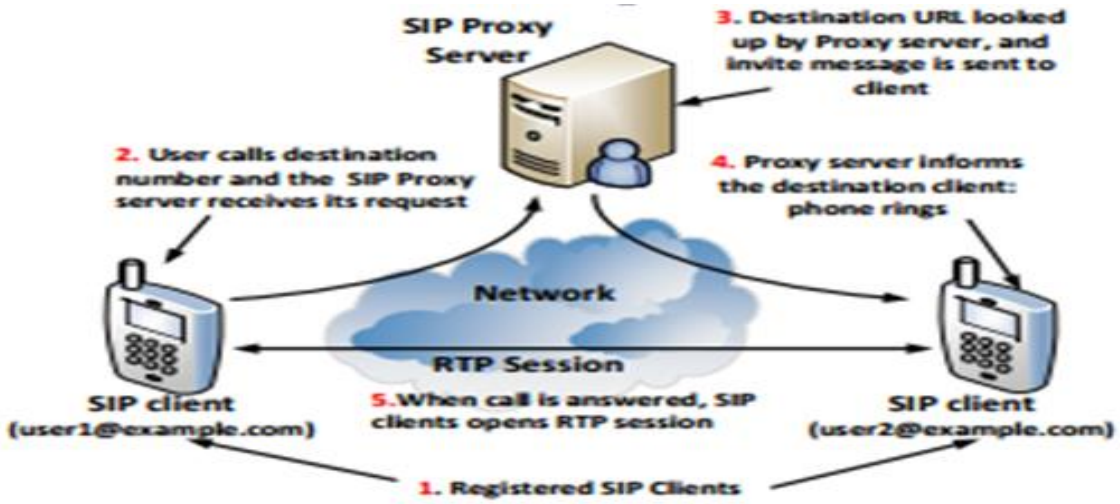


Figure 2.1: Basic flow of a SIP call
Source: (Jallow, Hwang, Nikoukar, & Liem, 2014)

2.2.3 Features of SIP-based VoIP networks

Since SIP is a text-based protocol it allows easy execution in object oriented programming languages such as Java and Perl while at the same time enabling easy debugging (Ferdous, 2014). The test-based aspect also ensures flexibility and extensibility of SIP-based VoIP networks. SIP is designed to meet the basic signaling requirements with the aim of simplifying SIP protocol as much as possible (Wulff & Hunt, 2010). Some of the parameters used in the establishment and negotiation of media stream during a call are encapsulated within the SIP message body. This in the long run makes SIP-based VoIP networks able to initiate and set up calls much faster which is critical in achieving high Quality of Service (Qos).

SIP-based VoIP is Independent of the transport layer protocols and can either use TCP or UDP. However by default SIP uses UDP due to delays experienced in the TCP. By using UDP the timing of messages and their retransmission can be controlled by the application-layer (Yuan, 2002). The destination can be located via multicast, without the need to specify a different TCP channel for each signaling connection. A parallel search can be done on a SIP-based VoIP networks as SIP servers have the capability of splitting or "forking" incoming calls so as several extensions can be ring at once and first extension to answer takes the call.

2.3 Factors Influencing Security on SIP-based VoIP network

Security is considered an essential part in every communication network because conversations within users or employees require privacy, integrity, security, and confidentiality. The security risks in SIP-based VoIP encompass not only the faults inherent inside the SIP Protocol, but also the operating systems, applications, and other protocols. Security risks are defined as, "something or someone likely to cause danger or difficulty" (Jones et al. 2013). The complexity of SIP-based VoIP creates a high number of security risks that affect the three major areas of information security that is; confidentiality, availability and integrity (Albers et al. 2005). Although this study acknowledges that most security risks cut across different sections of a network, it has mainly focused on organizational, structural security lapses and SIP protocol security flaws.

2.3.1 Security flaws in SIP as a SIP-based VoIP protocol

Internet security and threat reports show that the SIP-based VoIP attack surface is growing (Center, 2008; TESPOK, 2014). This is both due to more people using SIP-based VoIP services, as well as more malicious hackers and criminals focusing on attacking these networks. Attackers mainly target small companies due to their lax in security measures and their purchase of off-the-shelf systems such as the PBX which they have implemented by inexperienced persons making it prone to security risks (Capacity business briefing, 2013).

Due to the inherent nature of SIP where encryption is rarely used as it is not configured by default, a third party can harvest the credentials of a user when the user is communicating with their registrar. This third party can then make expensive long distance calls or even configure a gateway with the stolen user details and sell minutes in bulk to expensive routes (Capacity business briefing, 2013). SIP security risks include;

Identity theft- A hacker can also steal the identity of the user and obtain significant information regarding, such as, financial loans that are often tied to a specific phone number (Enterprise Risk Management, 2011).

Eavesdropping- It mainly comprises the interception of a conversation between persons that is usually private and confidential. Once an attacker has identified vulnerabilities on SIP protocol, he or she can use them to capture information exchanged by two unsuspecting

individuals during a SIP session (Thermos & Takanen, 2008). SIP-based networks are vulnerable to eavesdropping as they are easy to access due to their use of IP-based networks.

Message tampering -Occurs when an attackers intercepts and alters SIP messages exchanged between SIP devices (Asghar & Azmi, 2010). It can occur due to registration hijacking and proxy impersonation; as the attacker is logged into a device that legitimately processes SIP messages (Arafat, Ahmed, & Sobhan, 2013).

Replay – It is a security risk that targets SIP traffic. The attacker captures SIP traffic and resends it after a period of time. It can lead to data integrity issues as; if the data resent contains SIP user credentials, unauthorized users may be able to access VoIP services (Zhang, 2012). This can result in high costs on an organization because of illegitimate calls to expensive call cost locations by the attacker.

Port 5060 attack- according to Serianu (2012) Port 5060 is among the top 10 targeted ports by hackers in Kenya. This is as the port's traffic uses an unencrypted mode of transmission. Due to lack of encryption on the port, attackers can easily intercept, manipulate and eavesdrop on the traffic following through SIP.

Man in the middle attack- This is whereby an attacker intercepts a SIP call through manipulating SIP signaling messages by disguising themselves as a caller or receiver in a call session. Once the attacker has achieved this, he/she is able to hijack calls through use of a redirection server (Bader-uz-zaman et al. 2010).

Registration hijacking- It is undertaken when an attacker impersonates a legitimate UA on the registrar and replaces the UA's SIP address with his address (Arafat, Ahmed, & Sobhan, 2013; Thermos & Takanen, 2008). Registration mainly requires a username and password authentication. If weak passwords are set within an organization, an attacker is easily able to learn SIP registration passwords of users and hence able to hijack SIP calls in the organization (Capacity business briefing, 2013). The registration session is vulnerable because it uses UDP protocol, which has a weak security mechanism (Arafat, Ahmed, & Sobhan, 2013; Asghar & Azmi, 2010), and the SIP registration server cannot dispute the legitimacy of a SIP proxy server or UA (Asghar & Azmi, 2010).

DoS – A DoS attack is the flooding of a network inevitably resulting to a service outage ensuring that legitimate users cannot be reached within the network (Asghar & Azmi, 2010). In a SIP-based VoIP network it can be as a result of;

1. **Session Tear down** attack through use of SIP BYE or CANCEL messages resulting to termination of SIP sessions or requests (Arafat, Ahmed, & Sobhan, 2013). The attacker sends a falsified, spoofed; SIP BYE or CANCEL message during an ongoing call, which in turn terminates the call or request. Session tear down can result to a DoS attack whereby the attacker floods the SIP network with SIP BYE or CANCEL messages resulting to termination of SIP sessions or requests resulting to SIP-based VoIP service outage (Asghar & Azmi, June 2010).
2. **Call flooding** attack, it occurs when an attacker sends massive valid SIP request messages to a SIP device. It can be undertaken through sending a large number of INVITE messages to a SIP proxy server or UA resulting to its crashing or rebooting or inability to receive new SIP INVITE messages (Bader-uz-zaman et al. July 2010).

Billing attack- Calls outside the service providers VoIP network are billed based on the destination and duration of the call. An attacker can initiate unauthorized calls, using a user's account and this, results in billing of calls and services a user did not directly make. This can be done through SIP messages manipulation. If an attacker accesses call records on a SIP proxy, they can manipulate them by either modifying or deleting records resulting to billing issues on the service provider's end (Thermos & Takanen, 2008). An attacker can also interfere with the billing process by intercepting the ACK message sent to signify a SIP session has started, this will result to the SIP proxies not recording the call as they will assume that the call has not been established as shown on the figure below;

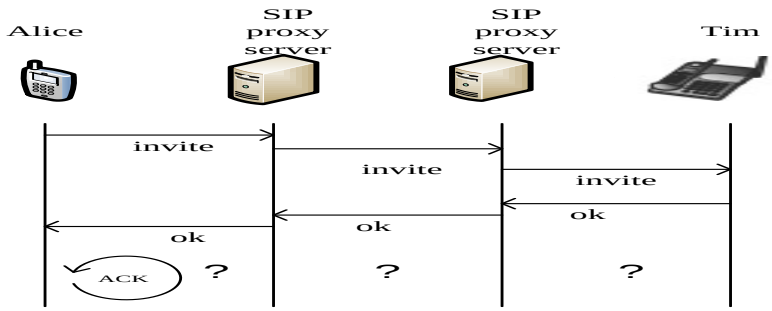


Figure 2.2: SIP Message Suppression attack
Source :(Thermos & Takanen, 2008)

Further SIP vulnerabilities and attacks

Several further possibilities for attacks exist in SIP-based VoIP networks, with the most common ones being toll fraud or sending unsolicited messages (Spam over IP Telephone, SPIT). However, they might require different detection and prevention methods not covered in this study. Several studies give a wider overview of multiple SIP vulnerabilities and attacks (Kuhn et al., 2005; Geneiatakis et al., 2006; VoIPSA, 2005; Zhang et al., 2007; Rosenberg and Jennings, 2008).

2.3.2 Lapses in an Organization that can lead to a security risks

Organizations place more emphasizes on technology to protect their information, networks and infrastructure, forgetting involvement of human beings in the process (Ashraf, 2005). It is noted that majority of security risks are human related and not as a result of technological faults (Ashraf, 2005; Al-Awadi & Renaud, 2007). This is due to organizations overlooking the human role in ensuring security (Al-Awadi & Renaud, 2007).

Organizations need to employ security awareness to its staff so as ensure security measures placed are all rounded; that is, they cater not only for the technological based risks but also the human based risks. Security awareness involves change in perception and view of target audience in terms of how they use information technology services by enforcing suitable security practices (European Network and Information Security Agency, 2010; Wilson & Hash, 2003). Organizations need to ensure information technology security at all times.

I. Lack of proper information security awareness in an organization

Security risks can be greatly influenced by lack of a person's knowledge and awareness of information security (Parsons et al., 2010). It has resulted to organizational financial, confidentiality and integrity issues as a result of employees inserting infected devices into the network or unknowing exposing highly sensitive information. Individuals need to be educated on the organizations information security expectations to help them comprehend the seriousness of security risks, their magnitude and the need to secure organization's information, systems and network against these risks (Parsons et al., 2010).

An Organization should also ensure presence of materials such as policies; documenting security expectations to staff on how they should handle the organizations information and technology. These materials should also clearly document, and also state consequence and

penalties to an employee, if found engaging in activities that may compromise the organizations information, networks and infrastructure security.

II. Cost versus benefits

The budget is not only important in executing and acquiring security measures, but also when implementing this measures in an organization; however, without presence of money, and organization will not be able to effectively implement and execute security measure and practices (Al-Awadi & Renaud, 2007). Investments on security should be aimed at saving organizations cost in the long run; this can be effectively achieved through analysing security measures in a cost-benefit view (Al-Awadi & Renaud, 2007).

Cost-benefit view involves viewing the various security risks an organization's assets are vulnerable to and comparing the likelihood of their manifestation with the impact faced if they were to manifest; this is with an aim of establishing the amount to invest in securing information, networks and infrastructure (Bishop, 2002; Trim, 2005).

III. Lack of decisive IT Policies

An organization need to properly document processes and procedure in undertaking; granting of system or device access, system upgrades and configuration changes (Blythe, 2011). This is most security attacks occur after a system upgrade or a configuration change as the new software or configuration change may have not been properly scrutinized to ensure that it is secure with no loop holes through which a hacker can access the organizations network and systems (Ngoma, 2012). A clear password management policy should also be present so as to ensure frequent changing of passwords and employees have complex passwords that can be easily hacked using dictionary and brute force attacks just to mention a few. In SIP-based VoIP network this attacks can result to further security risks such as identity theft and registration hijacking.

2.4 SIP-Based VoIP networks security models

A well-structured network security model is very critical in implementing and maintaining security. This is as it ensures that network architects are not missing any crucial security detail during designing and implementation of a network (Backfield, 2008). In existing networks, a security model is useful in developing a maintenance schedule and lifecycle for securing existing network. It is also useful in detecting where network breaches have

occurred so as to mitigate security risks. A network security model provides the basic structure needed in securing a network. It provides a security personal with an overview to pin point implemented security measures and as a result discover security gaps in an existing network (Backfield, 2008).

2.4.1 Multilayer secured SIP-based VoIP Model

It mainly focuses on Dos, eavesdropping and main-in-the-middle security risks. Its architecture is developed based on three categories of security techniques have been based on their functions. They include (Sadek, Ghalwash, & Basem, 2015);

1. Security enabling through authentication and encryption
2. Security protection through use of firewalls to protect the network from external threats
3. Network violation detection techniques

Security enabling techniques are implemented in authentication process by incorporating use of a username, password and MAC address of the UA. During the registration of a UA, authentication is granted through ensuring that a valid username and password is provided together with checking that the UA MAC is same mac address set for the specific UA on the system. This security measure helps to prevent some integrity based security risks. The UA credentials are further protected by storing them in an encrypted format; rather than a clear text in the database. Media and signaling protocols are also encrypted through use of Open Virtual Private Networks (VPN), hence ensuring confidentiality for the UA during a call as traffic is transmitted over a Secure Sockets Layer – based (SSL) VPN improving call quality due to UDP VoIP packet encapsulation of SIP. RTP and Open VPN also encrypt the data using a simple encryption protocol with a smaller key, and then using that key for short time; after the key expires, a new key is generated randomly and exchanged securely using RSA (Rivest, Shamir and Adleman) encryption.

The Security protection technique aims at securing the perimeter from external security risks such as DoS. It is achieved through deploying an inline snort (intrusion prevention system) located immediately after the firewall that filters traffic and only allows traffic based on configured rules set. The Firewall is first layer of defense and is located in between the private and public network. It is a bottleneck for network traffic because when designed properly no traffic can enter or exit LAN without passing through firewall. Rule based

priority queuing on firewall is the configuration set up for the model; rules have been categorized into three main rules for frequent users, normal users, and unknown users. Queuing mechanism has been preferred on the model as it prevents flooding based DoS security can be reduced if system has a good queuing mechanism.

Security violation detection techniques have been implemented using Intrusion Prevention System (IPS) three; Detection phase, Correlation phase, and automated policy driven response phase. Detection phase involves anomaly detection and misuse detection methods; misuse detection methods uses information from a known security policy that states out the vulnerabilities and security risks to VoIP systems, this approach compares the network activity with known attacks signatures, or other misuse indicators. Correlation phase involves gathering of data from multiple sites, and then intelligently correlating the data. In the automated policy driven response phase defines the appropriate action to be taken in case the correlation process detects a probable intrusion, a response of reject, drop or alert can be set. Signature based detectors determine the likelihood of an attack issuing an alert. Fig 2.3 below displays the set up.

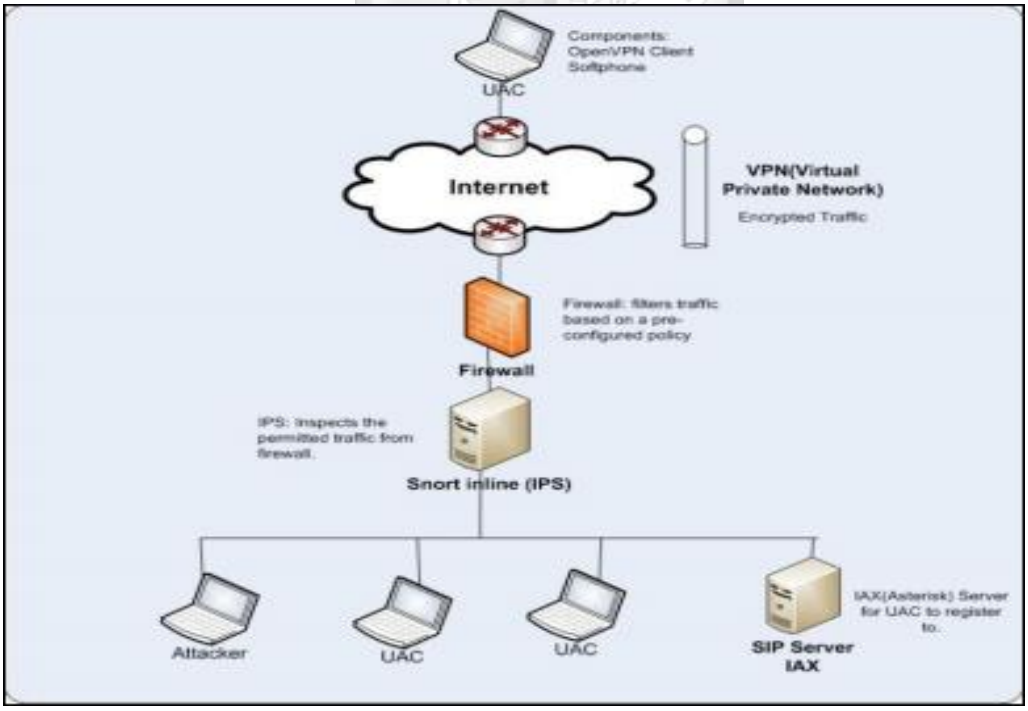


Figure 2.3: Multilayer secured SIP-based VoIP model
Source: (Sadek, Ghalwash, & Basem, 2015)

2.4.2 End to End Encryption Model

This model implements its architecture through use of triangular routing technique as shown in Fig 2.4. It makes use of two DNS servers i.e. a home DNS which belongs to the network on which SIP client was first registered, and a Foreign DNS which represents other networks other the home network of the client. Communication on this model takes place by IP resolution and encryption of the entire SIP session packet. The encryption algorithm used is based on a symmetric key block cipher technique. It applies a Feistal cipher technique and derives its base from TEA. A 256 bit key is used during encryption as a 128 bit key is less secure. When a user makes a call, the UA IP address of the callee is resolved using its home DNS. The IP is globally unique IP hence the session packet is formed using this IP. All the SIP message packet contents are encrypted using the above encryption algorithm except the "To" field. Once the packet is encrypted, it is sent via the internet cloud to reach its destination and the routing is handled by the intermediate routers. The callee receiving the packet decrypts the packet using the symmetric key shared. The encryption technique is based on the assumption that the callee is in the address book of caller.

If the callee moves into a different network, the callee will attach itself to the new network and send an IP update to its respective Home DNS and the DNS of other network on which it has contacts are on. This ensures generation of less over head as only limited DNS will be updated. Thus any known contact of callee wants to communicate then it will get the IP address from its DNS which has been updated. However, when a user is not in the callee contact book and the callee wants to call them the SIP session is routed through the home DNS through triangular routing the request will be sent to the home DNS. The home DNS will sort for the new location of its callee and forward the address to the caller after which the SIP session will be established.

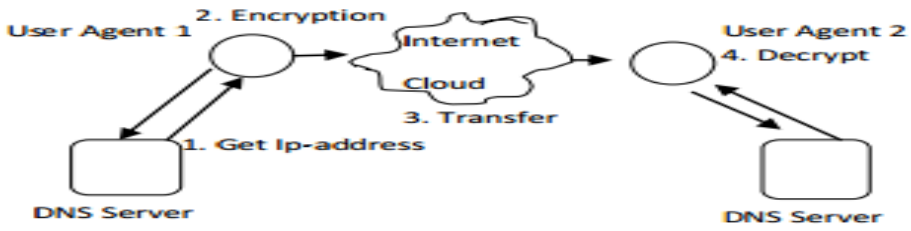


Figure 2.4: End to End Encryption Model
Source: (Lohiya, Shekokar, & Devane, 2012)

2.4.3 Comparison of existing SIP-based VoIP models

Securing of SIP-based VoIP using a firewall as depicted in the Multilayer secured SIP-based VoIP model presents certain challenges in the implementation of the model. It is essential to note that not all firewalls are SIP-based VoIP aware (Ruck, 2010); older firewall versions do not recognize VoIP protocol such as SIP and may block SIP-based traffic. Many firewalls also undertake scanning of traffic as intrusion detection or prevention systems; this is not recommended as since SIP-based VoIP is time sensitive and high relies on QoS. Intrusion detection or prevention systems set to be implemented on SIP-based VoIP networks need to be fully tested to ensure they do not inherently cause QoS issues to the SIP-based VoIP service (Ruck, 2010).

Though encryption of SIP-based VoIP, SIP packets illustrated on both models is a good approach, encryption policies are barely scalable due to the open and dynamic architecture of the Internet (Ferdous, 2014). Encryption as a security measure may also degrade the SIP-based VoIP network performance due to time taken during the encryption process and added authentication headers for packets (Sadek, Ghalwash, & Basem, 2015). It is also important to note that SIP-based VoIP highly relies on proper security measures being put into place in the organization's networks as a whole; however, despite presence of various security measures on the traditional data networks; those measure are not fully applicable on the SIP-based VoIP networks (Epps, 2006; Ruck, 2010).

2.5 Features of MPLS

The popularity of Multiprotocol Label Switching (MPLS) is increasing, particularly, as a set of protocols providing and managing of core networks in organizations. MPLS can integrate into data-networks, voice networks or a combination of both as long as this networks use the IP-based platform in the transmission of their traffic. MPLS superimposes IP-based networks and enables reserving of resources and predetermination of IP routes (Gupta et al., 2013).

MPLS effectively overlays connection-oriented framework over a connectionless network, and hence, providing virtual links or tunnels on the packet switched network that facilitates connections to nodes, which lie on the edge of the network. One of the main requirements of the telephony network is the availability and reliability on a real time basis as calls should

not be dropped or callee found unavailable due to service unavailability. Due to this, it is paramount for downtimes to be very minimal and redundancy ensured on all component such as the link, switch and SIP servers (Fjellskål and Solberg, 2002).

MPLS effectively addresses network backbone requirements as it enhances IP QoS on the core network. It offers capabilities such as; interoperability through providing a bridge between access IP and core ATM; IP QoS, through end-to-end traffic engineering on the Core network guarantying QoS, security, and finally it ensures scalability as MPLS can be used to evade some hitches associated with IP over ATM/FR overlay (Ahmed & Mushtaq, 2014).

There are numerous potential provisions in which voice is transmitted through MPLS infrastructure such as Voice over IP over MPLS (VoIPoMPLS) and Voice over MPLS (VoMPLS). In VoIPoMPLS, the protocol stack that comprises of voice data encapsulated in IP layer protocols (e.g., UDP/ RTP) followed by encapsulation in the MPLS protocol. Compressed headers can also be used in some setups. However, Voice can be directly carried over MPLS (VoMPLS) that is without encapsulation of the voice packets. In such a case, the typical protocol stack will consist of voice data encapsulated in the MPLS protocol on top of an MPLS transport arrangement such as FR, ATM, PPP, or Ethernet (Ahmed & Mushtaq, 2014).

VoIPoMPLS, is a technique of deploying VoIP and is largely supported by existing IETF standards however, it is not taken into consideration in this study. VoMPLS, enables an efficient transport mechanism for transmission of voice in the MPLS environment and is the technique taken into consideration in this study. There are many similarities to this technique and other architectures used today for VoATM and VoFR (Fjellskål and Solberg, 2002).

2.5.1 Adaptation of MPLS

Multi-Protocol Label Switching (MPLS) is a switching technology that regulates data traffic and packet forwarding in a complex network. A connection-oriented methodology that traverses packets from source to destination node across networks is what it does for fast packet transmission. It has the feature of encompassing packets in the presence different

network protocols. In traditional IP routing, packets undergo analysis at each hop, followed by forwarding decision using network header analysis and then lookup in routing table.

In an MPLS network, packets carrying data are assigned with labels on each node and the forwarding decision is totally based on these label headers. This is different from the conventional routing mechanism. Packet header is analysed only once while they enter the MPLS cloud from then the forwarding decision is 'label-based' that ensures fast packet transmission between local-local and local-remote nodes.

2.5.2 Framework/Architecture of Voice over MPLS

The MPLS network contains a number of devices which include Gateway devices, a transit router, and the Label Switched Path. Gateways may be directly connected to each other or indirectly connected through a number of transit routers. Figure 2.5 illustrates an MPLS network where customer traffic (Customer Edge, (CE)) is kept distinct by using unique labels (VRF (Virtual routing and forwarding)) for each customer connected to a PE (Provider Edge) router (Park, 2008). As per Figure 2.5 VoMPLS is not a complex implementation, it just needs the underlying MPLS infrastructure properly setup. It is not the intention of this document to detail all the internal workings of MPLS networks and the signaling that supports VoMPLS, there are many different variation of how VoMPLS may be executed and installed in a network. The intention of the reference design is to support all possible deployments of VoMPLS.

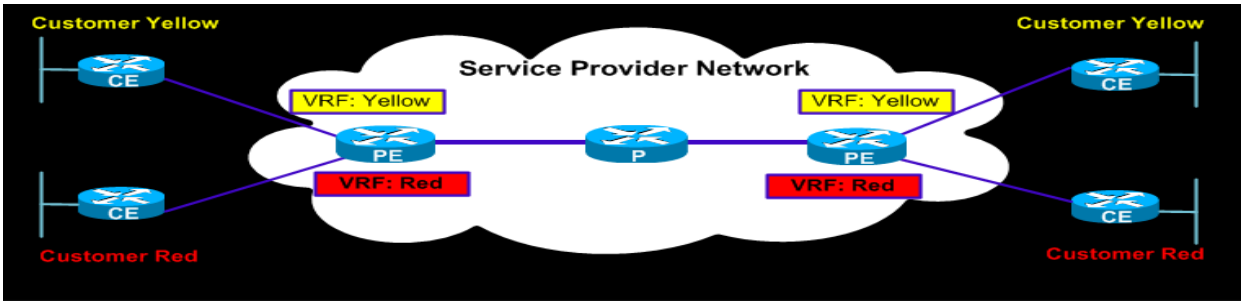


Figure 2.5: VoMPLS Reference Architecture

Source: (Park, 2008)

The above highlighted design must be capable of supporting many different LSP (Label switched paths) arrangements to convey voice payloads in the MPLS environment. For

example: One option may be an end-to-end Switched Path established between two voice devices currently within a single MPLS domain. A second option may be a LSP that has been proven to back only a portion of the voice connection between the end devices.

In the second case, multiple LSPs may need to be joined to form an end-to-end connection; or maybe interworking between a LSP and another type of bearer may be required. This is a common event in the current ISDN/PSTN environment where multiple service providers may be involved in carrying the call between the end devices. Cox (2009) stated that MPLS domain might exist between the entry and exit gateway nodes of the service provider network and the switched paths are created between these network entries to carry calls in a voice trunking arrangement. Customers demand predictable service, therefore to succeed, it is desirable to provide a high-quality backbone which minimizes bottlenecks and ensures dependable service provisioning. The capability to handle amplified traffic volumes, manage very dynamic traffic, supporting new customers' traffic without performance hits are considerations in this success equation. MPLS is the basis for cost-efficient, highly reliable infrastructure and multiservice IP networks. Its benefits include increased bandwidth efficiency and scalability, reduced operational and management expenses, and more reliable service delivery (Alcatel-lucent, 2010).

2.5.3 Security components of MPLS

There is a growing concern as to how secure MPLS really is and how it can be protected from Internet attacks. In MPLS, security is achieved through obscurity that is in a pure MPLS environments without Internet access leakage, the network is hidden; it is like the customer is setup on a private LAN but it is securely extended over the ISP's public network. This means that no information is revealed to third parties or the Internet. Since the customer has his own private cloud with no information being revealed to the outside, malicious attackers are unable to obtain access and even the attackers are unable to obtain the critical information needed in order to perpetrate attacks like Denial of Service (DoS) attacks and bring down the network.

In addition, since the security of MPLS is dependent on the service providers edge and core network being secure, the service providers prevent their routers from being reachable via the Internet by using methods like packet filtering and access control lists to limit access

only to the necessary ports to allow the routing protocols operate correctly from within their network. In one Kenyan ISP for instance, for a customer who needs Internet and MPLS, the customer has to get two different gateway equipment i.e. one router will be used for terminating and configuration of the MPLS network and another router with be configured for Internet access. This effectively isolates MPLS from the Internet and hence quite secure. However, this setup does not fully assure security because through the Internet, local machines can still be comprised and through these compromised machines attacks to the MPLS network can be launched. Through adequate and proper configuration of firewalls and good IT security policies can minimize the chances of being comprised via the Internet. In conclusion pure MPLS networks are secure in themselves due to the fact of their anonymity to the Internet.

2.5.3.1 MPLS Encryption

While MPLS provides an ascendable model in which customers can securely connect remote sites between each other, there have been fairly a few questions about the encryption services offered by service providers for these circuits. MPLS environments usually do not have encryption services. The MPLS architecture makes it pretty impossible to hack into the MPLS circuits and expose the internal network(s) and routes, unless a major bug or configuration flaw exists somewhere in the provider's network. Encryption of the MPLS is performed using IPsec, which essentially is a suite of protocols designed to provide a secure IP based pathway between two or more endpoints.

IPsec encryption between two sites connected via MPLS can be done by Customer Edge-Customer Edge IPsec, where the IPsec is set up between the CE's on each end, therefore the entire path between the CEs is protected. This setup offers the best possible protection against possible hacking attempts. Packets enter the CE router and are immediately encrypted and the packets are decrypted on the other end, they are located directly at the customers LAN network. This IPSec offers true protection against the change of transit packets between the sites and eavesdropping anywhere in the MPLS network.

The second encryption method is Provider Edge – Provider Edge IPSec which is by far less secure than the preceding one examined. Encryption occurs from the Provider network routers onwards, leaving the rest of the network unencrypted and therefore not providing

true end to end security. IPSec tunnels have a substantial administrative overhead for example, maintaining an IPSec topology between 5 sites requires the configuration of multiple Crypto IPSec tunnels on each router located at the 5 sites. Any alterations made to one router (e.g internal routes or LAN IP Addressing) necessitates the reconfiguration of all other routers so that the IPSec tunnels endure working properly.

2.6 Proposed SIP-based VoIP network security model derived from MPLS

The proposed models aims at securing the SIP-based VoIP network through implementing SIP-based VoIP on a network fully alienated from the internet i.e. the connection from the user to the SIP servers located at the voice service provider's end. This was achieved through implementation of SIP-based VoIP on the MPLS network infrastructure with the aim of inhibiting user devices located in the organization from being reachable from the internet which ensures availability, integrity and confidentiality of the voice traffic on the user's end at all times.

The VoMPLS set up will be implementing using private IP's such as 10.0.0.0/16 so as ensure there is a point to point (direct) connection between the organization's SIP-based VoIP network and the service provider's end. For this set up to be achieved an MPLS cloud on which the SIP packets will traverse through needs to be set up by the voice service provider so as routing of the tagged voice packets can be effectively done. .Due to this, the client must have a MPLS enabled router to managed routing of the voice traffic to the MPLS cloud. Cost was also considered in the proposed model so as to ensure that equipment's needed on the end and the infrastructure required was on the basic minimal. The proposed model is as shown below;

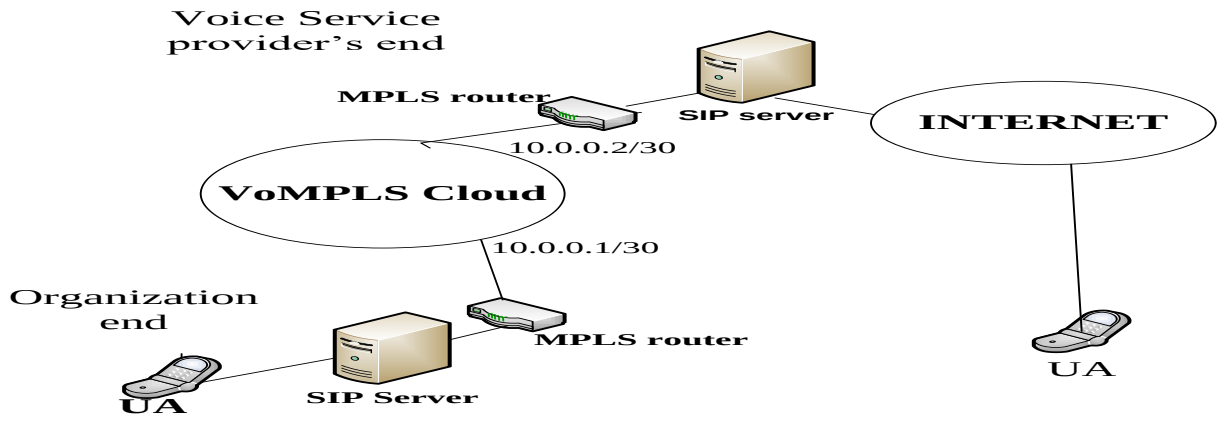


Figure 2.6: SIP-based VoIP security architecture

2.7 Conceptual framework

Conceptual framework is defined as the result of when a researcher conceptualizes the relationship between variables in the study and shows the relationship graphically or diagrammatically (Mugenda and Mugenda, 2003). A conceptual framework presents the constructs and interrelationships of a research study. It is meant to assist a researcher in generating an understanding on the concept under investigation.

The conceptual framework of the study was based on the relationship between network infrastructure , existing security risks and organizational security awareness with the aim of establishing security measures need in better mitigating security risks faced on SIP-based VoIP networks. In the development of an acceptable security model for SIP-based VoIP it is important to have a significant insight on the characteristics of the main adopters of the model and who are likely to reject its application and usage so as to better redesign it with the aim of ensure better organizational uptake and implementation of the model.

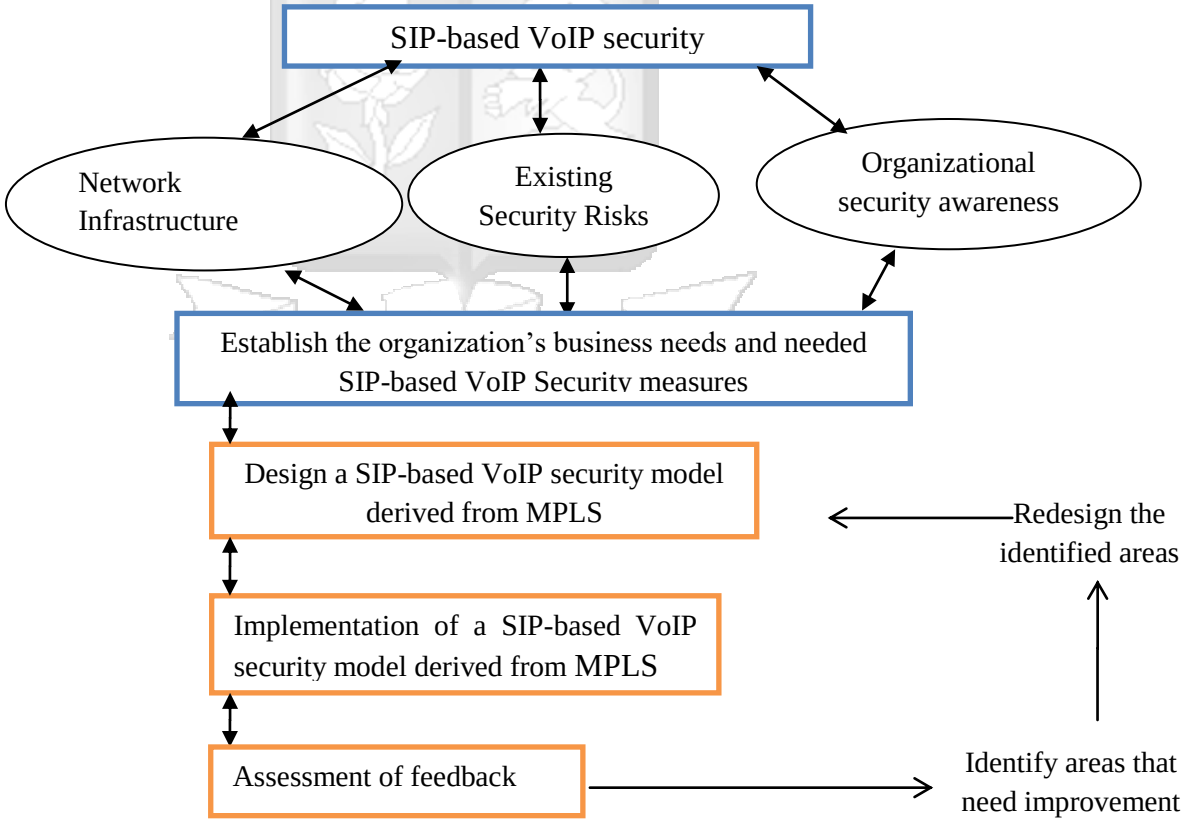


Figure 2.7: Conceptual framework for designing a SIP-based VoIP security model

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes methodology used in undertaking the study. Specifically, it describes issues related to the research design, population, sampling techniques, data collection instrument and validity and reliability of the instrument.

Research methodology involves systematical resolution of a research problem. It comprises theoretical analysis of the body of methods and principles associated with a branch of knowledge. A methodology offers the theoretical underpinning for understanding which method, set of methods, or so-called "best practices" can be applied to a specific case, for example, calculating a specific result (Irny & Rose, 2005).

An Applied research method was adopted, as applied research seeks to resolve practical, everyday problems by finding a solution to a specific problem (Roll-Hansen, 2009). Applied research design was particularly chosen as the research's aimed at developing a model through which organizations will be better placed in mitigating SIP-based VoIP security risks in their organization.

3.2 Research Design

Research design has been defined to be a scheme, outline or plan that is used to generate answers to research problems; a road map of how the researcher goes about answering the research questions ((Bryman & Bell, 2007) & (Orodho, 2003).

The research study used a quasi-experimental research design. Quasi-experimental research design tests casual relation in a given uncontrolled environment with the aim of analyzing an outcome of interest based on a treatment (Levy & Ellis , 2011). Quasi-experimental research design was particularly chosen as the research analyzed if the developed SIP-based VoIP security risks mitigation model based on MPLS was able to enable organizations better mitigating SIP-based VoIP security risks in their networks.

3.3 Target Population

Target population is described as the entire group a researcher is interested in; the group about which the researcher wishes to draw conclusions Glicken (2008). The research study mainly targeted organizations in the Nairobi County that use SIP-based VoIP and SIP-based

VoIP service providers; this was with the aim of achieving an all rounded research. The targeted population needed fiber optic, WiMAX, copper cable or other forms of internet and data subscriptions to be eligible for SIP-based VoIP services. According to TESPOK, fiber optic data and internet subscriptions in Kenya by 2013 were estimated at 79,484(Serianu Ltd, 2014). The target population of organizations using SIP-based VoIP was estimated to be a cross section of around 10% of the total internet and data subscriptions which translates to around 7,949 forming this studies target population.

3.4 Sample and Sampling Technique

A sample is a group of people representing the whole population. The study used simple random sampling technique to identify the research study sample. In simple random sampling; every element has an equal probability in the selection process from the population that is, (a sample n from the N population) (Meng, 2013).

The sample size is defined as the number of observations in a sample (Evans, Hastings & Peacock, 2000). The sample size was 97 based on the below formula which allowed reporting of results with 95% confidence and a 10% maximum error) thus allowing a non-discriminated representation of the target population hence eliminating any biasness in the sample size selection.

$$n = \frac{z^2 . p . (1-p)}{d^2}$$

$$n = \frac{(1.645)^2 (.10) (.90)}{(0.05)^2}$$

P - Expected proportion in the population =20%
n - sample size
z=1.645 Confidence level
$\mathbf{d^2}$ =absolute precision (5%) = 0.05

3.5 Data Collection Methods

Data collection is a means by which information is obtained from the selected subjects of an investigation with the aim of attaining numerical data through use of various tools (Creswell, 2012). The study used both primary and secondary data collection tools.

Primary data was collected through use of self-administered questionnaires and interviews. Denscombe (2007) observed that, a questionnaire defines the problem and the specific study objectives of a study. The questionnaires included structured while the interviews included structured and unstructured questions. Structured questions allow specific types of responses such as yes, no and likely scales. Unstructured questions on the end allow the respondents to give responses as they wish. The structured questions were used in an effort to conserve time and to facilitate an easier analysis as they are in immediate usable form. The unstructured questions were used to encourage the respondents to feel free to elaborate and not feel restricted.

The study also used secondary data in the analysis existing data relevant to the study. The secondary data tools used included; books, websites, indexing, online files and books enabling a conclusive literature review to be undertaken.

3.6 Data Analysis and Presentation

Data analysis is the process of examining data using analytical and logical reasoning with aim of evaluating each variable in the data provided. The data analyzed was collected through use of questionnaires and interviews which were edited, coded and descriptively analyzed. In addition, arithmetic mean model was applied to enable analysis of the data variables with the aim of representing factors such as average and mean which were used to better analyze the various research questions and variables used in the study. The data collected was presented using graphs, charts, and tables for interpretation.

3.7 Research Quality

Instrument validity refers to the accuracy and meaningfulness of inferences which are based on research results obtained from analysis of data that actually represent the phenomena under study. It therefore refers to how accurately the data obtained, (in this case through questionnaire sand interview questions) to ascertain their validity in the study (Orodho & Kombo, 2002). The research validity was ensured by administering the questionnaire and interviews to the correct organizations which had been randomly selected. Content validity is the degree to which the instrument fully assesses or measures the construct of interest (Miller, 2012 this was key in this research.

Reliability is a measure of the degree to which a data collection instrument yields consistent results or data after repeated trials (Drost, 2011). A reliable data collection instrument is one that produces consistent results when used more than once to collect data from a sample randomly selected from the sample population. Cronbach's Alpha test was used to provide a measure of internal consistency of the questionnaire. It is expressed as a number between 0 and 1, Cronbach (1951). The Cronbach Alpha test formula used in the study was;

$$\propto = \frac{n}{n-1}\left(1 - \frac{\sum Vi}{Vtest}\right)$$

n=number of items
Vi= Variance of scores on each question
Vtest= total variance of overall scores (not percentages)

3.8 Ethical Consideration

Oliver (2010) indicated that ethics must be considered in all aspects of the research study. The researcher has a moral obligation to protect the participants of the study from harm. Hence, the research must take all the necessary conditions to ensure that the rights and duties of all the research participants are respected and upheld. Oliver (2010) indicated that ethics in research must consider ethics in relation to the research design, data collection, data storage, and presentations of findings in a responsible and moral manner.

The study ensured that information provided by each individual was handled in a manner of confidentiality and integrity with respect to each individual's privacy. Organization's names were omitted in the research report to ensure privacy. The study also ensured that the research process was in line with the country's legal and copy right laws and that data used is in line with the social and organizational culture expectations.

CHAPTER FOUR: DATA ANALYSIS, PRESENTATION AND INTERPRETATION

4.1 Introduction

Data analyzed was summarized in line with the research objectives and appropriate frequency tables inserted for presentation. The analysis was conducted to examine the mitigating measures adopted to address security risks in sip-based VoIP networks in Kenya. The data analysis presentation and interpretation of subjects under study was presented in form of percentages, figures and frequency tables. This gives the reader an insight into the organizations' security risks and mitigation measures.

4.2 Questionnaire Response Rate

Questionnaire response rate refers to the proportion of the questionnaires returned after they are issued and filled by the respondents. The respondents who filled in the questionnaire were 66 from the targeted 97; this is a response rate of 68%. This was a good response rate based on Richardson (2005) findings who states that a response rate of 60% and above is acceptable.

4.3 Reliability Analysis

Reliability broadly refers to the capacity of a measurement to produce consistent results (Sarantakos, 2005). Along with this approach two additional measures were taken to check the reliability of the scales: At the development stage, after the pilot-test, a separate test-retest was conducted. Ten respondents completed the questionnaire and were asked three days later to complete the same questionnaire again. An analysis of all answers of the questionnaire indicated a very high Pearson correlation of above 0.78.

4.4 General Information

This section presents Part A. of the questionnaire aimed at collecting the background of the organizations. The background information in this study is characterized by collecting data about the use and importance of SIP-based VoIP in that organization together with the level of security awareness in the organization.

4.4.1 Duration of interaction with VoIP

The study sought to find out the respondent's and organization's perception on adoption of VoIP and experience they have had with SIP-based VoIP. The findings are illustrated in figure 4.1.

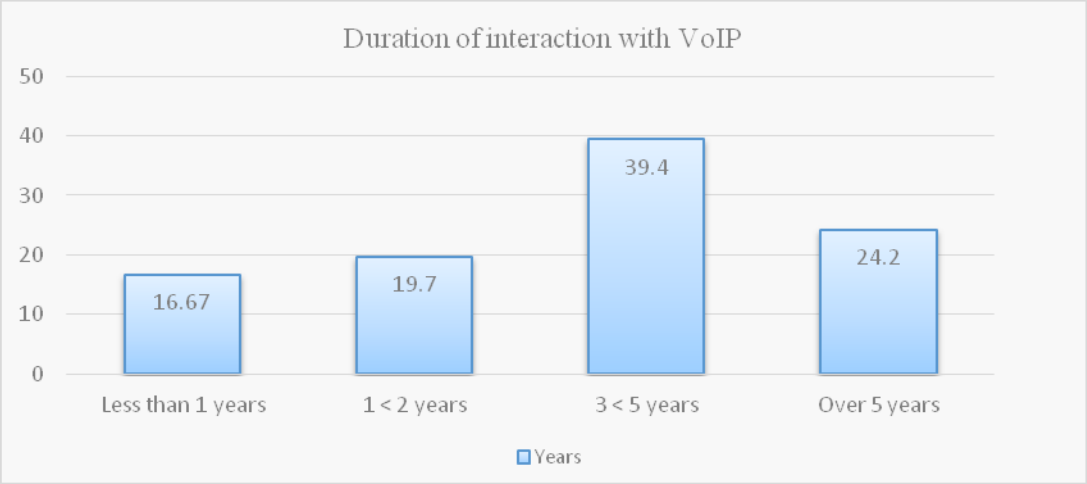


Figure 4.1: Duration of interaction with VoIP

From the survey (figure 4.1), the experience in use of VoIP in Kenya is still not high as most of the organizations surveyed have been using VoIP for less than 5 years. Only 24.2% of the organizations have used VoIP for over 5 years, the majority, 39.4% have used it for between 3 - 5 years. Quite a significant number 19.7% have used VoIP for 1-2 years but only 16.7% for less than a year.

4.4.2 Importance of voice communication in your organization

The question sought to ascertain how much organizations value the use of voice communication in the organization. About 72.7% of the respondents rated voice communications as highly important in the organization, 18.2% thought voice communication was of moderate importance while 9.1% respondents stated a low level of importance in voice communication which is captured in figure 4.2.

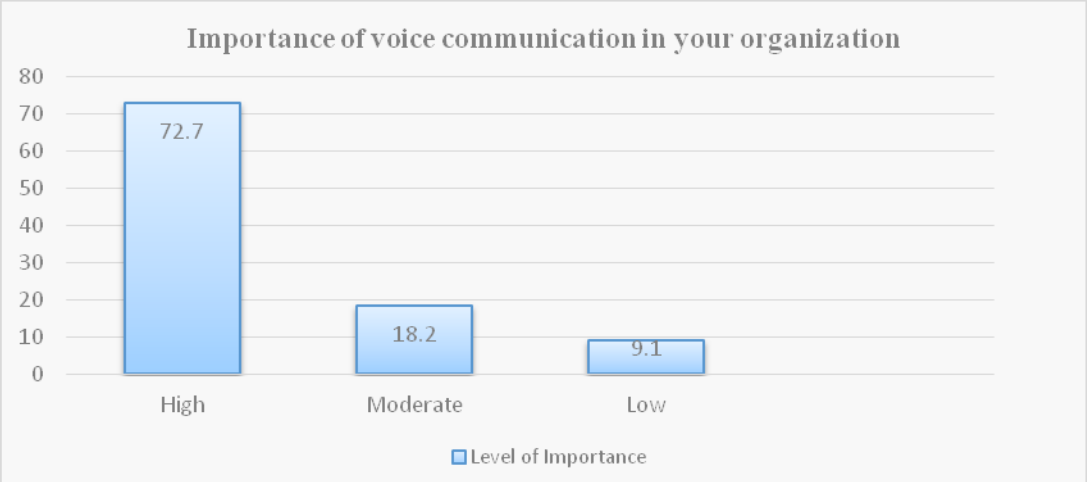


Figure 4.2: Importance of voice communication in your organization

4.4.3 IT security policy

This question aimed at establishing whether the organizations sampled had an existed security policy. This information was key to the study since VoIP runs on the existing IT infrastructure, the security of the infrastructure is absolutely key in mitigating the SIP-based VoIP network security risks. With security policies in force in an organization, the likelihood of security lapses can be minimized and caught before they can propagate and cause massive damage. Data from the survey figure 4.3 shows that most of the respondents' organizations (48.5%) have IT security policies present.

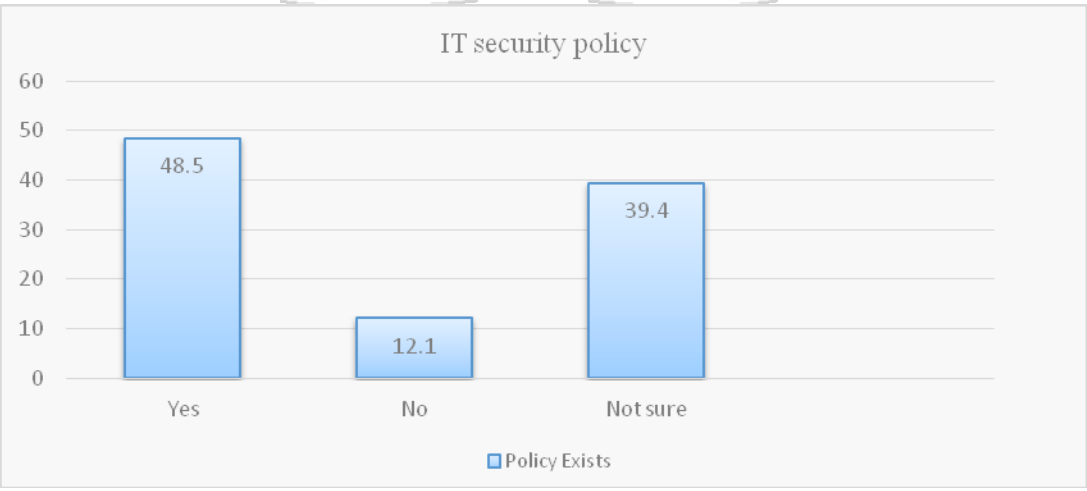


Figure 4.3: IT security policy

4.4.4 Level of IT security awareness in the organization

This question sought to establish level of IT security awareness among users in the organizations sampled. If the organization has a high level of security awareness present, it is able to implement IT security policies effectively and cater for not only the technology based security aspects but also the users or people based security aspects in the organization; otherwise IT security implementation will not be effective. Figure 4.4 illustrates data pertaining to the level of implementation of the IT security policies in the respondents companies. Most of the company had a moderate level of implementation at 53%, followed by low implementation of the security policies at 24.3% and lastly 22.7% of the respondents have a high implementation of IT security policies in their organizations.

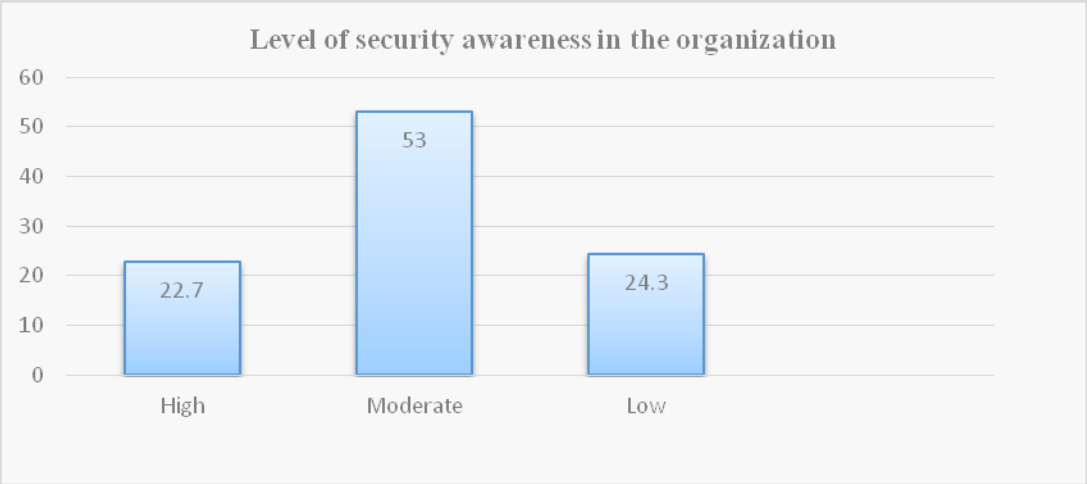


Figure 4.4: Level of security awareness in the organization

4.5 Security risks faced in organizations using SIP-based VoIP networks

The study sought to analyze security risks on SIP-based VoIP networks faced by organizations in Kenya. It aims at analyzing the various security risks discussed in chapter 2 and how they have affected SIP-based VoIP networks in organizations.

4.5.1 Occurrence of security risks in SIP-based VoIP network

The question sought to establish whether a security risk had ever occurred in the sampled organizations SIP-based VoIP network. The respondents' answers are tabulated in the figure 4.5. 45.45% of the respondents indicated that yes they have experienced security risk on their SIP-based VoIP network, 36.36% were not sure whether or not they had experienced

any security risk and 18% of the respondents' organizations' had faced no security risks on their SIP-based VoIP network.

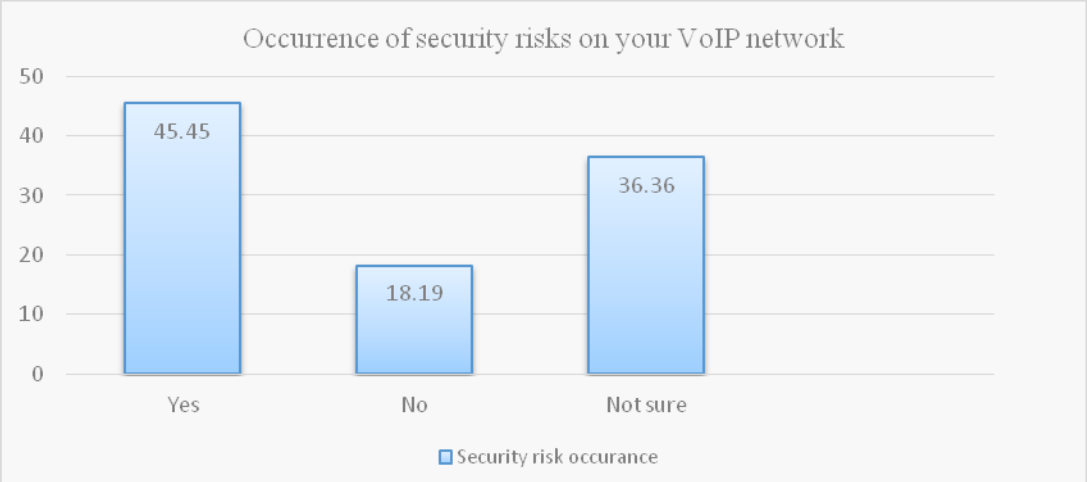


Figure 4.5: Occurrence of security risks on your VoIP network

4.5.2 Frequency of different types of security risks in SIP-based VoIP networks

The respondents were asked to state the frequency of different types of security risk on their SIP-based VoIP network and were allowed only one choice from the list (figure 4.6). The results of this question was that 30% of the respondents experienced authorization and authentication related risks, 37% experienced availability related security risks, & integrity related risks were rated at 18% and last was confidentiality related security risks at 15%. Availability security risks were rated highest.

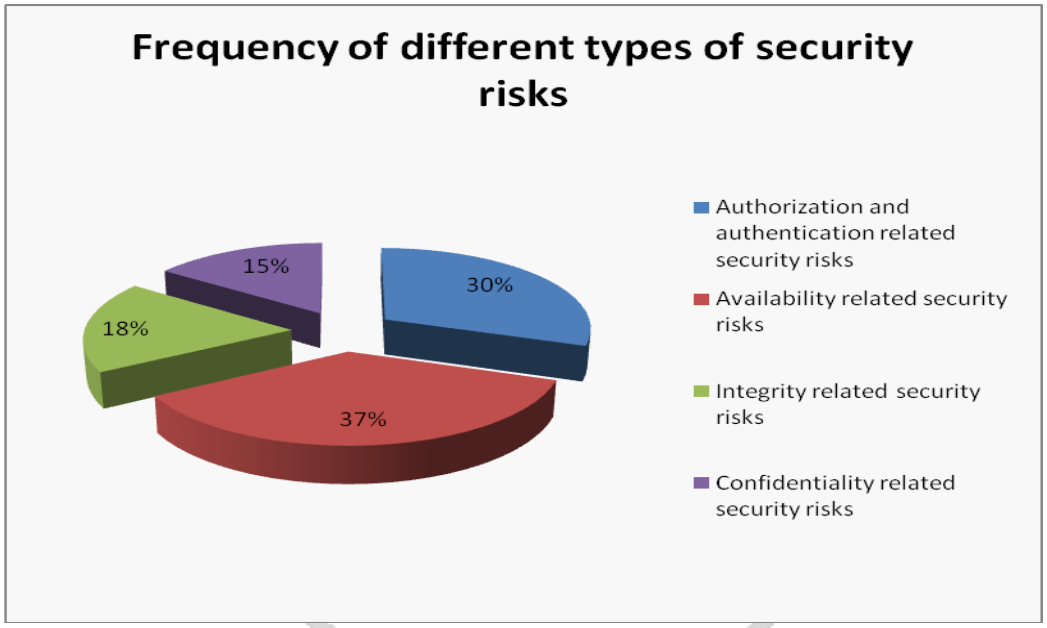


Figure 4.6: Frequency of different types of security risk in SIP-based VoIP networks

4.5.3 Likelihood of various SIP-based VoIP security risks

The respondents were also asked to rank the likelihood of listed SIP-based VoIP security risks on the questioner and the data has been tabulated in the table 4.7. The security risks that were ranked most likely to occur were Identity theft, denial of service, and eavesdropping. While the most unlikely security risks were Replay and message tampering in order.

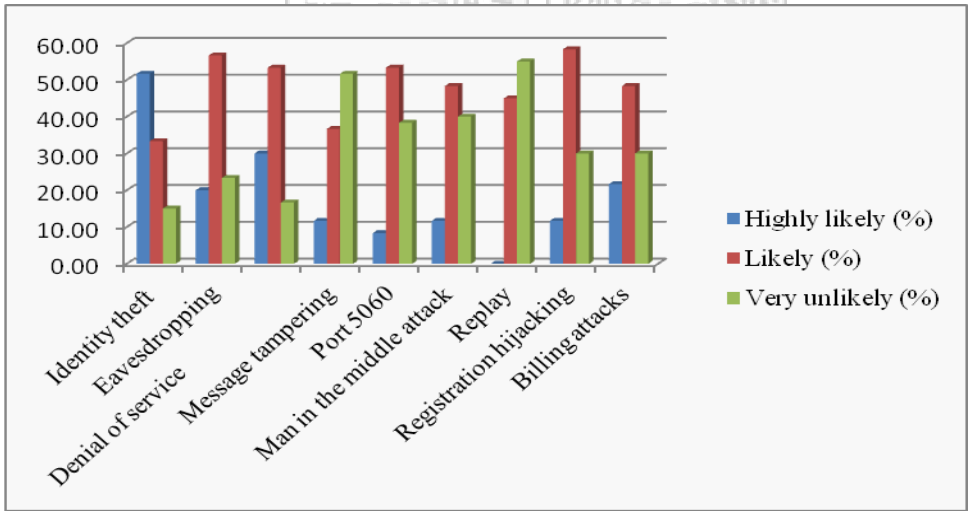


Fig 4.7: The likelihood of SIP-based security risks

4.6 Existing techniques against SIP-based security risks

The study sought to explore the existing SIP-based VoIP networks security measures employed by organizations in Kenya and their effectiveness in mitigating against SIP-based VoIP security risks.

4.6.1 Voice traffic segmentation

Figure 4.8 highlights the data collected from the respondents about whether VoIP traffic in their organization is isolated by a dedicated link from the rest of the data traffic. 57.58% of the respondents said that in their organizations, the VoIP traffic is carried on the same link with the rest of the traffic while 28.79% said yes that their company had acquired a dedicated link just for voice communication.

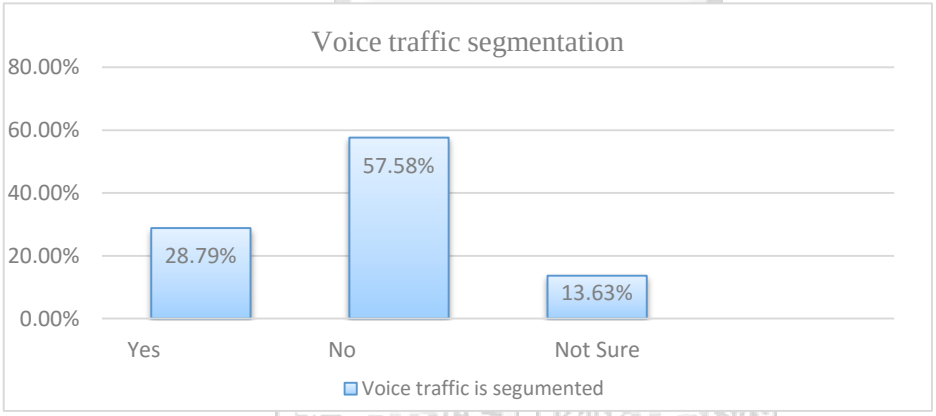


Figure 4.8: Voice traffic segmentation

4.6.2 Implementation of security on SIP-based VoIP networks

This question sought to establish whether the respondents' organizations had implemented any security measures on their SIP based VoIP networks. Surprisingly as per figure 4.9, the majority was 63.02% saying that there are no security measures specifically put in place to protect their SIP based VoIP networks while only low rate of 36.98% had security measures implemented on their SIP-based VoIP network.

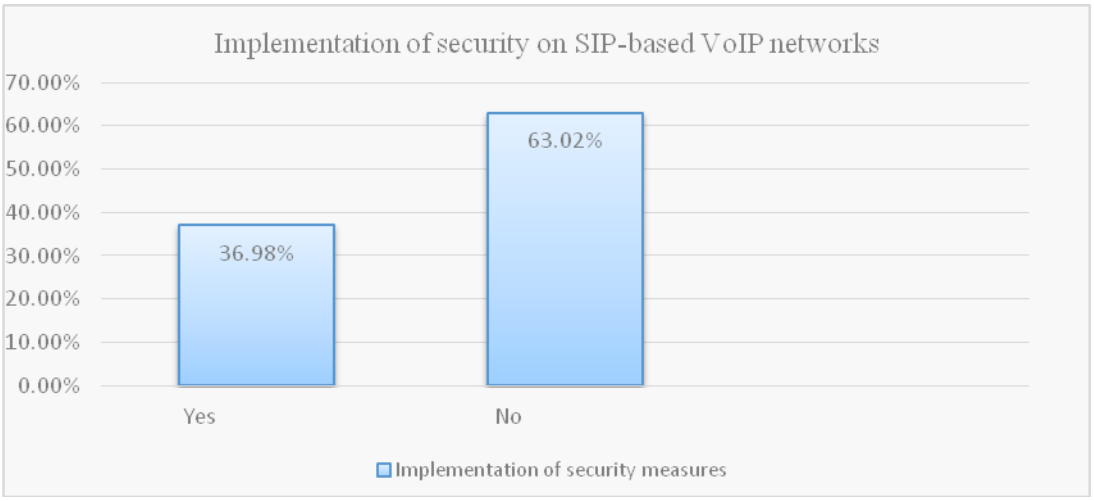


Figure 4.9: Implementation of security on SIP-based VoIP networks

4.6.3 Implementation of existing security approaches or models on SIP-based VoIP networks

Figure 4.10 highlights the data collected from the respondents on their SIP-based VoIP networks security with regards to which security measures they had implemented or would like to implement. 16 of the respondents stated end to end encryption model, 15 stated use of encryption, 12 of the respondents stated use of VPNs while the rest of the respondents that is; 10, 8, 5 stated use of firewalls, multilayer secured Sip-based VoIP model and Intrusion Prevention Systems respectively. Encryption security measures were ranked highest.

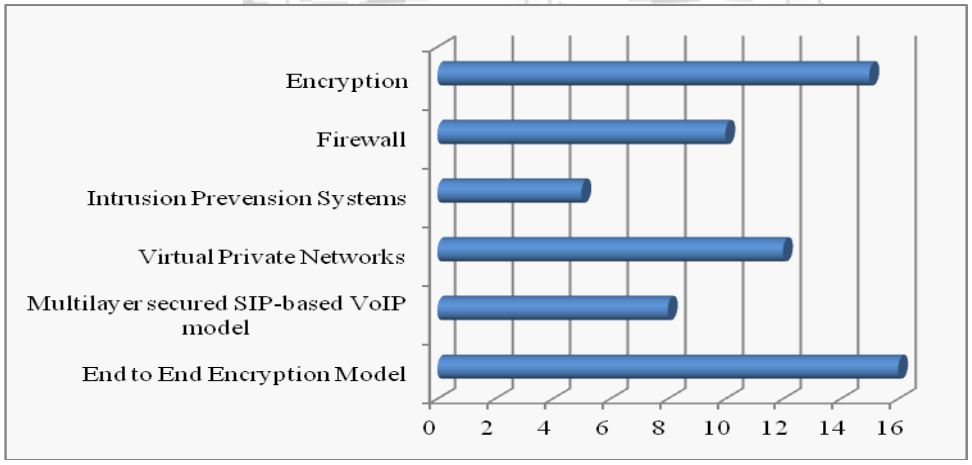


Figure 4.10: Implementation of existing security approaches or models on SIP-based VoIP networks

4.6.4 Suitability of existing security approaches and model

Figure 4.11 highlights the data collected from the respondents on the suitability of existing SIP-based VoIP security approaches and models. 29% of the respondents stated end to end encryption model as the best suited SIP-based VoIP security measure followed by use of encryption 20%. Use of a firewall and encryption were rated as moderately suitable security measures. Multilayer secured SIP-based VoIP model was however stated as the most unsuitable SIP-based VoIP security approach by respondents.

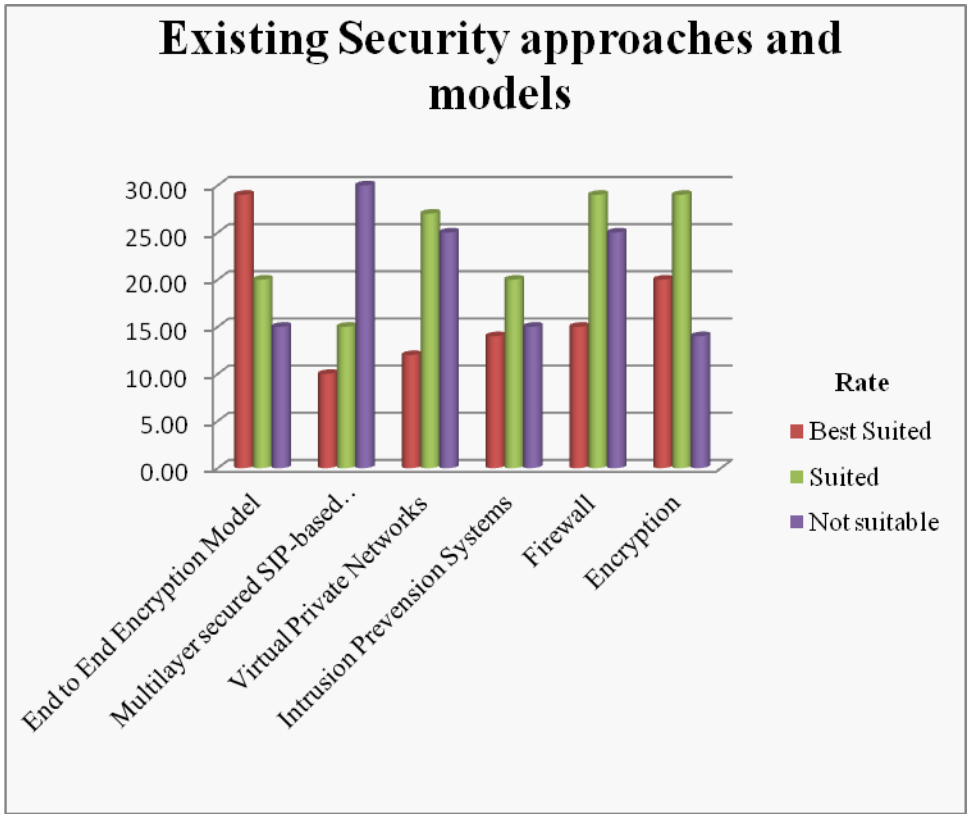


Figure 4.11: Suitability of existing security approaches and model

4.7 Effectiveness of MPLS in securing SIP-based VoIP networks

The study sought to analyze effectiveness of MPLS in mitigating SIP-based security risks on VoIP networks and its components.

4.7.1 Implementation of MPLS security components

This question sought to establish whether the respondents knew and had implemented MPLS technology in their organization's network. The findings as per figure 4.12 indicated that the majority 70% they knew what MPLS technology was and had implemented MPLS architecture in their network. The remaining 30% knew what MPLS technology was, however they had not implemented MPLS technology on their network.

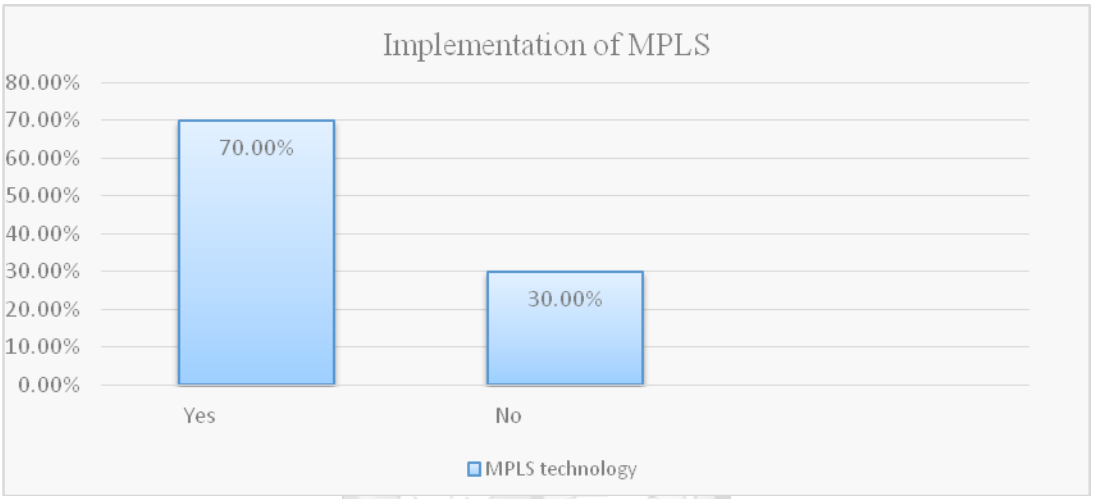


Figure 4.12: Implementation of MPLS

4.7.2 Effectiveness of various MPLS security components

This question sought to establish how effective the respondents who had implemented MPLS technology on their network viewed various MPLS components. The results indicated that the majority 41 respondents viewed internet anonymity as the most effective MPLS security component followed by private LAN. Based on figure 4.13 below, very few respondents felt that MPLS tunnels, 7and Encryption, 6 MPLS security components were not effective.

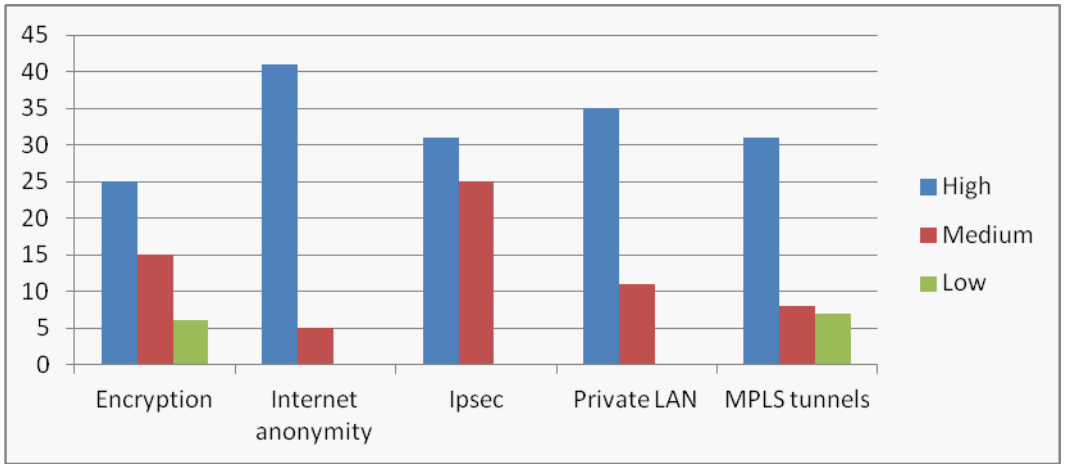


Figure 4.13: Effectiveness of various MPLS security components

4.7.3 Security on the MPLS network

The respondents were requested to rate how secure MPLS networks are in transmission of traffic. The results indicated that the majority, 60% felt that MPLS networks were highly secure, 32% felt that MPLS networks are secured while the remaining 8% felt that MPLS networks are not secure.

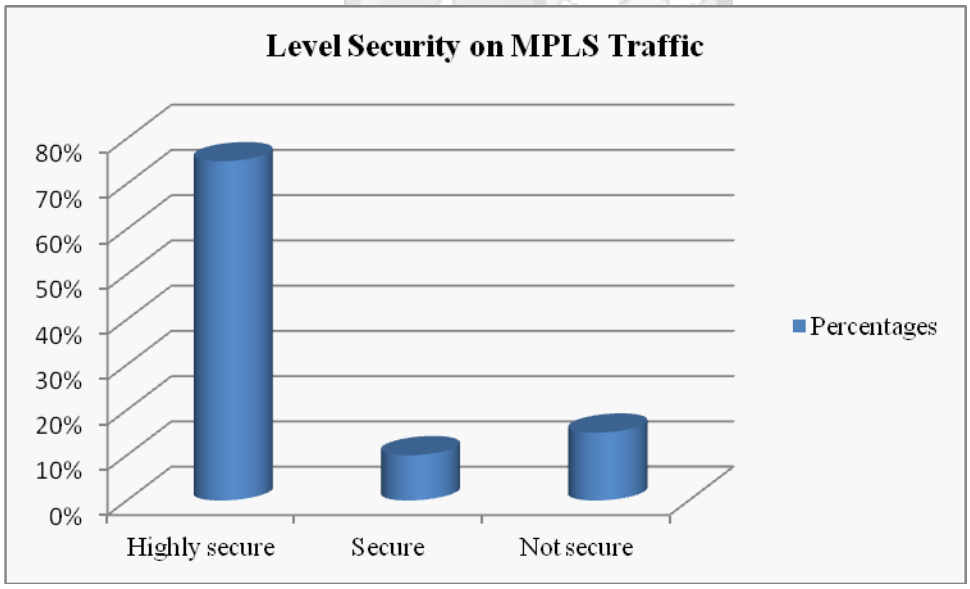


Figure 4.14: Level of Security on MPLS Traffic

CHAPTER FIVE: SIP-BASED VOIP SECURITY MODEL DEVELOPMENT

5.1 Introduction

The study has proposed a security model to guide in the implementation of a secure SIP-based VoIP network by an organization. The model was proposed against a background of in-depth examination of existing security measures and architectures already in existence. The findings helped identify the main pain points and issues a SIP-based VoIP security model should address. The proposed model is thus a result of the above.

5.2 Development of a SIP-based VoIP security model for organizations

Based on the study, the proposed SIP-based VoIP security model was developed using four main steps.

1. Analyze existing SIP-based VoIP security measures
2. SIP-based VoIP network infrastructure
3. SIP Protocol security
4. Organization security awareness

5.2.1 Analyze existing SIP-based VoIP security measures

67% of the respondents stated that they had implemented, or would like to implement encryption based security approaches on their SIP based VoIP networks. Encryption based approaches were rated top most suitable existing SIP-based VoIP security approaches. Firewalls and VPN were rated as the next most suitable SIP-based VoIP security measures after encryption. Table 5.1 below, presents a summary of the various SIP-based VoIP security measures implemented by the surveyed organization has been done. Also, the table analyzes the effectiveness of the different security measures.

Table 5.1: SIP-based VoIP security measures

Types of security measures	Characteristics	Effectiveness
Encryption	• Secures SIP-based VoIP traffic through encrypting voice traffic and SIP messages authentication. • Encryption may be done using either a stream or block cipher (Kuhn, Walsh, & Fries, 2005). If a stream cipher is used, very little delay is introduced if the key stream can be produced before or at least as fast as voice data	Encryption was listed as the most effective security measure. QoS is a big issue however as latencies and jitters

	arrives. Block ciphers may require one block of delay, which will vary with the method used, but still require relatively little overhead.	can be experienced if encryption is not correctly configured.
Firewalls	• Firewalls work by blocking traffic deemed to be invasive, intrusive, or just plain malicious from flowing through them. • Firewalls typically process such traffic using a technique called packet filtering. Packet filtering investigates the headers of each packet attempting to cross the firewall and uses the IP addresses, port numbers, and protocol type contained therein to determine the packets' legitimacy. • Firewalls could also be used to broker traffic between physically segmented traffic (one network for VOIP, one network for data)	Firewalls were listed as most suitable security measures after Encryption. Use of a VoIP aware firewall is highly recommended to eliminate any SIP calls drop or Qos issues that SIP unaware firewalls bring about
VPN	• Secures a SIP call by ensuring confidentiality for the UA during a call as traffic is transmitted over a Secure Sockets Layer – based (SSL) on the internet. • Data is encrypted using a simple encryption protocol with a smaller key, and then using that key for short time; after the key expires, a new key is generated randomly.	VPN's were also listed as most suitable security measures after Encryption. Proper configuration needs to be done to ensure VoIP service availability at all times.
IPSec	• IPsec, which essentially is a suite of protocols designed to provide a secure IP based pathway between two or more endpoints further details on section 2.5.3.1.	IPsec was listed as the second most effective MPLS security measure.
Internet Anonymity	• In MPLS, security is achieved through obscurity that is in a pure MPLS environments without Internet access leakage, the network is hidden • This means that no information is revealed to third parties or the Internet. Since the customer has his own private cloud with no information being revealed to the outside	Internet anonymity was listed as the most effective MPLS security measure as it eliminates the internet environment
MPLS Tunnels	• MPLS works by tagging the traffic entering the MPLS network. An identifier (label) is used to help distinguish the Label Switched Path (LSP) to be used to route the packet to its correct destination. • A different label is used for every hop and the label is	MPLS Tunnels were listed as the third most effective MPLS security measure.

	selected by the router (or switch) that is performing the forwarding operation.	

It is observed from the table that the different security measures existing in the surveyed organizations are important in the protection of the SIP-based VoIP networks. However if they are poorly implemented, not have SIP in mind, they can result to QoS issues on voice calls resulting in information security issues. According to Ruck (2010), a security measure should secure a service while at the same time ensure that quality of service is not compromised in any way.

5.2.2 SIP-based VoIP network infrastructure

Only 28.79 % of respondents stated that their voice and data traffic are segmented. Organizations need to highly consider traffic segmentation in securing voice communication so as to better protect their voice traffic from data related security risks. Traffic segmentation can be carried out through use of different VLANs for voice and data communication ensuring that security risks faced on the data segment to not easily affect the voice segment/network.

SIP-based VoIP infrastructure includes the different equipment's and links used in the routing, creation and termination of SIP traffic. Equipment's used include UA's, SIP servers, VoIP gateways, routers and firewalls. UA's such as SIP phones, soft clients together with SIP servers are used in the creation and termination of SIP traffic. Routers, VoIP gateways and firewalls, are mainly used in routing of voice traffic to the intended callee. For effective routing to occur SIP traffic needs to be routed either via an internet link or an MPLS link. This study advocates for use of an MPLS link due to its various security advantages stated in section 5.2.1 and chapter 2.

5.2.3 SIP Protocol security

As previously stated in chapter 2 section 2.2.2, security on SIP protocol has been greatly overlooked making the protocol highly susceptible to security risks (Ferdous, 2014). Research findings agreed with the above statement as nearly half of the respondents 45.45 % had experienced SIP-based VoIP attacks on their network; 36.36 % of the respondents were not sure whether they has faced any security risk on their network.

SIP methods have been susceptible to various security vulnerabilities that results to security risks such as billing attacks to an organization. Default features of SIP have also been misused by attackers; port 5060 is the default port used for all SIP traffic, attackers can easily initiate DOS attacks through the port if found open (SERIANU, 2012). 53 % of the respondents in chapter 4 stated that port 5060 attacks are likely to happen on the SIP-based VoIP network. An organization needs to secure itself by using a different port for all their SIP traffic. Security measures such as encryption discussed earlier are also necessary in ensuring SIP methods are securely transmitted at all times.

5.2.4 Organization security awareness

From the research findings, it was noted that voice communication is very important in organizations with 72.7% respondents saying it is of high importance. However, despite this more than half of the respondents, 60 %, had not implemented any known security measures on their SIP-based VoIP network. It is therefore important to ensure commitment of the organization in securing their voice network.

During Implementation of a security model into an organization; it is important to ensure all the security risks are addressed together with the organization's needs. This is so as to ensure a strategic implementation of the SIP-Based VoIP security Model. During development of a security model, one need not to concentrate only on technology and infrastructure aspects alone but also the aligning of the model with the organizations security objectives and user needs. This is so as to ensure maximum security benefits and high ROI (Return on Investment) for the organization on their SIP-based VoIP network.

5.3 SIP-based VoIP security model components

In order to ensure an all rounded security approach is implemented, this research has proposed three factors that an organization should evaluate. These form the components of the model.

5.3.1 Technological aspects

Based on the Literature reviewed, it is observed that SIP is becoming the predominate protocol used for voice communication. According to the findings in chapter 4; organizational security challenges such as identity theft, registration hijacking, Dos attacks

and eavesdropping were the top security risks organizations face on their SIP-based VoIP networks.

In order to develop a security model for SIP-based VoIP networks, the study needed to analyze the various security risks affecting SIP-based networks. Once this was accomplished, the study in section 5.2.1 analyzed the various security measures used against the analyzed security risks. The security measures were categorized into three; existing network security measures such as firewalls, SIP protocol security measures such as change of the default port 5060 and infrastructure security measures such as traffic segmentation. The above has been further discussed in section 5.2.

Through implementation of this security measures, the organization is able to secure the technological aspect of SIP- based VoIP which includes the network, SIP methods and equipment used.

5.3.2 People and organizational security aspects

As earlier stated, in section 5.2.4, a security model need not only cater for the technological aspect of security but also the organizational and user needs. Security is an all rounded activity which needs to cater for people's interactions with the secured technology. If the persons' interacting with the technology are not properly trained in its use and security risks that can affect the technology; this creates a vulnerability through which a user can expose the technology to a security risks unknowingly.

Organizations need to come up with proper IT policies that not only cater for the technological part of security but also one that ensures employees are fully trained on IT security and its importance. Since not all employees are usually tech survey, the organizations needs to properly secure its networks from internal security risks by ensuring employees are properly trained on the use of technology. IT policies should not only be created, but also effectively implemented to ensure high security awareness in an organization.

5.3.3 Information security

According to Albers et al, (2005), the key components fundamental in ensuring information security include: confidentiality, availability and integrity of information at all times. In

order for a security model to be effective in an organization, confidentiality, integrity and availability of information has to be ensured.

Information security aims at ensuring that both external and internal security risks are dealt with effectively. During development of the security model, the study aimed at not only catering for the technological security risks; but also the organizational and people security risks. This was with the aim of ensuring availability, integrity and confidentiality of information at all times.

5.4 Proposed SIP-based VoIP Security Model

The proposed model offers a comprehensive guide and procedure through which organizations can implement security on the SIP-based VoIP network. From the previous subsections on the various components of the model, it can be seen that the model addresses three major components; Technology, information security and organization and people. Looking at the Conceptual Framework proposed earlier on in Chapter 2 (See Figure 2.7), it is evident that network infrastructure, existing security risks and organizational security awareness are important factors to consider during development of the proposed model.

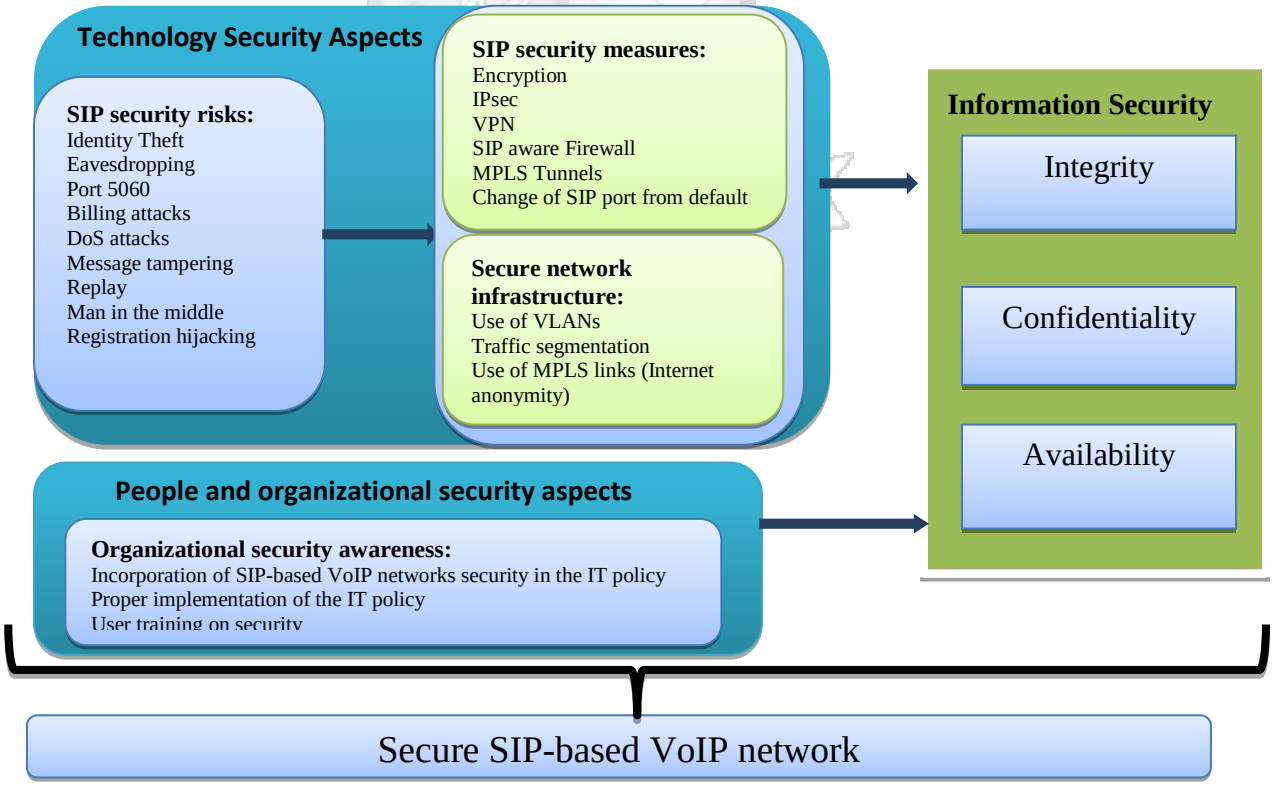


Figure 5.1: Proposed SIP-based VoIP security model

5.5 Model implementation

The proposed model enables the organization to better mitigate its SIP-based VoIP network against existing security risks that can compromise the major information security components that consists of; confidentiality, integrity and availability of information at all times. Based on the preceding subsections the design model is addressed three major components discussed in section 5.3.

The proposed model enables the organization to better mitigate its SIP-based VoIP network against existing security risks that can compromise the major information security components that consists of; confidentiality, integrity and availability of information at all times. The SIP-based VoIP architecture developed in the study figure. 2.6 mainly looks into securing the SIP-based VoIP network by fully eliminating the internet aspect on the clients end through introduction of a MPLS cloud that is completely alienated from the internet. This will work effectively in reducing the client's cost in purchase of security hardware, applications and implementation of security configuration on their end; it also helps in enabling easy implementation of the model on the clients end.

In order for the model to be effectively incorporated in the organizations environment, the various steps discussed in section 5.2 are important in ensuring that we not only cater for the technological aspects but also the people and organizations expectations and needs so as ease assimilation of the design and mitigation of security risks on the client's SIP-based VoIP environment

VT OMNES VNVM SINT

CHAPTER 6: DISCUSSION

6.1 Introduction

In this chapter the researcher discusses how the research objectives were addressed and if they were met. The research had five objectives with the development and validation of the security model being the main objective.

The study identified various security risks on the SIP-based VoIP network as analyzed in section 2.3 of the literature review. The security risks bordered on technology and organizational security awareness. These security risks included: identity theft, billing attacks, Dos and lack of decisive IT policies. The research, through the questioner, identified that despite presence of IT policies, organizational security awareness is only moderate.

To ensure communication is secured and accessible; availability, confidentiality, integrity of information has to be ensured at all times. The study analyzed two existing SIP-based VoIP security models: end to end encryption model and multilayer secured SIP based VoIP model. From the survey, respondents rated availability based security risks were the most frequent security risks faced and end to end encryption as the preferred model.

In order to analyze the effectiveness of MPLS in mitigating security risks, the study used various steps; 1. The study analyzed the MPLS architecture in order to understand how MPLS works. 2. The features of MPLS as a protocol were identified 3. Interactions between VoIP and MPLS were identified and analyzed. 4. Once it was identified that MPLS and VoIP are compatible, the study analyzed how the various security features on the MPLS architecture can be implemented and used to secure SIP-based VoIP networks. More details on the above are addressed extensively in section 2.5 of the literature review. From the survey, security on the MPLS platform was further emphasized as more than ¾ of the respondents stated that MPLS was highly secure.

The model was developed using a four step process which entails; analyzing existing SIP-based VoIP security measures, SIP-based VoIP network infrastructure, SIP protocol security and organization security awareness. The model accomplishes an effective and secure SIP-based VoIP network by supporting a systematic and thought of security approach. This ensures that security implementation is informed by the security risks identified and the organization's security needs.

6.2 Validation of the model

The key expectation of the SIP-based VoIP security model is its effectiveness in mitigating organizations' against existing security risks to their voice network. There exist various challenges in the implementation of SIP-based VoIP network security in an organization. These vary with regards to the existing SIP-based VoIP components and the level of security awareness in the organization. The key measure of security model effectiveness is its ability to enable the organization mitigate against existing SIP-based VoIP security risks. The inputs into the model and its outputs after implementation should be able to be quantified into an effective and efficient security solution. Table 6.1, uses components of the security model to help the organization ascertain not only how effective the security model is in mitigating against existing security risks.

The components were ranked on a scale of 1 to 5; 1 being the least favorable and 5 being the most favorable. The respondents used were using various SIP-based VoIP solutions; for the purpose of the study we selected 4 main solution scenarios in order to validate the model.

VT OMNES VNVM SINT

Table 6.1: Activities/Outputs and Measurement Metrics for the Model

Technological Aspects	Activities	Measurement Metrics	Score/Ranking				
			1	2	3	4	5
Analyse existing SIP-based VoIP security measures	• Evaluation of the exiting SIP-based VoIP network in order to identify security risks the current solution may be vulnerable to. • Identification of security gaps in the organization at large. • Implementation of various security measures; Encryption, Firewall, MPLS tunnels, IPsec, VPN on the organization's SIP-based VoIP network.	• Was an extensive evaluation done on your existing SIP-based VoIP network during identification of the security gaps? • Were security gaps clearly identified and documented as per you expectations? • Have all security gaps identified been protected against after implementation of the security model?					
SIP-based VoIP network infrastructure	• Design of a customized SIP-based VoIP security model suitable for the organization's existing SIP-based VoIP network. • Effective network infrastructure that ensures SIP-based VoIP communication availability, confidentiality and integrity at all times.	• Has the proposed security model been effectively incorporated into the existing SIP-based VoIP network? • Does the designed solution meet the expected security standards for your SIP-based VoIP network? • Do you have an efficient network infrastructure that facilitates information security after implementation of the proposed model?					
SIP Protocol security	• Configuration of SIP communication on a non-default port. • Encryption of SIP messages and methods transmitted.	• Has your SIP traffic been effectively encrypted and secured to ensure information confidentiality and integrity. • Has the SIP port changes better mitigated you against Dos attacks?					

Subtotal Ranking							

Organizational and people security aspect	**Activities**	**Measurement Metrics**	**Score/Ranking**				
			1	**2**	**3**	**4**	**5**
Organizational security awareness	• Ensuring a change in the organizations security awareness culture that is effective implementation of the IT security policies through frequent trainings and proper employee induction on the policies. • Implementation of internal security measures such as traffic segmentation and VLANs. • Clear documentation of the entire SIP-based VoIP security model spectrum including its scalability and how it handles security issues on the SIP-based VoIP network. • Knowledge transfer to the organizations technical staff.	• Are staff fully inducted and trained on the organizations security policies? • Is there a noticeable change for the better with regards to staff security awareness? • Do you have a training plan in which the technical staff will be trained on the implement security model? • Is VoIP and data traffic segmented to ensure voice traffic security? • Do you have a detailed documentation which can be used for future reference with regards to the implemented security model?					
Subtotal Ranking							
		Overall Ranking					

6.2.1 Model Validation Results

The validation results were collected from four organizations. The designed SIP-based VoIP security model scored high in regards to its efficiency and implementation. This is because as illustrated in the model, the tight link between People and Technology is crucial for success of a security model as security is an all rounded factor. Critical selection of vendors/integrators based on the existing different SIP-based VoIP network components in the organizations, lead to the success of the model.

The selected organizations gave a fair representation of the different SIP-based VoIP solutions in which the research findings were mainly based. The selection as stated was based on the various VoIP solutions implemented by the organizations based on figure.1.1. Overall, these firms already have SIP-based VoIP solutions through which they can measure themselves against.

Table 6.2: Model Validation Results

	Organization	**Score 1**	**Score 2**	**Total Score**
1	XTX Communications Provider	39	20	59
2	ABC networks solutions provider	40	22	62
3	EFG Bank	35	23	58
4	NYZ Sacco	30	22	52
Maximum Score		40	25	65

Note:

Score 1: Technological aspect

Score 2: Organizational and people security aspect

The organizations names were hidden due to their anonymity request. The maximum score that could be obtained was 65, which is a score of 5 for each metric. The minimum score is 13 indicating a score of 1 for each metric.

Table 6.3: Score indicator interpretation

13- 29	Indicates that the security model components were not clearly aligned to the organizational security requirements.
30 -54	Indicates that the proposed SIP-based VoIP security model has medium effectiveness in ensuring security on organizations SIP-based VoIP networks.
54 -65	Indicates that the proposed SIP-based VoIP security model has high effectiveness in ensuring security on organizations SIP-based VoIP networks.

Organizations that involved users, business Process and Technology into their SIP-based VoIP security strategy scored much higher as expected. From Table 6.2, we note the closeness in scores indicating that technological, organizational and people security aspects are closely linked to success of securing a SIP-based VoIP network and the security model proposed. The validation results also show that the security model is valid.

6.3 Discussion summary of the Proposed Model

As indicated, during design and implementation of a security model two main aspects need to be considered and put into consideration by an organization. These aspects include: Technology, organization and people. From the discussion of findings it is important to note that different factors influence a security model in an organization. They range from technological aspects, business processes; user incorporation and security sensitization which are interweaved. This factor are very important in ensuring information security is attained.

In order for a security model effects and efficiency to be able to resonate within the organization, an organization needs to ensure that the users are well inducted and aware of the organization's information security stand. This can be achieved through strict implementation and induction to the organizations the security policies and repercussion on failure of adherence.

CHAPTER SEVEN: CONCLUSION AND RECOMMENDATIONS

7.1 Conclusions

The research has highlighted the security risks and gaps in the SIP-based VoIP network in Kenya, and pin pointed causes that have led to VoIP scoring highest as a top security risk in Kenya. It has achieved its aim by confirming the need of appropriate security measures in organizations in mitigating SIP-based security risks and has gone as far as proposing a SIP-based VoIP security model.

Ensuring of a secure IP-based environment is an all rounded approach which needs to cater for not only the technological security risks but also the human based risks. The organization need to not only cater for the technological based risks but also ensure that its staff is well knowledgeable and trained on the use of IT services and information. In order to do so, an organization needs to understand the SIP-based VoIP network fully in terms of its implementation, maintenance, security risks and measures.

The study concludes that MPLS technology by designing and proposing an all rounded SIP-based VoIP security model that provides security not only secure the SIP-based VoIP network but also highlights how to best implement the model.

7.2 Recommendations

From the study findings and conclusions, the study recommends that Kenya is still on the early stages of securing the IT environment against logical security risks with the formulation of the Kenya Information and communications act in 2009. The researcher has the below recommendations aimed at better mitigating SIP-based security risks as below;

The government needs to place security regulations with regards to not only securing data traffic but also to security of voice traffic on the open internet environment. Data traffic has been greatly highlighted of late in terms of its security. However as SIP-based VoIP security has been greatly bypassed in Kenya as there is minimal documentation in regards to its security and regulations in Kenya.

The VoIP service providers need to assist organizations in securing their voice networks by advising them to continually enhance their security against SIP-based VoIP security risks. The VoIP service provider also needs to secure the VoIP network on their end at all times.

Organizations need place more emphasis on securing their IT environment. IT policies should be present and implemented in the at all times. New staff should also be inducted on the firm's security policies as soon as they are hired. They need to also ensure that the implementation of SIP-based networks is done in a secure manner in their networks at all times.

Security measures and risks are ever evolving therefore the above parties need to keep on adjusting, updating and modifying the security measures in place. New security risks are always emerging making security an ongoing process at all times.

7.3 Further research areas

Security measures needed in mitigating SIP-based security risks are ever evolving and even increasing. This research can be advanced further through further modification of the proposed security model with regards to upcoming SIP-based VoIP security risks. Further research also needs to be done on how quality of service can be ensured during the implementation of SIP-based VoIP security measures in SIP-based networks.

VT OMNES VNVM SINT

REFERENCES

Al-Awadi, M., & Renaud, K. (2007). *SUCCESS FACTORS IN INFORMATION SECURITY IMPLEMENTATION IN ORGANIZATIONS.* Lilybank Gardens, Glasgow: University of Glasgow.

Alcatel-lucent. (2010). Rail-system Operator Telecommunications. *Enhancing security, boosting efficiency and increasing passenger services with the Alcatel-Lucent Mission-critical WAN Infrastructure*, pp. 1- 13.

Arafat, M. Y., Ahmed, F., & Sobhan, A. M. (2013). SIP security in IP telephony. *Elastix world mexico 2013*.

Asghar, G., & Azmi, Q. J. (June 2010). *Security Issues of SIP.* BLEKINGE INSTITUTE OF TECHNOLOGY SCHOOL OF ENGINEERING.

Ashraf, S. (2005, February 08). Global Information Assurance Certification Paper. (G. I. Certification, Ed.) *Orgasnization needs and everyone's responsibity,Information Security Awareness*(Version 1.4c).

Aziz, A., Hoffstadt, D., Rathgeb, E., & Dreibholz, T. (2014). *A Distributed Infrastructure to Analyse SIP Attacks in the Internet.* Institute for Experimental Mathematics. Germany: University of Duisburg-Essen.

Backfield, J. (2008). *Network Security Model.* SANS Institute Reading Room site.

Bader-uz-zaman, S., Razzaq, F., Arshad, F., Khayyam, S., & Ahmed, S. (July 2010). Synopsis of Security Threats and Implements in SIP-Based VoIP System. *Canadian Journal on Network and Information Security Vol. 1, No. 5*, 51 - 55.

Bishop, M. (2002). *Computer security Art and Science.* Addison Wesley.

Blythe, J. M. (2011). Cyber security in the workplace: Understanding and promoting behaviour change. New castle, United Kingdom: Springer.

Bryman, A., & Bell, E. (2007). *Business Research Methods revised edition.* Oxford University Press.

Capacity business briefing. (2013, August). Fraud & security. *Fraud types*, 12-15.

Cisco. (2014). State of Security Report 2014. *Voice & Unified Communications*. Retrieved from http://products.mcisco.com/c/dam/en/us/products/collateral/unified-communications/unified-border-element/sl-securityreport2014-041814.pdf

COX Business. (2009). Carrier Ethernet:Transforming Business Telecommunications. *Metro Ethernet Whitepaper*, 1-8.

Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research* (4th ed.). Upper Saddle River: NJ: Merrill.

Dantu, R., Fahmy, S., schulzrinne, H., & Cangussu, J. (2009, May 3). Issues and challenges in securing VoIP. *Computer & Security*, pp. 1-11.

Denscombe, M. (2007). *The good research guide : for small-scale social research projects.* New York: Open University Press.

Davis, F, D. (1986). A technology acceptance model for empirically testing new end-user information systems: Theory and results. Doctoral dissertation. Cambridge, MA: MIT Sloan School of Management.

Dishaw, M., T, & Strong, D, M. (1999). Extending the technology acceptance model with task-technology fit constructs. *Information & Management*, 36(1), 9-21

Ehlert, S. (2009). *Denial-of-Service Detection and Mitigationfor SIP Communication Networks.* Berlin: Institute for Open Communication systems.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review 14*, 57-74.

Enterprise Risk Management, Inc. (2011, February). *Securing Information Protecting Reputations.* Retrieved from VoIP Security: Do You Have a Good Voice…over IP?: http://www.emrisk.com/sites/default/files/newsletters/ERMNewsletter_February_2011.pdf

Epps, D., Tanner, S., & Silva, C. (2006, May). Can VoIP Secure Itself for the Next Technology Wave?. *Information Systems Security*, 15(2), 9-15.

European Network and Information Security Agency. (2010, November). The new users' guide:How to raise information security awareness. Heraklion, Greece.

Evans, M., Hastings, N., & Peacock, B. (2000). Statistical Distributions, 3rd ed. New York: Wiley.

Ferdous, R. (2014, May). *Analysis and Protection of SIP based ServicesRaihana Ferdous.* University of Trento. Retrieved from http://eprints-phd.biblio.unitn.it/1264/1/PhD-Thesis-RaihanaFerdous.pdf

Fjellskål , E. B., & Solberg , S. (2002, May). Evaluation of Voice over MPLS (VoMPLS) compared to Voice over IP (VoIP). Grimstad: Agder University College.

Geneiatakis, D., Lambrinoudakis, C., & Kambourakis, G. (2008). An Ontology Based-Policy for Deploying Secure SIP- based VoIP Services. Samos, Greece: University of the Aegean.

Geneiatakis, D., Dagiuklas, T., Kambourakis, G., Lambrinoudakis, C., Gritzalis, S., Ehlert, S., & et al. (2006, July). Survey of security vulnerabilities in Session Initiation Protocol. *IEEE Communications Surveys and Tutorials, 8*(3), 68-81.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*.

Ho, T. H., & Chen, Y. (2014, April 18). Vietnamese Consumers' Intention to Use Online Shopping: The Role of Trust. *International Journal of Business and Management, 9(5)*, 145-159.

House of buck. (n.d.). *A Brief History*. House of buck. Retrieved from http://houseofbuck.com/images/History_of_Computers.pdf

International Telecommunication Union. (2007, January 12). The status of Voice over Internet Protocol (VoIP) worldwide, 2006. (P. Biggs, Ed.) *The future of voice*.

Irny, S. I., & Rose, A. A. (2005). Designing a Strategic Information Systems Planning Methodology for Malaysian Institutes of Higher Learning (isp- ipta). *Issues in Information System, VI*(1).

Jaber, A. N., Tan, C.-W., Manickam, S., & Khudher, A. A. (2012). Session Initiation Protocol Security: A Brief Review. *Journal of Computer Science*, *8*(3), 348-357.

Jallow, L., Hwang, I.-S., Nikoukar, A., & Liem, A. T. (2014, March). A SIP-based VoIP Application in Enhanced Ethernet Passive Optical Network Architecture. *International MultiConference of Engineers and Computer Scientists, II*.

Jensen, M. C., & Meckling, W. H. (1976, October). Theory of the Firm: Managerial Behavior,Agency Costs and Ownership Structure. *Journal of Financial Economics*, 305-360.

Jones, D., Roach, P., Setter, J., & Esling, J. (2013, June 24). Cambridge Advanced Learner's Dictionary. Cambridge: Cambridge University Press; 4 edition. Retrieved from http://dictionary.cambridge.org/us/dictionary/british/

Keller, S. (1977). The telephone in new, and old, communications. In Ithiel de Sola Pool (Ed.). The social impact of the telephone, Cambridge, MA: MIT press, 281-298.

Kenya Law Report. (2009). The Kenya Information And Communications Act. *LAWS OF KENYA*. National Council for Law Reporting.

Kowitlawakul, Y. (2008). *TECHNOLOGY ACCEPTANCE MODEL:PREDICTING NURSES' ACCEPTANCE OF TELEMEDICE TECHNOLOGY(eICU).* Fairfax,VA: George Mason University.

Kuhn, R., Walsh, T., & Fries, S. (2005, January). Security considerations for Voice over IP systems – recommendations of the National Institute of Standards and Technology. *Technical Report SP 800-58. USA:National Institute of Standards and Technology*.

Lazzez, A. (2013). *VoIP Technology: Security Issues Analysis.* Kingdom of Saudi Arabia: Taif University.

Leung, L. (2001). Gratifications, chronic loneliness and internet use. *Asia Journal of Communication*, 96-119.

Lohiya, K., Shekokar, N., & Devane, S. R. (2012, March). End to End Encryption Architecture for Voice over Internet Protocol. *International Journal of Computer Applications (0975 – 8887), 41*, 31-34.

Microsoft Corporation. (2015). *Session Initiation Protocol Extensions.* Microsoft Corporation.

Mowery, C. D., & Simcoe, T. (1998). *Is the Internet a U.S. Invention? – An Economic and Technological History of Computer Networking.* Berkeley: University of California. Retrieved from http://www.druid.dk/conferences/nw/paper1/movery.pdf

Ngoma, S. (2012, March 4). Vulnerability of IT Infrastructures: Internal and External Threats.

Noble, G. (1989). Towards a "uses and gratifications" of the domestic telephone. *In Telefon und Gesellschaft*, Berlin: Volker Spiess, 198-307.

Ogunsola, L. A. (2005). Information and communication technologies and the effects of globalization: Twenty-first century "digital slavery" for developing countries--myth or reality? *Electronic journal os academic and special librarianship, 6*.

Oliver, B. (2010). *TEACHING FELLOWSHIP: FOR GRADUATE EMPLOYABILITY BENCHMARKING PARTNERSHIPS.* Bentley: Curtin University.

Orodho, A. J. (2003). *Essentials of Educational and Social Sciences Research Method.* Nairobi: Masola Publishers.

Orodho, A., & Kombo, D. (2002). *Research Methods.* Nairobi: Kenyatta University Institute of Open Learning.

Packetizer Inc. (2013). *Introduction to VoIP*. Retrieved December 18, 2013, from Packetizer:

http://www.packetizer.com/ipmc/papers/understanding_voip/voip_introduction.html

Park, P. (2008). *Voice over IP Security: Security Best Practices Derived from Deep Analysis of the Latest VoIP Network Threats.* Cisco Press.

Parsons, K., McCormac, A., Butavivius, M., & Ferguson, L. (2010). Human Factors and Information Security: Individual, Culture and Security Environmen. Edinburgh, South Australia. Retrieved from http://www.dtic.mil/dtic/tr/fulltext/u2/a535944.pdf

Pavlovski, C. (2007).IP Multimedia Systems (IMS) Infrastructure and services: Service delivery platforms in practice. Communications Magazine, (45), 114-121.

Rahangdale, T. G., Tijare, P. A., & Sawalkar, S. N. (2014, April). An overview on security analysis of Session Initiation Protocol in VoIP network. *International Journal of Research in Advent Technology, 2*(4), 190-195.

Richardson, J. (2005). Assessment & Evaluation in Higher Education 30. *Instruments for obtaining student feedback: a review of the literature, 4*, 387–415.

Ruck, M. (2010). Top Ten Security Issues Voice over IP (VoIP). *Project VoIP Security*.

Rogers, E.M. (2003). *Diffusion of innovations* (5th ed.). New York: Free Press.

Roll-Hansen, N. (2009). Why the distinction between basic (theoretical) and applied (practical) research is important in the politics of science . In D. Fennell (Ed.), *Centre for the Philosophy of Natural and Social Science Contingency and Dissent in Science* (pp. 1-31). London: Contingency And Dissent in Science Project.

Rosenberg, J., & Jennings, C. (2008). *The Session Initiation Protocol (SIP) and spam.* RFC 5039.

Rubin, A. M. (2002). Media uses and effects: A uses and gratifications perspective. (J. Bryant, & D. Zillmann, Eds.) *Media effects: advances in theory and research*, 525-544. Retrieved from http://wf2dnvr1.webfeat.org:80/rn8nG183/url= http://site.ebrary.

Rubin, A. M., & Papacharissi, Z. (2000). Predictors of internet use. *Journal of Broadcasting and Electronic Media, 44*(2), 175-196.

Sarantakos, S. (2005). *Social Research* (3rd ed.). Melbourne: Macmillan Education.

Schlienger, T., & Teufel, S. (2003). Information security culture: From analysis to change. *Proceedings of the 3rd Annual Information Security South Africa Conference (ISSA),* Johannesburg, South Africa,183–196.

Sadek, R. A., Ghalwash, A. Z., & Basem, B. (2015). Multilayer Secured SIP Based VoIP Architecture. *International Journal of Computer Theory and Engineering, 7*, 453-462.

SERIANU cyber intelligence team. (2012). *Kenya cyber security report 2012, Getting back to security basics , edition one.* Kenya: SERIANU.

Serianu Limited. (2014). Rethinking Cyber Security – "An Integrated Approach: Processes, Intelligence and Monitoring.". *Kenya cyber Security Report 2014*.

Singer, B. (1981). Social Functions of the Telephone. Palo Alto, CA: R & E Research Associates.

Suruhanjaya Komunikasi dan Multimedia Malaysia. (2007). *IP Telephony.* Selangor Darul Ehsan: Off Persiaran Multimedia.

Tao, D. (2008, May). USING THEORY OF REASONED ACTION (TRA)IN UNDERTANDING SELECTION AND USE OF INFORMATION RESOURCES:AN INFORMATION RESOURCE SELECTION AND USE MODEL. Columbia: University of Missouri.

TELES AG Informationstechnologien. (2009). TELES Class 5 NGN. 10587 Berlin, Germany.Retrieved November 27, 2013, from http://sintel.com/bibli/telechargement/143/document_Multi.pdf

TESPOK. (2014). *Background*. Retrieved March 10, 2014, from TESPOK: http://www.tespok.co.ke/?page_id=17

Thermos, P., & Takanen, A. (2008). *Securing VoIP Networks: Threats, Vulnerabilities, and Countermeasures.* Boston: Pearson Education, Inc.

Toivanen, T. (2006, May). A study on interworking between centralized SIP, P2P-SIP and PSTN Networks. *TKK T-110.5190 Seminar on Internetworking* .

Trim, P. R. (2005). Managing computer security issues: preventing and limiting future threats and disasters. *Disaster Prevention and Management, 14*(4), 493 - 505.

Ubiquity Software Corporation Limited. (2003). Understanding SIP. *Today's hottest communications protocol comes of age*.

Udoh, E. E. (2010). *The Adoption of Grid Computing Technology by Organizations: A Quantitative Study Using Technology Acceptance Model*. Minneapolis: Capella University

VOIPSA. (2005, October 24). VoIP Security and PrivacyThreat Taxonomy 1 .0. Retrieved from http://www.voipsa.org/Activities/VOIPSA_Threat_Taxonomy_0.1.pdf

Wilson, M., & Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. Wahington DC, USA: National Institute of Standards and technology. Retrieved from http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

World Economic Forum. (2012). Living in a hyperconnected world. (S. Dutta, & B. Bilbao-Osorio, Eds.) *The global information technology report 2012*.

Wulff, T., & Hunt, R. (2010). New Approaches to Mitigation of Malicious Traffic in VoIP Networks. *Proceedings of the 8th Australian Information Security Management Conference* (pp. 173- 181). Christchurch, New Zealand: Research Online.

Yuan, Z. (2002). *SIP-Based VoIP Network And Its Interworking With The PSTN*. China: Shandong University.

Zafar, M. S., & Gill , M. S. (2008, November). Evaluation of UDP and SCTP for SIP-T and TCP, UDP and SCTP with constant traffic. Karlskrona, Sweden: Blekinge Institute of Technology.

Zhang, G. (2009). Performance-related Attacks and Preventions. *Towards Secure SIP Signalling Service for VoIP applications*, pp. 1-21.

Zhang, G. (2012). *Unwanted Traffic and Information Disclosure in VoIP Networks- Threats and Countermeasures.* Karlstad University , Faculty of Economic Sciences, Communication and IT. Karlstad, Sweden: Karlstad University.

Zhang, R., Wang, X., Yang, X., & Jiang, X. (2007, August). Billing attacks on SIP-based. *First USENIX workshop on offensive technology (WOOT '07)*.

Zheng, C., & Kashi, K. (2013, March 1). Extending Technology Acceptance Model to the E-recruitment Context in Iran. *International Journal of Selection and Assessment*, 121-129.

Appendix A: Data Collection Instrument

QUESTIONNAIRE

Dear Participant,

My name is Farida Gakii Kamuti, currently a graduate student, pursuing a Masters in Computer based information systems at Strathmore University. For my final project/Thesis, I am inviting you to participate in this research by completing the attached Questionnaire. This questioner is based on my research, **SECURITY RISKS MITIGATION IN SESSION INTIATION PROTOCOL BASED VOIP NETWORKS IMPLEMENTATION USING MPLS.** The information provided on this questioner is private and shall be used in discretion; no institutions will be named during my study. Your assistance will be highly appreciated.

Research Objectives:

The main objective of this research is to come up with a SIP-based VoIP security model derived from MPLS to use the implementation of SIP-based VoIP network security with the aim of mitigating security risks. This will enable businesses to derive secure VoIP networks and systems through use of MPLS.

PART A: General Information

A1: Duration of interaction with VoIP

Less than a year ☐

1-2 years ☐

3-5 years ☐

Over 5 years ☐

A2. What is the level of importance of voice communication in your organization?

High ☐ Moderate ☐ low ☐

A3. Do you have an IT security policy in your organization?

Yes ☐ No ☐ Not sure ☐

A4.What is the level of IT security awareness among users in your organization?

High ☐ Moderate ☐ Low ☐

PART B: Security risks faced in organizations using SIP-based VoIP networks:

B1. Have you experienced security risks on your SIP-based VoIP network?

Yes ☐ No ☐ Not sure ☐

B2. Please indicate the most frequent type of security risk experience on your SIP-based VoIP network (Select only 1)

Authorization and authentication related security risks ☐

Availability related security risks ☐

Integrity related security risks ☐

Confidentiality related security risks ☐

B3. Please rate the likelihood of the below SIP-based security risks (you can select more than 1)

	Highly likely	Likely	Very unlikely
Identity theft	☐	☐	☐
Eavesdropping	☐	☐	☐
Message Tampering	☐	☐	☐
Replay	☐	☐	☐
Denial of service	☐	☐	☐
Port 5060	☐	☐	☐
Man in the middle attack	☐	☐	☐
Registration hijacking	☐	☐	☐
Billing attacks	☐	☐	☐

VT OMNES VNVM SINT

PART C: Existing security approaches or models against SIP-based VoIP security risks:

C1. Is voice traffic on a dedicated link?

Yes ☐ No ☐ Not sure ☐

C2. Has your organization implemented any security mitigation strategy or policy on the SIP-based VoIP network?

Yes ☐ No ☐

C3. If Yes please answer the below question;

C3a. Please identify which of the below security mitigation approaches or model you have applied in your organization.

Multilayer secured SIP-based VoIP model ☐

End to End Encryption Model ☐

Virtual Private Networks ☐

Intrusion Prevention Systems ☐

Firewall ☐

Encryption ☐

C4. Please rate on a scale of 1 to 3 which of the below security approaches or models suits your organization's SIP-based VoIP network given 1 represents best suited, 2 represents can suit and 3 represents not suitable.

	1	2	3
Multilayer secured SIP-based VoIP model	☐	☐	☐
End to End Encryption Model	☐	☐	☐
Virtual Private Networks	☐	☐	☐
Intrusion Prevention Systems	☐	☐	☐
Encryption	☐	☐	☐
Firewall	☐	☐	☐

PART D: Effectiveness of MPLS to Secure SIP-based VoIP networks

D1. Does your organization have an existing MPLS network?

Yes ☐ No ☐

If yes, please answer the below questions;

D1a. Rate on a scale of 1 to 3 the effectiveness of the below MPLS security components given that 1 represents high , 2 represents medium and 3 represents low.

	1	2	3
Encryption	☐	☐	☐
Internet anonymity	☐	☐	☐
IPsec tunnels	☐	☐	☐
Private LAN	☐	☐	☐
MPLS tunnels	☐	☐	☐

D1b. How do you rate security on your MPLS network?

Highly secure ☐ Secure ☐ Not secure ☐

Thank you for accepting and taking the time to fill in the questioner. In order to ensure that all information will remain CONFIDENTIAL (please DO NOT include your name).